CiscoPro CPA750 Series Command Reference

ciscopro™

CISCO SYSTEMS®

CiscoPro CPA750 Series Command Reference

Corporate Headquarters
170 W. Tasman Drive
San Jose, CA 95134-1706
USA

Customer Order Number: DOC-CPA750CR=
Text Part Number: 78-2163-01

The products and specifications, configurations, and other technical information regarding the products contained in this manual are subject to change without notice. All statements, technical information, and recommendations contained in this manual are believed to be accurate and reliable but are presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this manual.

The following information is provided for FCC compliance of Class A devices:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is provided for FCC compliance of Class B devices:

The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception.

This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices.

If your equipment does cause interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The following third-party software may be included with your product and will be subject to the software license agreement:

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, THE CD-ROM, THE CD-ROM SOFTWARE, AND THE DOCUMENT FILES AND SOFTWARE OF THE ABOVE-LISTED SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Notice of Restricted Rights:

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR §52.227-19 and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS §252.227-7013. The information in this manual is subject to change without notice.

CiscoPro CPA750 Series Command Reference

959R

SOFTWARE LICENSE

READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE.

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THE SOFTWARE. BY USING THE SOFTWARE OF CISCO SYSTEMS, INC. AND ITS SUPPLIERS FROM TIME TO TIME, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT AGREE WITH THE TERMS OF THIS LICENSE, PROMPTLY RETURN THE UNUSED SOFTWARE, MANUAL, AND RELATED EQUIPMENT (WITH PROOF OF PAYMENT) TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Cisco Systems, Inc. ("Cisco") grants to Customer ("Customer") a nonexclusive and nontransferable license to use the Cisco software ("Software") in object code form solely on a single central processing unit owned or leased by Customer or otherwise embedded in equipment provided by Cisco. Customer may make one (1) archival copy of the software provided Customer affixes to such copy all copyright, confidentiality, and proprietary notices that appear on the original.

EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, CUSTOMER SHALL NOT: COPY, IN WHOLE OR IN PART, SOFTWARE OR DOCUMENTATION; MODIFY THE SOFTWARE; REVERSE COMPILE OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, SELL, OR CREATE DERIVATIVE WORKS OF THE SOFTWARE.

Customer agrees that aspects of the licensed materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Cisco. Customer agrees not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior consent of Cisco. Customer agrees to implement reasonable security measures to protect such trade secrets and copyrighted material. Title to Software and documentation shall remain solely with Cisco.

LIMITED WARRANTY. Cisco warrants that the Software will substantially conform to the published specifications for such Software, if used properly in accordance with the Documentation, for a period of one year from the date of shipment. To be eligible for a remedy, Customer must report all warranted problems within the warranty period to the party that supplied the Product to Customer or to the Cisco Service Partner if the Software was exported under the multinational uplift program. Cisco's sole and exclusive obligation and Customer's exclusive remedy with respect to nonconforming Software upon contact will be, at Cisco's option and potentially through the Sales or Service Partner, either (i) to provide a correction or a workaround for any reproducible errors, or (ii) to refund to Customer the license fee for the Software in the event that a license fee was paid and the other remedy is not available, or, if the license fee was zero, refund the price of the hardware less depreciation calculated on a straight-line basis. Customer agrees to cooperate with Cisco or its Sales or Service Partner in creating the environment in which the error occurred. Further, Customer agrees to supply any necessary equipment for such tests.

This Limited Warranty does not apply to Software which (1) has been altered, except as authorized by Cisco, (2) has not been installed, operated, repaired, or maintained in accordance with any installation, handling, maintenance, or operating instructions supplied by Cisco, (3) has been subjected to unusual physical or electrical stress, misuse, negligence, or accident, (4) is used in ultrahazardous activities, (5) has been used in such a way that Cisco or its Sales Partner cannot reasonably reproduce the Software error, (6) has been exported from the original country of destination without payment of an uplift, or (7) has been misapplied. In no event does Cisco warrant that the Software is error free or that Customer will be able to operate its networks without problems or interruptions.

DISCLAIMER. THIS WARRANTY IS IN LIEU OF AND CISCO DISCLAIMS ALL OTHER WARRANTIES AND CONDITIONS, EXPRESSED OR IMPLIED, INCLUDING THOSE OF MERCHANTABILITY, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS CISCO SOFTWARE, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

Customer will comply with all applicable export laws and regulations if it exports the products. This restriction shall survive termination of this Agreement.

This License is effective until terminated. Customer may terminate this License at any time by destroying the software together with all copies thereof. Cisco may immediately terminate this License if the Customer fails to comply with any term or condition hereof. Upon any termination of this License, Customer shall discontinue use of the Software and shall destroy all copies of the software.

This License shall be governed by and construed in accordance with the laws of the State of California. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This License constitutes the entire License between the parties with respect to the use of the Software.

Restricted Rights - Cisco's software and supporting documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR §52.227-19 and subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS §52.227-7013.

HARDWARE WARRANTY

Performance Warranty. Cisco warrants to Customer, for a period of one year from the shipping date, that Hardware purchased from Cisco will be free from hardware defects in material and workmanship. To be eligible for a remedy, Customer must report all warranted problems within the warranty period to the party that supplied the Product to Customer or to the Cisco Service Partner if the Hardware was exported under the multinational uplift program.

Hardware Remedies. In the event of a warranted problem with respect to the Hardware, Customer must contact the place it acquired the Hardware or the Cisco Service Partner if the Hardware was exported pursuant to the multinational uplift program as soon as possible after Customer becomes aware of the defect. Cisco or the Sales or Service Partner (as appropriate) will supply replacement parts for the products listed in Cisco's recommended spares list. Replacement parts will be shipped within five (5) working days after receipt of Customer's request. Cisco or its Sales or Service Partner will bear the cost for shipment of advance replacements to Customer. Customer must return all defective boards and assemblies prior to installation of the replacement boards and assemblies to Cisco or the Sales or Service Partner in accordance with the then-current return material authorization (RMA) procedures. Cisco's sole and exclusive obligation with respect to defective Hardware will be, at Cisco's option and through a Sales or Service Partner if necessary, to either (i) provide advance replacement service as described above, (ii) replace the Product with a Product that does not contain the defect, or (iii) refund the price paid for the Hardware less depreciation calculated on a straight-line basis.

Exclusions. The above warranty does not apply to any Product which (1) has been altered, except as authorized by Cisco, (2) has not been installed, operated, repaired, or maintained in accordance with any installation, handling, maintenance, or operating instructions supplied by Cisco, (3) has been subjected to unusual physical or electrical stress, misuse, negligence, or accident, (4) is used in ultrahazardous activities, (5) has been used in such a way that Cisco cannot reasonably reproduce the Software error, or (6) has been exported from the original country of destination without payment of an uplift. In no event does Cisco warrant that Customer will be able to operate its networks without problems or interruptions.

DISCLAIMER. THIS WARRANTY IS IN LIEU OF AND CISCO DISCLAIMS ALL OTHER WARRANTIES AND CONDITIONS, EXPRESSED OR IMPLIED, INCLUDING THOSE OF MERCHANTABILITY, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS CISCO SOFTWARE, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

TABLE OF CONTENTS

LIST OF TABLES

About This Manual

This section discusses the objectives, audience, organization, and conventions of the *CiscoPro CPA750 Series Command Reference* publication.

CiscoPro product documentation and additional literature are available on UniverCD for CiscoPro. UniverCD for CiscoPro is updated and shipped monthly, so it might be more up to date than printed documentation. UniverCD for CiscoPro is available both as a single CD and as an annual subscription. To order UniverCD for CiscoPro in North America, contact your local reseller; international customers, contact your local Cisco sales office.

Document Objectives

This document provides descriptions of the commands necessary for configuring and maintaining your CiscoPro CPA750 series router. It describes tasks only in the context of using a particular command. It does not describe how the tasks interrelate or provide comprehensive configuration examples. It can be used as a standalone reference manual or in conjunction with the *CiscoPro CPA750 Series User Guide*, *Setting Up Your ISDN BRI Service for CiscoPro CPA750 Series*, *CiscoPro Configuration Guide,* and the *CiscoPro Command Reference.*

Audience

This publication is intended as a standalone document for users who will be configuring and maintaining the CiscoPro CPA750 series router and just need to reference commands.

Document Organization

This publication is divided into chapters, describing related tasks or functions. The chapters in the publication are as follows:

- Chapter 1, "CiscoPro CPA750 Series Overview," provides an overview of the CiscoPro CPA750 series dial-on-demand routers.
- Chapter 2, "Terminal Setting Commands," describes the commands used for configuring the terminal emulation software.
- Chapter 3, "System Management Commands," describes the commands pertaining to system interfaces, system booting, and terminal sessions.
- Chapter 4, "Profile Commands," describes the commands used to create and configure user profiles.
- Chapter 5, "Security Commands," describes the commands used to configure router security.

- Chapter 6, "Ethernet Interface Commands," describes the commands used to configure the Ethernet interface.
- Chapter 7, "ISDN Commands," describes the commands used to configure ISDN calling, such as on-demand, CALLBACK, and CALLERID.
- Chapter 8, "IP Commands," describes the commands used to configure IP routing, such as IP static routes, RIP, and IP filters.
- Chapter 9, "Novell IPX Commands," describes the commands used to configure IPX routing, such as IPX static routes, RIP, SAP, and SPX service routes.
- Chapter 10, "Transparent Bridging Commands," describes the commands used to configure transparent bridging, such as filtering and address learning.
- Chapter 11, "PPP Commands," describes the commands used to configure Point-to-Point protocol (PPP) parameters, such as call negotiation and authentication.
- Chapter 12, "SNMP Commands," describes the commands used to configure System Network Management Protocol (SNMP) parameters, such as management station and traps.
- Chapter 13, "DTMF Commands," describes the commands used to configure the basic telephone service interface.

Document Conventions

Software and hardware documentation uses the following conventions:

- The caret character (^) represents the Control key.

  For example, the key combinations ^D and Ctrl-D are equivalent: Both mean hold down the Control key while you press the D key. Keys are indicated in capitals, but are not case sensitive.
- A string is defined as a nonquoted set of characters.

  For example, when setting an SNMP community string to "public," do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command descriptions use these conventions:

- Vertical bars (|) separate alternative, mutually exclusive, elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) indicate a required choice.
- Braces within square brackets ([{ }]) indicate a required choice within an optional element.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values; in contexts that do not allow italics, arguments are enclosed in angle brackets (< >).

Examples use these conventions:

- Examples that contain system prompts denote interactive sessions, indicating that the user enters commands at the prompt. The system prompt indicates the current command mode. For example, the prompt `router(config)#` indicates global configuration mode.
- Terminal sessions and information the system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).

Timesaver This symbol means the described action saves time. You can save time by performing the action described in the paragraph.

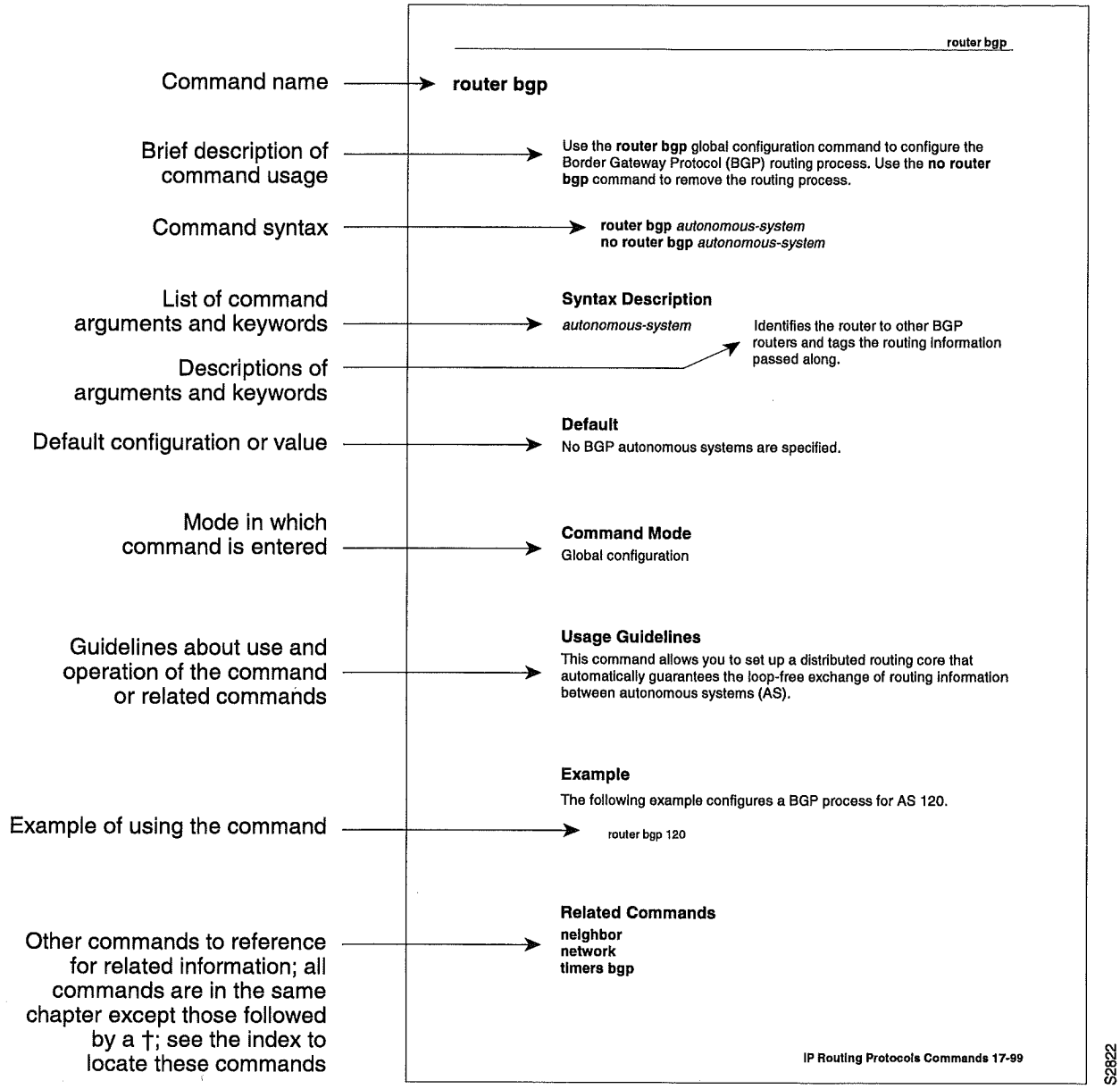
Caution This symbol means *reader be careful.* In this situation, you might do something that could result in equipment damage or loss of data.

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translated versions of this warning, refer to the appendix "Translated Safety Warnings."

Note Means *reader take note.* Notes contain helpful suggestions or references to materials not contained in this manual.

The following illustration explains the fields of a typical command reference page.

Figure 1 Typical Command Reference Page Fields



CHAPTER 1

CiscoPro CPA750 Series Overview

The CiscoPro CPA750 series routers connect small office Ethernet LANs to corporate networks through Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) lines. After configuration, the router automatically routes packets to and from remote destinations using Internet Protocol (IP) or (Internetwork Packet Exchange) IPX. The remote dial-up network routing connections are made on-demand.

Supported Protocols

The CiscoPro CPA750 series routers support the following protocols:

- IP
- IPX
- Point-to-Point Protocol (PPP)
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Routing Information Protocol (RIP) for IP and IPX
- Service Advertisement Protocol (SAP)
- Address Resolution Protocol (ARP)
- Simple Network Management Protocol (SNMP)
- Trivial File Transfer Protocol (TFTP)
- Internet Control Message Protocol (ICMP)
- Internet Protocol Control Protocol (IPCP)
- Internetwork Packet Exchange Control Protocol (IPXCP)

Supported Interfaces and Connections

The CiscoPro CPA750 series routers have the following port for LAN and WAN connections:

- 1 RJ-45 10BaseT port for connection to a 10BaseT Ethernet network
- 1 BNC 10Base2 port for connection to a 10Base2 Ethernet network
- 1 RJ-45 ISDN BRI S port for connection to the ISDN line (CiscoPro CPA751)
- 1 RJ-45 ISDN BRI U port for an optional connection to an ISDN device, such as telephone or fax (CiscoPro CPA752 and CiscoPro CPA753)
- 1 RJ-11 basic telephone service port for connection to an analog device, such as telephone, modem, or fax (CiscoPro CPA753)

Administrative Configuration Options

The CiscoPro CPA750 series router can be configured through the configuration port or across an Ethernet network using Telnet.

CHAPTER 2

Terminal Setting Commands

This chapter describes the commands used for configuring the terminal emulation software.

set baud

To configure the baud rate for the console port, use the **set baud** command.

set baud {1200 | 2400 | 9600 | 19200 | 38400}

Syntax Description

1200	Configures the console port for 1200 baud.
2400	Configures the console port for 2400 baud.
9600	Configures the console port for 9600 baud.
19200	Configures the console port for 19200 baud.
38400	Configures the console port for 38400 baud.

Default

9600

Command Mode

System level

Example

The following example configures the console port for 2400 baud:

```
Host> set baud 2400
```

set screen

To set the maximum number of lines that will be displayed on your terminal, use the **set screen** command.

set screen *lines*

Syntax Description

lines	Maximum number of lines that will be displayed on your terminal. Must be between 2 and 128.

Default

20

Command Mode

System level

Example

The following example configures the terminal to display 30 lines at once:

```
Host> set screen 30
```

CHAPTER 3

System Management Commands

This chapter describes the commands pertaining to system interfaces, system booting, and terminal sessions.

change user

To enter profile mode or return to the system level, use the change user command.

cd [*profile-name*]

Syntax Description

profile-name	(Optional) Name of the profile. You can abbreviate the profile name to the fewest characters that make it unique—a minimum of two characters. Profile names are not case-sensitive for this command. If you do not enter this argument, the command (cd alone) takes you to the system level.

Command Mode

System level or profile mode

Usage Guidelines

Use this command at the system level or to enter the profile mode for any profile or in profile mode to return to the system level.

Example

The following example changes you from the system level to profile mode for profile 2503:

```
Host> cd 2503
Host:2503>
```

Related Commands

set user

help

To display a list of commands and their syntax, use the help command.

help [*action*] [*modifier*]

Syntax Description

action	(Optional) Can be **set** (set commands), **reset** (reset commands), **show** (show commands), **log** (log commands), **test** (test commands).
modifier	(Optional) Can be **ip** (Internet Protocol), **ipx** (Internetwork Packet Exhange), **snmp** (Simple Network Management Protocol).

Command Mode

System level or profile mode

Usage Guidelines

Use to display on-line help reference on commands.

log

To implement the routers logging functions, use the **log** command.

log [{*connection-number* | lan}] [none | calls | cause | messages [verbose] | state | error] [time]

Syntax Description

connection-number	(Optional) Enables router logging for the connection specified. If no connection is entered, the router determines the connection from the current profile.
lan	(Optional) Enables logging for the LAN connection.
none	(Optional) Disables all logging.
calls	(Optional) Logs call statistics. Each major call event is logged and message is displayed every time a channel is assigned a connection.
cause	(Optional)
messages	(Optional) Logs messages that are passed on the ISDN call control stack from the network layer up. Used primarily for troubleshooting the ISDN line.
verbose	(Optional) Modifies the action of the **messages** keyword by logging all layers of the ISDN call control stack.
states	(Optional) Logs the call start-up state and all messages received for negotiation. Also displayed are the channel and connection to which the information applies. Used to troubleshoot any negotiation problems.
errors	(Optional) Logs error messages that otherwise are not displayed, including buffer allocation errors, mail delivery errors, and chip level errors.
time	(Optional) Displays time and date of each logged event or message.

Note More than one keyword can be entered at one time.

Command Mode

System level or in profile mode

Examples

The following example shows output from the **log calls** command:

```
Host> log calls time
04/11/1994 15:41:09  L12  0                        Disconnected Remotely
04/11/1994 15:41:09  L00  0
Cause 16  Normal Disconnect
04/11/1994 15:41:09  L27  1                        Disconnected
04/11/1994 15:41:09  Connection 5 Remove  Link 1   Channel 1
04/11/1994 15:41:09  L12  0                        Disconnected Remotely
04/11/1994 15:41:09  L00  0
Cause 16  Normal Disconnect
04/11/1994 15:41:09  L27  10                       Disconnected
```

```
04/11/1994 15:41:09  Connection 5 Remove  Link 1  Channel 10
04/11/1994 15:41:09  Connection 5 Closed
04/11/1994 15:41:11  L11  20                      Call Requested
```

The following example shows output from the **log messages** command:

```
Host> log messages
>  0300 --> 0400 01 0000 0341 0005
 05 02 8f 37 90 04 02 88 90 18 03
 a9 83 83 70 08 c1 39 38 38 39
 35 33 36
Host>  0400 --> 0500 0003
 03 00 03 00 15 04 03 08 00 10 18
 03 01 03 03 70 09 04 01 39 38
 38 39 35 33 36 04 02 88 90 18
 03 a9 83 83 70 08 c1 39 38 38
 39 35 33 36
Host>  0400 --> 0300.01 0003 0340 0005
 08 02 8f 37 87
```

The following example shows output from the log messages verbose command:

```
Host> log messages verbose
Host> 0200 --> 020a 00 0000 0141 0003 02 01 01 83
Host> 020a --> 0200 01 0000 0140 0003 02 01 01 c7
Host> 0200 --> 020a 00 0000 0141 0003 02 01 01 83
Host> 020a --> 0200 01 0000 0140 0003 02 01 01 c7
Host> 0200 --> 020a 00 0000 0141 0003 02 01 01 83
Host> 020a --> 0200 01 0000 0140 0003 02 01 01 c7
Host> 0200 --> 020a 00 0000 0141 0003 02 01 01 83
Host>  L11  3                    Call Requested
Host>  L14  3                    Accepting Call
Host>  0500 --> 0400 0021
 21 00 03 00 04 18 03 01 03 03
Host>  L08  3                    Call Connected
```

The following example shows output from the **log states** command:

```
Host> log states
Host> 05/11/1994 10:04:10  L11  1                    Call Requested
Host> 05/11/1994 10:04:10  L14  1                    Accepting Call
Host> 05/11/1994 10:04:10  L08  1                    Call Connected
Host> Log States   Event: Incoming Call   Channel:  1
Log States   Event: Inband Packet   Channel:  1
  Port 1 Number =              9031600
  Port 2 Number =              9031601
  Origination Port = 1
  Protocol = 1
  Protocol List
    Protocol 0 = 1
    Protocol 1 = 2
    Protocol 2 = 3
  Password =   ****
  Ethernet = 00 40 f9 01 18 4e
  Line Integrity = 10
  IP Address = 192.216.55.205
  Remote Bridge =  DMS160
Old State: Called Start
New State: Called Wait for Complete
```

The following example shows output from the **log errors** command:

```
Host> log errors
Host> Log Errors: 1009 Wrong channel selected to forward received out of sequence data 3
Host> Log Errors: 1009 Wrong channel selected to forward received out of sequence data 4
Host> Log Errors: 1012 WAN Driver could not send data on channel 5
Host> Log Errors: 1012 WAN Driver could not send data on channel 5
Host> L1  6           Call Requested
```

Ping

Use the **ping** command to determine the reachability of a system on any connected interface.

ping [*destination ip address*]

Syntax Description

destination ip address	Specifies the ip address of the system connected to an interface on the CiscoPro CPA750.

Command Mode

System level

Usage Guidelines

If the destination can be reached, the round trip delay is determined and reported. If the destination cannot be reached, a no response message is generated.

The ping command is retried three times if the destination cannot be reached.

Example

The following example illustrates a successful ping:

```
Host> ping 172.16.2.1
start sending : round trip time is 40 msec.
```

The following example illustrates an unsucessful ping:

```
Host>ping 172.16.2.1
start sending : no response
start sending : no response
start sending : no response
```

reboot

To boot the router manually, use the **reboot** command.

reboot

Syntax Description

This command has no keywords or arguments.

Command Mode

System level

Example

The following example shows how to manually boot the router:

```
Host> reboot
```

set date

To set the current date, use the **set date** command.

set date *month/date/year*

Syntax Description

month	A two-digit number from 01 to 12.
date	A two-digit number from 01 to 31.
year	A four-digit number from 1994 to 2020.

Command Mode

System level

Usage Guidelines

You must reset the date every time the router is rebooted.

Example

The following example configures the current date in the CiscoPro CPA750 series router:

```
Host> set date 08/07/1995
```

set default

To set all variable parameters to their default values, use the **set default** command.

set default

Syntax Description

This command has no keywords or arguments.

Command Mode

System level or in profile mode

Usage Guidelines

The system deletes all parameters and their profiles that have none as a default.

Example

The following example configures the CiscoPro CPA750 series router to default values:

```
Host> set default
```

set echo

To enable and disable terminal echo of keyboard entry, use the **set echo** command.

set echo [on | off]

Syntax Description

on	Enables terminal echo.
off	Disables terminal echo.

Default

Enabled

Command Mode

System level

Example

The following example disables terminal echo for the CiscoPro CPA750 series router:

```
Host> set echo off
```

Set Encapsulation

This command sets the encapsulation method for packets that are sent over the WAN links.

set encapsulation [ppp|cpp]

Syntax Description

ppp	Sets encapsulation to point-to-point (PPP) protocol.
cpp	Sets encapsulation to Combinet Packet Protocol (CPP).

Default

cpp

Command Mode

Profile mode

Example

The following example sets encapsulation to PPP:

```
Host>set encapsulation ppp
```

set ipx trace

To convert IPX packets to hexadecimal values for troubleshooting purposes, use the **set ipx trace** command.

set ipx trace {*packet-length* | **on** | **off**}

Syntax Description

packet-length	Can be from 1 to 65,535.
on	Enables IPX packet conversion to hexadecimal numbers.
off	Disables IPX packet conversion to hexadecimal numbers.

Default

off

Command Mode

Profile mode.

Example

The following example enables ipx trace and sets packet length to 4,096:

```
Host>set ipx trace 4096 on
```

The following example disables ipx trace:

```
Host>set ipx trace off
```

set loop

To create a loop from the router towards the ISDN line, use the **set loop** command. This used with the **test** command.

set [*connection-number*] **loop {on | off}**

Syntax Description

connection-number	(Optional) Specifies a connection number on which to create a loop. If no connection number is specified, a loop is created on the connection associated with the current profile. If the router cannot determine the connection number from the profile, an error message will be displayed.
on	Enables a loop.
off	Disables a loop.

Default

Disabled

Command Mode

System level or profile mode

Usage Guidelines

Use this command at the system level with the *connection-number* argument or in profile mode. This command is used for troubleshooting purposes.

Example

The following example creates a loop on connection 14:

```
Host> set 14 loop on
```

set system

To configure the router's name that is used as the system prompt and during PPP authentication, use the **set system** command.

set system *system-name*

Syntax Description

system-name	Name used as the system prompt. The system name is case sensitive and can be from 1 to 20 characters.

Default

Standard prompt sign (>).

Command Mode

System level

Usage Guidelines

To delete the system name, enter the command without the *system-name* argument.

Example

The following example configures the CiscoPro CPA750 series router with a system name:

```
> set system Host
Host>
```

set time

To set the current time, use the **set time** command.

set time *hours*:*minutes*:*seconds*

Syntax Description

hours	A number from 1 to 23.
minutes	A two-digit number from 00 to 59.
seconds	A four-digit number from 00 to 59.

Command Mode

System level

Usage Guidelines

The time must be reset every time the router is rebooted.

Example

The following example configures the current time in the CiscoPro CPA750 series router:

```
Host> set time 8:48:20
```

show

To display the router's configuration and the status of both ISDN B channels, use the **show** command.

show

Syntax Description

This command contains no keywords or arguments.

Command Mode

System level or profile mode

Usage Guidelines

In profile mode, the **show** command displays only profile-based configurations. Parameters that have been configured at the profile level are indicated by <*>. All other values are inherited from the profile template.

Example

The following example shows output from the **show** command at the system level:

```
Host> show
System Parameters
    Environment
      Screen Length          20
      Echo Mode              ON
    Bridging Parameters
      LAN Forward Mode       ANY
      WAN Forward Mode       ONLY
      Address Age Time       OFF
    Call Startup Parameters
      Multidestination       OFF
    Line Parameters
      Switch Type            5ESS
      Numbering Plan         NORMAL
      PS1detect              OFF
    Call Parameters          Link 1            Link 2
      Retry Delay            30                30
Profile Parameters
    Bridging Parameters
      Bridging               ON
      Routed Protocols
      Learn Mode             ON
      Passthru               OFF
    Call Startup Parameters
      Encapsulation          PPP
    Line Parameters
      Line Speed             64K/Line
    Call Parameters          Link 1             Link 2
      Auto                   ON                 ON
      Called Number          5551234
      Ringback Number        5556789
Status    07/01/1995 19:49:29                  Connection Link
Line Status
 Line DeActivated
 Terminal Identifier Unassigned
```

```
 Port Status
  Ch: 1 Waiting for Call
  Ch: 2 Waiting for Call
```

The following example shows output from the **show** command in profile mode:

```
Host:2503> show

Profile Parameters
    Bridging Parameters
      Bridging                OFF<*>
      Routed Protocols        IP IPX <*>
      Learn Mode              ON
      Passthru                OFF
    Call Startup Parameters
      Encapsulation           PPP
    Line Parameters
      Line Speed              64K/Line
    Call Parameters           Link 1              Link 2
      Auto                    ON                  ON
      Called Number           5551111<*>          5551111<*>
      Ringback Number    814155554321<*>          814155554321<*>

Status      01/01/1995 19:52:14                   Connection Link
Line Status
  Line DeActivated
  Terminal Identifier Unassigned
Port Status
  Ch: 1 Waiting for Call
```

show config

To display a subset of the current configuration parameters, use the **show config** command.

show config [all]

Syntax Description

all	(Optional) Use this keyword in profile mode to display system configurations in addition to profile configurations (the same display shown at the system level).

Command Mode

System level or profile mode

Usage Guidelines

In profile mode, the show config command displays only profile-based configurations. Parameters that have been configured at the profile level are indicated by <*>. All other values are inherited from the profile template.

Examples

The following example shows output from the **show config** command at the system level:

```
Host> show config

System Parameters
    Environment
      Screen Length          20
      Echo Mode              ON
    Bridging Parameters
      LAN Forward Mode       ANY
      WAN Forward Mode       ONLY
      Address Age Time       OFF
    Call Startup Parameters
      Multidestination       OFF
    Line Parameters
      Switch Type            5ESS
      Numbering Plan         NORMAL
      PS1detect              OFF
    Call Parameters          Link 1              Link 2
      Retry Delay            30                  30

Profile Parameters
    Bridging Parameters
      Bridging               ON
      Routed Protocols
      Learn Mode             ON
      Passthru               OFF
    Call Startup Parameters
      Encapsulation          PPP
    Line Parameters
      Line Speed             64K/Line
    Call Parameters          Link 1               Link 2
      Auto                   ON                   ON
      Called Number
      Ringback Number
```

show connection

To display all current connections, use the **show connection** command.

show connection

Syntax Description

This command has no keywords or arguments.

Command Mode

System level

Example

Following is sample output from the **show connection** command:

```
Host> show connection
Connections       10/30/1995 16:45:26
    Start Date & Time   # Name          # IP              # Ethernet
  1 10/30/1995 16:32:07 # Engin         # 198.95.216.74    # 00 00 0c 00 56 b2
  2 10/30/1995 16:33:00 # Engin         # 198.95.216.75    # 00 00 0c 00 54 c2
           Link: 1   Channel: 1 Phone: 9018
```

Table 3-1 describes the fields shown in the display.

Table 3-1 Show Connection Field Descriptions

Field	Description
Connection	Connection number assigned by the router.
Start Date	Call start date.
Start Time	Call start time.
Name	System ID of remote router.
IP	IP address of remote router.
Ethernet	Ethernet address of remote router.

show demand

To display demand and timeout configurations, use the **show demand** command.

show demand

Syntax Description

This command has no keywords or arguments.

Command Mode

System level or profile mode

Usage Guidelines

In profile mode, the **show demand** command displays only profile-based configurations. Parameters that have been configured at the profile level are indicated by <*>. All other values are inherited from the profile template.

The following example shows output from the **show demand** command at the system level:

```
Host> show demand
Demand Calling Parameters          Link 1        Link 2
  Connection Type                  Auto ON       Auto ON
  Threshold                        0 kbs         48 kbs
  Duration                         1 sec         1 sec
  Source                           LAN           BOTH
Timeout (call tear down) Parameters
  Threshold                        0 kbs         48 kbs
  Duration                         OFF           OFF
  Source                           LAN           BOTH
```

Related Commands

demand
set timeout
timeout

show packets

To display packet count statistics, use the **show packets** command.

show [*connection-number* | *lan*] **packets**

Syntax Description

connection-number	(Optional) Displays packet statistics for the connection number indicated. If no connection number is entered, statistics for the current profile are displayed.
lan	(Optional) Displays packet statistics for the LAN connection.

Command Mode

System level or profile mode.

Example

The following example shows output from the **show packets** command for a specified connection:

```
Host> show 14 packets
Packet Statistics for Connection 14
Filtered: 11013246  Forwarded: 8400  Received: 5993
Dropped: 263  Lost: 0  Corrupted: 0  Misordered: 1
Compression Ratio:  1.73:1
```

The following example shows output from the **show packets** command for the LAN connection:

```
Host> show lan packets
Packet Statistics for LAN
Filtered: 11001795  Forwarded: 12411637  Received: 25496880
Dropped: 0  Lost: 6911  Corrupted: 46  Misordered: 0
Ethernet Type: 0806 Count: 3375
Ethernet Type: 0800 Count: 979
Ethernet Type: 80f3 Count: 1068
Ethernet Type: 809b Count: 48718
```

Table 3-2 Show Packets Field Descriptions

Field	Description
Filtered	Total of packets received
Forwarded	Packets received from the Ethernet and forwarded onto the ISDN line.
Received	Packets received from the ISDN line.
Dropped	Packets received from the Ethernet and dropped because the queue of packets to be forwarded was too long.
Lost	Packets received from the ISDN line but not successfully transmitted on the Ethernet (usually due to a faulty Ethernet).
Corrupted	Packets received from the ISDN line with a bad checksum (CRC) that were discarded as corrupted.

Field	Description
Misordered	Packet received out of sequence when using ordered protocol.
Ethernet Type	Packet types received.
Count	Number of packets of this type received.

show users

To display all profiles and their status, use the **show users** command.

show users

Syntax Description

This command has no keywords or arguments.

Command Mode

System level

Example

The following example shows output from the **show users** command:

```
Host> show users

User        State       Connection
--------------------------------
LAN         Active      LAN
Internal    Active      BRIDGE
Standard    Active      4
2503        Active      5
```

Table 3-3 describes the fields shown in the display.

Table 3-3 Show Users Field Descriptions

Field	Description
User	Name of profile.
State	Active or Inactive.
Connection	Name or number of connection assigned to the profile.

software load

To download new software through the configuration port or across a TCP/IP network using TFTP, use the **software load** command.

swl [tftp]

Syntax Description

tftp (Optional) Use when loading software across a TCP/IP network using TFTP.

Command Mode

System level

Example

Following is an example of the **software load** command.

Note You will need terminal emulation software to load new software.

To load software with the **software load** command, take the follwoing steps:

Step 1 Connect the serial cable from your terminal to the configuration port on the CiscoPro CPA750 series router.

Step 2 On the terminal emulation software, set the baud rate to 9600.

Step 3 Power on the CiscoPro CPA750 series router.

Step 4 In the terminal emulation software, enter the **software load** command:

```
Host> swl
```

Step 5 Enter y in response to the prompt:

```
Are you sure? y
```

Step 6 At the prompt, enter one of the load rates listed, and make sure that the load rate you choose (See Table 3-4 for approximate software load times according to baud rate) is supported by your terminal emulation software:

Note Do not press the Return key after entering the number.

```
Ready to upload new firmware into flash.

Baud (1=19.2K, 2=2400, 3=38.4K, 9=9600)? 9
```

Step 7 Change the baud rate of the terminal emulation software to the rate indicated in Table 3-4.

Step 8 From the terminal, load the file containing the new software by following the prompts from your terminal emulation program. The LINE LED should blink throughout the loading process.

Step 9 When the software has been downloaded, you will be prompted to change the terminal emulator's baud rate back to 9600, and then you will be prompted to press any key.

If the load is successful, the LINE LED will turn off, and the RDY LED should be on. If the load was not successful, refer to Table 3-5 for possible symptoms and solutions.

Table 3-4 Approximate Software Load Time

Load Rate (Baud)	Approximate Time (Minutes)
2400	48
9600	12
19200	6
38400	3

Table 3-5 Software Load Command Troubleshooting

Symptom	Probable Cause/Solution
Load takes significantly longer than the approximate time listed in Table 3-4.	The terminal emulation program's interline and intercharacter delays are not set to zero.
The terminal displays unrecognizable text after the load is completed.	The terminal has not been reset to 9600 baud. Reset the terminal anytime after loading the new software. After changing the terminal baud rate, press Return to gain access to the standard prompt (>).
Two or more LEDs are blinking.	Incorrect configuration of the PC's COM port or a defective console cable. Press Escape on the terminal and try the software load again.

The following is an example of the **software load tftp** command:

Before beginning this procedure, you should configure your workstation to operate as a TFTP server. In server mode, the workstation will only accept **put** requests for the file.

Step 1 Confirm that the new software and, optionally, the new configuration file are installed on the client machine.

Step 2 Confirm that the CiscoPro CPA750 series router can be reached from the client machine by pinging the CiscoPro CPA750 series router:

```
Host> ping ip address
```

Step 3 Enter the **login** command to log into the CiscoPro CPA750 series router:

```
Host> login
```

Note If local access has been restricted with the **set local access** command, you will be required to enter the system password before being allowed to log into the router.

Caution Once the **software load tftp** command is entered, the existing software is erased. If a catastrophic event, such as a power failure, occurs before the transfer of the CODE file has been completed, the CiscoPro CPA750 series router must be initialized through the configuration port.

Step 4 Enter the software load command to configure the CiscoPro CPA750 series router for TFTP server mode:

```
Host> swl tftp
  Are you sure? yes
  Erasing Flash memory, please standby...
  Ready for software load.
```

Note Entering the **software load tftp** command on the CiscoPro CPA750 series router causes it to enter TFTP server mode and wait for client requests. The TFTP server mode will timeout in one minute.

Step 5 On the client machine, enter TFTP client mode, using the CiscoPro CPA750 series router's IP address:

```
Client> tftp ip address
```

Step 6 On the client machine, select binary file transfer mode:

```
Client> binary
```

Step 7 On the client machine, enter the **put code** command to transfer the new software file to the CiscoPro CPA750 series router:

```
Client> put file-name code
```

If the transfer is successful, the CiscoPro CPA750 series router will reboot with the new software and the new configuration (if a new configuration file was loaded).

test

To generate test packets, use the **test** command.

test {*connection-number* | **wan** | **ether** | **all**} [**stop**] [**result**] [**rate** *speed*] [**min** *packet-size*] [**max** *packet-size*]

Syntax Description

connection-number	Number of the connections where test packets will be generated.
wan	Generates test packets on the ISDN line. Packets should be sent to a remote router that has a loop enabled with the **set loop** command. Compare number of sent packets to number of received packets.
ether	Generates test packets on the LAN and compares number of sent packets to number of received packets.
all	Generates test packets on both the ISDN line and on the LAN.
stop	(Optional) Stops all test packets from being generated.
result	(Optional) Displays results of last completed test.
rate *speed*	(Optional) Rate in packets per second at which test packets are generated. Default value is 10. Can be between 1 and 100.
min *packet-size*	(Optional) Minimum size in bytes of test packets. Default value is 60. Can be between 60 and 1514. Packets are generated in geometrically larger sizes, starting with the minimum size and ending with the maximum size. After the maximum length is reached, the next packet is the minimum size.
max *packet-size*	(Optional) Maximum size in bytes of test packets. Default value is 1514. Can be between 60 and 1514.

Command Mode

System level

Usage Guidelines

This command is useful for troubleshooting purposes.

Example

The following example enables a test on the ISDN line and the Ethernet with a minimum packet size of 255 bytes and a maximum packet size of 1024 bytes:

```
Host>test all min 255 max 1024
```

upload

To send a set of ASCII strings containing the current configuration to the terminal, use the **upload** command.

upload

Syntax Description

This command has no keywords or arguments.

Command Mode

System level

Usage Guidelines

You can use the captured file to reconfigure the router after loading new software or to configure multiple routers with the same parameters.

When downloading the file, set the ASCII download for 1 second so that each line will be correctly processed.

Note Use the **set echo off** command to prevent the **upload** command from being captured in the file.

Example

The following example shows the upload command and the following output:

```
Host> upload
CD
SET SCREENLENGTH 20
SET LAN MODE ANY
SET WAN MODE ONLY
SET AGE OFF
SET MULTIDESTINATION OFF
SET SWITCH 5ESS
SET PLAN NORMAL
SET 1 DELAY 30
SET 2 DELAY 30
SET BRIDGING ON
SET PASSTHRU OFF
SET ENCAPSULATION CPP
SET SPEED AUTO
SET 1 AUTO ON
SET 2 AUTO ON
SET 1 NUMBER
SET 2 NUMBER
SET 1 RINGBACK
SET 2 RINGBACK
LOG CALLS TIME VERBOSE
SET UNICASTFILTER OFF
DEMAND 1 THRESHOLD 0
DEMAND 2 THRESHOLD 48
DEMAND 1 DURATION 1
DEMAND 2 DURATION 1
```

```
DEMAND 1 SOURCE LAN
DEMAND 2 SOURCE BOTH
TIMEOUT 1 THRESHOLD 0
TIMEOUT 2 THRESHOLD 48
TIMEOUT 1 DURATION 0
TIMEOUT 2 DURATION 0
TIMEOUT 1 SOURCE LAN
TIMEOUT 2 SOURCE BOTH
SET UNICASTFILTER OFF
SET REMOTEACCESS PROTECTED
SET LOCALACCESS ON
SET CALLERID OFF
SET PPP AUTHENTICATION IN CHAP
SET CALLBACK OFF
SET CALLBACKID OFF
SET PPP AUTHENTICATION OUT CHAP
SET CPP NEGOTIATION INTEGRITY   10
SET CPP NEGOTIATION ABORT DISCONNECT
SET CPP NEGOTIATION COUNT   6
SET CPP NEGOTIATION RETRY   1000
SET PPP NEGOTIATION INTEGRITY 10
SET PPP NEGOTIATION COUNT 10
SET PPP NEGOTIATION RETRY  3000
SET PPP TERMREQ COUNT 2
SET PPP MULTILINK ON
SET CPP PROTOCOL   ORDERED
SET CPP COMPRESSION STAC
SET SNMP CONTACT
SET SNMP LOCATION
SET SNMP TRAP COLDSTART OFF
SET SNMP TRAP WARMSTART OFF
SET SNMP TRAP LINKDOWN OFF
SET SNMP TRAP LINKUP OFF
SET SNMP TRAP AUTHENTICATIONFAIL OFF
SET USER LAN
SET USER Internal
SET USER Standard
SET PROFILE POWERUP ACTIVATE
SET PROFILE DISCONNECT KEEP
```

Related Commands

set echo

version

To display the software release level and date, use the **version** command.

version

Syntax Description

This command has no keywords or arguments.

Command Mode

System level or profile mode

Example

The following example shows output from the version command:

```
Host> version
Software Version WBE3.0 - Oct 30 1995 09:00:46
ISDN Stack Revision US 2.00 (5ESS/DMS/NI-1)
```

CHAPTER 4

Profile Commands

This chapter describes the commands used to create and configure user profiles.

reset packets

To set accumulated packets counts to zero for one connection, use the **reset packets** command.

reset [lan] packets

Syntax Description

lan (Optional) Sets accumulated packets counts to zero on the LAN connection.

Command Mode

Profile mode

Example

The following example resets the packets counts for profile 2503:

```
Host:2503> reset packets
```

Related Commands

show packets

reset user

To delete a profile, use the **reset user** command.

reset user *profile-name*

Syntax Description

profile-name	Name of the profile to be deleted.

Command Mode

Profile mode or system level

Usage Guidelines

After you perform this command, you will be at the system level.

Example

The following steps delete profile 2503:

Step 1 Enter the **reset user** command:

```
Host:2503> reset user 2503
```

Step 2 Enter **y** in response to the prompt:

```
Are you sure> y
```

If you do not want to delete the profile, press Return in response to the prompt:

```
Host:2503>
```

Related Commands

set user

set active

To set a profile to either active or inactive, use the **set active** command.

set {active | inactive} *profile-name*

Syntax Description

active	Creates a virtual connection to the remote router associated with this profile. Incoming packets from the LAN causes a call to be made to the remote router (if on-demand dialing is enabled with the **set auto** command). Incoming calls from the remote router associated with the profile use the profile's configurations.
inactive	Closes all virtual and physical connections to the remote router. Any calls in process will be disconnected. Outgoing packets destined for the remote router associated with this profile will be ignored. Incoming packets from the remote router cause the profile to be active for the duration of the command. Depending on how the profile has been configured with the **set profile** command, the profile either is inactive or remains active once the physical connection is disconnected.
profile-name	Profile name.

Default

active

Command Mode

System level or profile mode

Useage Guidelines

Newly created profiles are inactive until activated, or until a reboot is performed.

Example

The following example configures profile 2503 to be inactive and closes its connection:

```
Host> set 2503 inactive

Connection 2 Closed
```

Related Commands

set auto
set user

set profile

To configure profile activity status after power on and call disconnect, use the **set profile** command:

set profile [power {active | inactive}] [disconnect {deactivate | keep}]

Syntax Description

power	(Optional) Router power on.
active	Profile becomes active when router is powered on. Incoming packets from the LAN causes a call to be made to the remote router (if on-demand dialing is enabled with the **set auto** command). Incoming calls from the remote router associated with the profile use the profile's configurations.
inactive	Profile is inactive when router is powered on. Outgoing packets destined for the remote router associated with this profile are ignored. Incoming packets from the remote router cause the profile to be active for the duration of the command. Depending on how the profile has been configured with the **set profile** command, the profile either is deactived or remains active once the physical connection has been disconnected.
disconnect	(Optional) Connection is terminated.
deactivate	Profile becomes inactive when its associated connection is disconnected.
keep	Profile remains active when its associated connection is disconnected.

Default

power active
disconnect keep

Command Mode

Profile mode

Example

The following example configures the profile 2503 to be inactive after the unit powers up and inactive after any physical link to the remote router is disconnected:

```
Host:2503> set profile power inactive disconnect deactivate
```

set profile id

To associate the Ethernet address of a remote router with a profile, use the **set profile id** command.

set profile id *ethernet-address*

Syntax Description

ethernet-address	Ethernet address of the remote router that is associated with the profile. Every profile using Combinet Packet Protocol (CPP) must have an Ethernet address entered with this command. When it receives a call, the CiscoPro CPA750 series router uses the Ethernet address of the remote router to locate the correct profile to be used with the remote router.

Default

No Ethernet address configured.

Command Mode

Profile mode for the profile you are configuring.

Example

The following example configures the profile 2503 with the Ethernet address of the remote router:

```
Host:2503> set profile id 00000c0012ff
```

set user

To create a new profile or modify an existing profile, use the **set user** command.

set user *profile-name* **[incoming | outgoing]**

Syntax Description

profile-name	Name of profile. A profile name can be 1 to 8 characters. Names are case sensitive only when being displayed.
incoming	(Optional) Profile will apply only to incoming calls. Incoming profiles have the following default values: • power inactive (change with **set profile** command) • disconnect deactivate (change with **set profile** command) • on-demand dialing off (change with **set auto** command) If this keyword is not specified, the profile applies to both incoming and outgoing calls.
outgoing	(Optional) Profile will apply only to outgoing calls. Outgoing profiles have the following default values: • power active (change with **set profile** command) • disconnect keep (change with **set profile** command) • on-demand dialing on (change with **set auto** command) If not specified, profile applies to both incoming and outgoing calls.

Default

outgoing

Command Mode

System level or profile mode

Examples

The following example configures a new profile, 2503:

```
Host> set user 2503 outgoing
```

The following example changes an outgoing profile to apply only to incoming calls:

```
Host> set user 2503 incoming
```

Related Commands

set auto
set profile

show profile

To display the Ethernet address and activity status of the current profile, use the **show profile** command.

show profile

Syntax Description

This command has no keywords or arguments.

Command Mode

Profile mode

Example

The following example shows output from the **show profile** command for profile 2503:

```
Host:2503> show profile

Profile for user 2503<*>
    Ethernet Address 00 00 0c ff ff ff<*>
    Power Up         ACTIVATE<*>
    Disconnect       KEEP<*>
```

Table 4-1 describes the fields shown in the display.

Table 4-1 Show Profile Field Descriptions

Field	Description
Ethernet Address	Ethernet address of the remote router associated with the profile. Configured with the **set profile id** command.
Powerup	Indicates whether the profile is active when the router is powered on. Configured with the **set active** command
Disconnect	Indicates whether the profile remains active after a physical connection to the remote router has been terminated. Configured with the **set active** command.
<*>	Indicates that the values shown apply to this profile only.

unset

To return profile-configured parameters to the profile template value, use the **unset** command.

unset *command-modifier*

Syntax Description

command-modifier Original command modifier used to configure the parameter. Refer to Table 4-2 for a complete list of all **unset** commands with the original command modifier.

Command Mode

Profile mode

Table 4-2 Unset Command Syntax Descriptions

Original Command	Unset Command Syntax
demand	**unset** *channel*[1] **demand**
set auto	**unset** *channel* **auto**
set billing spc	**unset billing**
set bridging	**unset bridging**
set callback	**unset callback**
set callbackid	**unset callbackid**
set callerid	**unset callerid**
set compression	**unset compression**
set encapsulation	**unset encapsulation**
set learn	**unset learn**
set number	**unset** *channel* **number**
set passthru	**unset passthru**
set password client	**unset password client**
set ppp authentication	**unset ppp authentication**
set ppp password host	**unset ppp password host**
set ppp secret host	**unset ppp secret host**
set protocol	**unset protocol**
set ringback	**unset** *channel* **ringback**
set speed	**unset speed**
set timeout	**unset** *channel* **timeout**

1. The channel argument can be 1 or 2.

Example

The following example returns the profile 2503's PPP client password to the profile template value:

```
Host:2503> unset ppp client password
```

CHAPTER 5

Security Commands

This chapter describes the commands used to configure router security.

login

To log in to a remote router to make configuration changes, use the **login** command.

login [*ip-address* | *ethernet-address* | *connection-number* | **remote**]

Syntax Description

login	Used without an argument or keyword, this command enables you to log in to a router that is directly connected to your terminal through the console port. If access to the router has been restricted with the **set local access** command, you will be required to enter the router's system password before making any configuration changes.
ip-address	(Optional) Enables you to log in to a router on the same IP network or to a remote router connected across the ISDN line. The IP address must be in four-part dotted decimal format. If access to the router has been restricted with the **set remote access** command, you will be required to enter the router's system password before making any configuration changes.
ethernet-address	(Optional) Used with bridging. Enables you to log in to a router on the same Ethernet segment or to a remote router connected across the ISDN line. The Ethernet address must be entered as 12 contiguous hexadecimal characters with no spaces. If access to the router has been restricted with the **set remote access** command, you will be required to enter the router's system password before making any configuration changes.
connection-number	(Optional) Used with Combinet Packet Protocol (CPP). Enables you to log in to a router that is connected across the ISDN line. The connection numberr must be the number assigned by the router to the connection. If access to the router has been restricted with the **set remote access** command, you will be required to enter the router's system password before making any configuration changes.
remote	(Optional) Used with Combinet Packet Protocol (CPP). Enables you to log in to a router connected across the ISDN line. This keyword should be used while in profile mode.

Command Mode

None

Usage Guidelines

You can only log in to a remote router that is directly connected to your terminal or that has an active ISDN or Ethernet connection to your local router. After five minutes of no activity, you will be logged out of the remote router. Use the **logout** command to manually log out of the remote router.

Example

The following example enables you to log in to a remote router across the ISDN connection using the remote router's IP address:

```
Host> login 150.150.50.25
```

Related Commands

logout
set local access
set remote access

logout

To end any remote session initiated by the **login** command, use the **logout** command.

logout

Syntax Description

This command does not contain any keywords or arguments.

Command Mode

System level or in profile mode

Example

The following example ends a remote session initiated with the login command:

```
Host> logout
```

Related Commands

login

reset password

To delete one or all of the host passwords, use the reset password command.

reset password [all]

Syntax Description

all	(Optional) Deletes all host passwords.

Command Mode

System level

Usage Guidelines

This command does not delete client or system passwords. See the following section, "Examples," for the procedure to change these passwords.

Examples

The following example deletes a single host password:

Step 1 Enter the **reset password** command:

```
Host> reset password
```

Step 2 At the prompt, enter the host password that you want deleted. The password will not be echoed on the terminal:

```
Enter new Password: <host-password>
```

You have deleted one host password.

The following example deletes or changes client and system passwords:

Step 1 Enter the **set password** command with the correct keyword (either **client** or **system**):

```
Host> set password client
```

Step 2 To delete the password, press Return in response to the prompt. To change the password, enter the new password in response to the prompt. The password will not be echoed on the terminal.

```
Enter new Password: <new-password>
```

Step 3 If you entered a new password, you will be prompted to reenter it for confirmation:

```
Re-Type new Password: <new-password>
```

set local access

To restrict commands that can be entered at the local configuration port, use the **set local access** command.

set local {on | partial | protected}

Syntax Description

on	Sets commands to be performed without restriction.
partial	Sets commands to be performed with partial restrictions.
protected	Sets commands to be performed with system password only.

See Table 5-1 for a summary of each keyword's security level.

Default

on—enabled for all commands

Command Mode

System level

Example

The following example configures local configuration access to protected:

```
Host> set local protected
```

Table 5-1 describes how configuration through the local configuration port is affected by the **set local access** command.

Table 5-1 Set Local Access Command Settings

Commands	On	Partial	Protected
call	See Note[1]		P[2]
demand		P	P
disconnect			P
help			P
log commands			P
login			
logout			
reboot			P
reset commands		P	P
set commands		P	P
show commands			P
software load		P	P
test commands			P

Commands	On	Partial	Protected
timeout		P	P
unset commands		P	P
upload			P
version			P

1. Note: An empty cell indicates that the command can be performed remotely without restrictions.
2. P indicates that a system password must be entered before performing the `set local` command at the local configuration port.

Related Commands

set password

set remote access

To restrict remote configuration access to the router, use the **set remote access** command.

set remote {partial | protected | off}

Syntax Description

partial	Sets commands to be performed without restriction.
protected	Sets commands to be performed with partial restrictions.
off	Sets commands to be performed with system password only.

See Table 5-2 for a summary of each keyword's security level.

Default

off

Command Mode

System level.

Example

The following example configures the router for protected remote access:

```
Host> set remote access protected
```

Table 5-2 describes how remote configuration is affected by the **set remote access** command.

Table 5-2 Set Remote Access Command Settings

Commands	Partial	Protected	Off
call	See Note[1]	P[2]	X[3]
demand	P	P	X
disconnect		P	X
help		P	X
log commands		P	X
login			X
logout			X
reboot		P	X
reset commands	P	P	X
set commands	P	P	X
show commands		P	X
software load	P	P	X
test commands		P	X
timeout	P	P	X

Commands	Partial	Protected	Off
unset commands	P	P	X
upload		P	X
version		P	X

1. Note: An empty cell indicates that the command can be performed remotely without restrictions.
2. P indicates that a system password must be entered before this command can be performed remotely.
3. X indicates that this command cannot be performed remotely.

Related Commands

set password

set password

To set the password, use the set passward command.

set password {system | client | host}

Syntax Description

system Configures the system password that is used to authenticate users requesting a local or remote configuration session. The system keyword can consist of a combination of 1 to 7 characters. The CiscoPro CPA750 series router can have one system password. This keyword should be used at the system level only.

client Configures the client password that is sent by the router when making an ISDN connection. The remote router compares the CiscoPro CPA750 series router's client password to its list of host passwords to authenticate the call.
The client keyword can consist of a combination of 1 to 7 characters. The CiscoPro CPA750 series router can be configured with one client password per profile. This keyword should be used while in profile mode.

host Configures the host password that is used to authenticate remote ISDN calls. The CiscoPro CPA750 series router compares its list of host passwords to the remote router's client password to authenticate the call.
The host keyword can consist of a combination of 1 to 7 characters. The CiscoPro CPA750 series router can be configured with multiple host passwords. This keyword should be used while in profile mode. Any host password configured at the system level is inherited by all user-created profiles.

Default

No passwords are configured.

Command Mode

System level

Usage Guidelines

The **set password** command should be preceded with the **set remote access** command. After entering the command you will be prompted to enter the password. When configuring a host password, you will also be prompted for a user name to associate with the password. This user name can consist of a combination of 1 to 7 characters.

To delete or change passwords, use the **reset password** command.

Example

The following example configures a host password for profile 2503:

Step 1 Enter the set password host command:

```
Host:2503> set password host
```

Step 2 At the prompt, enter your host password. Your password will not be echoed on the screen:

```
Enter new Password: <password>
```

Step 3 At the prompt, reenter your host password again for confirmation:

```
Re-Type new Password: <password>
```

Step 4 At the prompt, enter the user name you wish to associate with the host password:

```
Enter User Name: JohnDoe
```

Related Commands

reset password

show security

To display the router's security configurations, use the **show security** command.

show security [all]

Syntax Description

all	(Optional) In profile mode, displays all security configurations. This keyword has no effect when used in the profile mode.

Usage Guidelines

Use this command at the system level with the **all** keyword to display all security configurations. Use this command while in profile mode to display the security configurations for that profile.

Example

The following example shows output from the **show security** command at the system level:

```
Host> show security
System Parameters
    Security
      Access Status              ON
      System Password            EXISTS
      Remote Configuration       PROTECTED
      Local Configuration        PROTECTED
      Caller ID Security         OFF
      Caller Id Numbers

    PPP Security
      PPP Authentication    IN   CHAP
      PAP Client Password        EXISTS
      CHAP Client Secret         EXISTS

Profile Parameters
    Callback                  ON
    CPP Security
      Client Password            EXISTS
      Callback ID Security       OFF
      Callback Numbers
      Number of Host Passwords 3
      Host Passwords         User          Password
                             JohnDoe       *
                             Engin         *
                             Home          *

    PPP Security
      PPP Authentication   OUT   PAP
      PAP Host Password          EXISTS
      CHAP Host Secret           EXISTS
```

Table 5-3 list the significant fields shown in the display.

Table 5-3 Show Security Field Descriptions

Field	Description
System Parameters	Security configurations that apply to the system level.
Access Status	Indicates if remote access is enabled. Can be On or Off.
System Password	Indicates if a system password has been entered with the **set password** command. Can be *none* or *exists*.
Remote Configuration	Remote access restriction as configured with the **set remote access** command.
Local Configuration	Local configuration restriction as configured with the **set local access** command.
Caller ID Security	Indicates if Caller ID is enabled. Can be On or Off.
Caller ID Number	The phone numbers entered with the **set caller id receive number** command.
PPP Authentication	The PPP authentication method used for incoming calls. Can be PAP, CHAP, *none*, or any combination of these three. Set with the **set ppp authentication** command.
PAP Client Password	Indicates if a PAP client password has been entered with the **set ppp password** command. Can be *none* or *exists*.
CHAP Client Secret	Indicates if a CHAP client secret has been entered with the **set ppp password** command. Can be *none* or *exists*.
Profile Parameters	Security configurations that apply to the profile. If you are using the **show security** command at the system level, these configurations make up the profile template for security parameters.
Client Password	Indicates if a client password has been configured with the **set password** command. Can be *none* or *exists*.
Callback	Indicates if callback is enabled. Can be On or Off.
Callback ID Security	Indicates if callback authentication is enabled. Can be On or Off.
Callback Numbers	Numbers entered with the **set callback id receive number** command.
Number of Host Passwords	Number of host passwords that have been entered with the **set password** command.
Host Passwords	Lists the user name. An asterisk (*) indicates that a password exists for the user.
PPP Authentication	PPP authentication method used for outgoing calls. Can be PAP, CHAP, *none*, or any combination of these three. Set with the **set ppp authentication** command.
PAP Host Password	Indicates if a PAP host password has been entered with the **set ppp password** command. Can be *none* or *exists*.
CHAP Host Secret	Indicates if a CHAP host secret has been entered with the **set ppp password** command. Can be *none* or *exists*.

CHAPTER 6

Ethernet Interface Commands

This chapter describes the commands used to configure the Ethernet interface.

reset address

To delete one or all of the manually entered Ethernet addresses stored in the filtering table with the **set address** command, use the **reset address** command.

reset address {*ethernet-address* | **all**}

Syntax Description

ethernet-address	Deletes an Ethernet address that has been previously entered with the **set address** command. Must be entered as 12 contiguous hexadecimal characters (no spaces).
all	Deletes all Ethernet addresses that have been entered with the **set address** command.

Command Mode

Profile mode

Example

The following example deletes one static address from the profile 2503:

```
Host:2503> reset address 00000c00755d
```

Related Commands

set address

set address

To add an Ethernet address to a profile's static address table, use the **set address** command.

set address *ethernet-address*

Syntax Description

ethernet-address Adds the specified Ethernet address to the profile's static address table. Must be entered as 12 contiguous hexadecimal characters (no spaces). The Ethernet address cannot exist on the same network as the router. A maximum of four addresses per profile can be entered with this command.

Static addresses are associated with the profile's connection. Packets received from the LAN or ISDN line that contains a static address as a destination address will be forwarded to the connection of the profile containing that static address.

Default

No static addresses are configured.

Command Mode

Profile mode

Usage Guidelines

To delete an address entered with this command, use the reset address command. The CiscoPro CPA750 series router can store up to four Ethernet address in a combination of learned and static addresses.

Example

The following example adds a static Ethernet address to the profile 2503:

```
Host:2503> set address 00000c1235ff
```

Related Commands

reset address

Note Static addresses are stored in nonvolatile memory (NVRAM). When there is no more NVRAM available, a warning will be displayed. A static address is entered after this warning has been displayed will be stored in RAM and lost when the router is powered down.

---

set age

To specify the maximum amount of time that a learned Ethernet address will remain in the address table, use the **set age** command.

set age {*time* | **off**}

Syntax Description

time	The amount of time in seconds that any inactive learned Ethernet address will remain in the address table. Must be be between 1 and 1,000,000. When the router receives a packet with a source address matching a learned address, the age time for that address is reset to 0.
off	Learned Ethernet addresses will remain in the address table indefinitely.

Default

off

Command Mode

System level

Example

The following example configures the router to delete learned Ethernet addresses after 1 hour of no activity from the address:

```
Host> set age 3600
```

show address

To display information about the router's system and profile address configurations, use the **show address** command.

show address

Syntax Description

This command contains no arguments or keywords.

Command Mode

System level or profile mode

Examples

The following example shows the output of the **show address** command at the system level:

```
Host> show address

 INT 00 40 f9 02 c3 4c  Static
   2 00 40 f9 00 56 b2  Age: 0
 LAN 08 02 17 01 12 28  Age: 1
Number of Ethernet Addresses: 3
IP Address: 149.7.8.5
Ethernet Address: 00 40 f9 02 c3 4c
Subnet Mask: 255.255.0.0
Default Gateway: 0.0.0.0
```

Table 6-1 describes the fields shown in the display.

Table 6-1 Show Address Field Descriptions—System Level

Field	Description
INT	IP address of the internal profile
Any number	IP address of active connections.
LAN	IP address of the LAN profile.
Number of Ethernet addresses	The number of Ethernet addresses associated with the system level.
IP Address	IP address of the system level.
Ethernet Address	Ethernet address of the router.
Subnet Mask	Subnet mask of the system level.
Default Gateway	Default gateway of the system level.

The following example shows the output of the **show address** command for the profile 2503:

```
Host:2503> show address

   2 00 40 f9 ff ff ff  Static
   2 00 40 f9 12 34 56  Static
Number of Ethernet Addresses: 2
Ethernet Address: 00 40 f9 00 5b 18
```

Table 6-2 describes the fields shown in the display.

Table 6-2 Show Address Field Descriptions—Profile Mode

Field	Description
ip-address	Static and learned Ethernet addresses associated with the profile.
Number of Ethernet addresses	The number of Ethernet addresses associated with the profile.
Ethernet Address	Ethernet address of the router.

CHAPTER 7

ISDN Commands

This chapter describes the commands used to configure ISDN calling, such as on-demand dialing and security.

call

To make a manual ISDN call, use the **call** command.

call [*channel*] [*phone-number*]

Syntax Description

channel	(Optional) ISDN B channel can be either CH1 or CH2. If no channel is entered, the call is made on both channels.
phone-number	(Optional) The telephone number of the remote ISDN device. If no telephone number is entered, the router will call the number configured in the current profile with the **set number** command. If no number is entered and the current profile has not been configured with a number, this command has no effect.

Command Mode

Profile mode

Example

The following example makes a manual call on the second channel to 408- 555-1212 while in profile mode for profile 2503:

```
Host:2503> call 2 4085551212
```

Related Commands

set number

demand

To specify when an on-demand ISDN call will be made, use the **demand** command.

demand *channel* **[threshold** *data-rate***] [duration** *time***] [source {wan | lan | both}]**

Syntax Description

channel	ISDN B channel to which the demand parameters apply. Can be set to 1 or 2. If no channel is entered, the demand parameters apply to both channels.
threshold *data-rate*	(Optional) Minimum data rate (in kbps) that must exist on the channel before the call will be made. The range is 0 to 128. Inband negotiation traffic (traffic that terminates at the router) is not taken into account for the threshold level.
duration *time*	(Optional) Length of time (in seconds) that the traffic is to be above the data threshold before the call is made. The range is 1 to 255.
source	(Optional) Source of traffic that is counted.
lan	Traffic received from the LAN.
wan	Traffic received from the ISDN line.
both	The value of LAN or the ISDN traffic, whichever is higher.

Default

Channel 1—**threshold** 0 **duration** 1 **source lan**
Channel 2—**threshold** 48 **duration** 1 **source both**

Command Mode

System level or profile mode

Usage Guidelines

On-demand dialing must be enabled with the **set auto** command for this command to work.

Example

The following example determines when on-demand dialing will take place for profile 2503's connection:

```
Host:2503> demand 1 threshold 10 duration 2 source lan
```

Related Commands

set auto

disconnect

To manually terminate an ISDN call, use the **disconnect** command.

disconnect [*channel*]

Syntax Description

channel (Optional) ISDN B channel. Can be either 1 or 2. If no channel is entered, any connected calls are terminated.

Command Mode

Profile mode

Usage Guidelines

If the channel argument is used, the router will use the current profile to determine the connection number. However if the profile is in use, the command will disconnect both channels.

Example

The following example disconnects a call on the first channel:

```
Host> disconnect 1
```

The following example disconnects any calls on both channels of the current connection:

```
Host> disconnect
```

Note The router may automatically reconnect the call after using the **disconnect** command. This can occurs if on-demand dialing is enabled and a telephone number has been entered with the **set number** command. If the router receives enough packets to meet the demand threshold parameters, a new call will be made.

---

establish

To reassign a released service profile identifier (SPID) to the CiscoPro CPA750 series router, use the **establish** command.

establish {1 | 2}

Syntax Description

1	Reassigns the first B channel's SPID.
2	Reassigns the second B channel's SPID.

Command Mode

System level

Usage Guidelines

This command is used to reassign one of the CiscoPro CPA750 series router's SPIDs after it has been released to a device other than the CiscoPro CPA750 series router.

Example

The following example releases and reassigns the Channel 1 SPID from the CiscoPro CPA750 series router so that it can be used by another device on the same ISDN line:

```
Host> establish 1
```

Related Commands

release

release

To use a service profile identifier (SPID) for a device that shares the same ISDN line with the CiscoPro CPA750 series router, use the **release** command.

release {1 | 2}

Syntax Description

1	Uses the SPID assigned to the first ISDN B channel.
2	Uses the SPID to assigned to the second ISDN B channel.

Command Mode

System level

Usage Guidelines

This command is used to assign one of the CiscoPro CPA750 series router SPIDs to an ISDN B channel when it is being used for a device other than the CiscoPro CPA750 series router. Use this command when your ISDN line only supports two SPIDs. To reassign the SPID back to the CiscoPro CPA750 series router, use the **establish** command.

Example

The following example releases the Channel 1 SPID from the CiscoPro CPA750 series router so that it can be used by another device on the same ISDN line:

```
Host> release 1
```

Related Commands

establish

reset caller id receive number

To delete one or all of the telephone numbers from which the router will receive calls when Caller ID is enabled, use the **reset caller id receive number** command:

reset callid {*number* | **all**}

Syntax Description

number	Deletes the specified remote router telephone number that has been entered with the **set caller id receive number** command.
all	Deletes all remote router telephone numbers that have been entered with the **set caller id receive number** command.

Command Mode

System level

Example

The following example deletes a caller id receive number that has been entered with the **set caller id receive number** command:

```
Host> reset callid 14085559020
```

Related Commands

set caller id receive number

set auto

To enable or disable on-demand dialing, use the **set auto** command.

set [*channel*] **auto {on | off}**

Syntax Description

channel	(Optional) ISDN B channel on which on-demand dialing is enabled or disabled. Can be set to 1 or 2. If no channel is specified, on-demand dialing will be enabled or disabled on both links.
on	Enables on-demand dialing.
off	Disables on-demand dialing.

Default

channel 1—Enabled (**on**)
channel 2—Enabled (**on**)

Command Mode

Profile mode.

Example

The following example disables on-demand dialing for the second channel:

```
Host:2503> set 2 auto off
```

set billing spc

To set billing services for semi-permanent connections, use the **set billing spc** command.

set billing spc {*spc-number* | **timelink** | **none**}

Syntax Description

spc-number	Number assigned by AUSTEL when you subscribe to a semi-permanent connection ISDN BRI service.
timelink	Used in Australia (PRI) only. Sets Austel billing services for timelink services. This is an economical billing process for calls of more than one hour but less than three or four hours.
none	Used in Australia (PRI) only. Disables timelink services on Austel billing. This is used on calls of less than one hour.

Command Mode

System level

Usage Guidelines

Use this command when using AUSTEL as your ISDN BRI service provider. Only one side can set the SPC, therefore, set the timeout to off at the called side of the particular user.

set caller id

To enable ISDN Caller ID authentication, use the **set caller id** command.

set callerid {on | off}

Syntax Description

on	Enables ISDN Caller ID authentication.
off	Disables ISDN Caller ID authentication.

Default

off—(disabled)

Command Mode

System level

Usage Guidelines

This configuration applies to all ISDN connections. Caller ID is a service offered by the ISDN service provider in which the calling router is authenticated by its telephone number.

Example

The following example enables Caller ID checking for all ISDN connections:

```
Host> set callerid on
```

Related Commands

set caller id receive number

set delay

To set the time between unsuccessful call attempts, use the **set delay** command.

set [*channel*] **delay** *time*

Syntax Description

channel	(Optional) ISDN B channel to which the delay time applies. Can be either 1 or 2. If no channel is entered, the delay time is set for both links.
delay	Time in seconds between unsuccessful call attempts. Can be between 10 and 32,767. An unsuccessful call will be attempted once the delay time has expired only if the parameters set by the **demand** command are met.

Default

Channel 1—30
Channel 2—30

Command Mode

System level

Usage Guidelines

The delay time applies to all ISDN call attempts.

Example

The following example sets the first channel to retry unsuccessful calls every 15 seconds:

```
Host> set 1 delay 15
```

Note If the CiscoPro CPA750 series routers at both ends of an ISDN connection are configured with on-demand dialing enabled and the same delay time, unsuccessful calls can lead to a nonterminating error condition. This occurs when each router repeatedly tries to call the other at exactly the same delay time. Neither call will be successful, and both routers will repeat the call attempt at the same delay interval.

---

set directory number

To enter the CiscoPro CPA750 series router directory number, use the **set directory number** command.

set [*channel*] **directory** *number* [*.subaddress*]

Syntax Description

channel	(Optional) ISDN B channel to which the directory number applies. Can be 1 or 2. Depending on your ISDN service provider, your line may be assigned one or two SPIDs. If no channel is specified, the directory number applies to both B channels.
directory *number*	The directory number assigned by the telephone company. Can consist of 1 to 20 digits.
.subaddress	(Optional) Subaddress of a device on a multipoint ISDN line. Can consist of 1 to 10 digits.

Default

No directory number is configured.

Command Mode

System level

Usage Guideline

To delete a directory number, enter the command without the number argument.

Examples

The following example sets directory numbers for both Channel 1 and Channel 2:

```
Host> set 1 directory 5551234
Host> set 2 directory 5555678
```

The following example deletes the Channel 2 directory number:

```
Host> set 2 directory
```

set multidestination

To enable multidestination dialing, use the **set multidestination** command.

set multidestination {on | off}

Syntax Description

on	Enables multidestination dialing. The CiscoPro CPA750 series router, through the use of profiles, is able to connect to multiple remote locations over ISDN.
off	Disables multidestination dialing.

Default

off—(disabled)

Command Mode

System level

Note When setting multidestination, ensure you are creating a bridging loop.

Example

The following example enables multidestination dialing:

```
Host> set multidestination on
```

set number

To enter the ISDN telephone number that each ISDN channel calls, use the **set number** command.

set [*channel*] **number** *phone-number* [*.subaddress*]

Syntax Description

channel	(Optional) The ISDN B channel to which the telephone number is assigned. Can be 1 or 2. If no channel is specified, the number is applied to both B channels.
number *phone-number*	The telephone number called when dialing on demand. Can consist of 1 to 32 digits. This number should include all numbers required for the CiscoPro CPA750 series router to complete the call, for example access codes and area codes.
.subaddress	(Optional) The subaddress of a device on a multipoint ISDN line. Can consist of 1 to 10 digits.

Default

No ISDN phone numbers configured.

Command Mode

profile mode

Usage Guidelines

To delete a number entered with the **set number** command, enter the command without the phone number argument and make sure you are in profile mode for the correct profile.

Examples

The following example sets a telephone number that is automatically dialed for profile 2503:

```
Host:2503> set 1 number 14085551234
```

The following example deletes the dialed number for profile 2503:

```
Host:2503> set 1 number
```

Related Commands

set auto

set plan

To set the numbering plan for outgoing calls, use the **set plan** command. The numbering plan is the type of telephone numbering plan the router uses when making callbacks. Numbering plans are predefined settings that configure callbacks so that they conform to local, international, or domestic phone system requirements.

set plan {normal | international | national | subscriber}

Syntax Description

normal	The ISDN switch determines the numbering plan.
international	Callbacks use the international numbering plan.
national	Callbacks use the domestic numbering plan.
subscriber	Callbacks are local calls.

Default

normal

Command Mode

System level

Example

The following example sets the router to use the international numbering plan when making callbacks:

```
Host> set plan international
```

set power source detect

To set the router to use Power Source 1, use the **set powers source detect** command.

set ps1 {on | off}

on	Sets the router to use Power Source 1.
off	Use in areas that do not support Power Source 1.

Default

off

Command Mode

System level

Usage Guidelines

This command applies outside of the United States.

Example

The following example enables the router to use Power Source 1:

```
Host> set ps1 on
```

set protocol

To configure how Ethernet packets are sent over the ISDN line, use the **set protocol** command.

set protocol {hdlc | ordered | fragment}

Syntax Description

hdlc	Packets are encapsulated in standard HDLC. This protocol cannot be used when data compression is enabled with the **set compression** command.
ordered	Packets are arranged in the order they are received.
fragment	Packets are fragmented before being sent over the both ISDN B channels simultaneously. The remote router reassembles the fragments and sends them onto the remote LAN.

Default

ordered

Command Mode

Profile mode

Example

The following example configures profile 2503 for packet fragmentation:

```
Host:2503> set protocol fragment
```

Related Commands

set compression

set ringback number

To set the router's ringback number, use the **set ringback number** command. The ringback number is used by the remote router to make a callback to the CiscoPro CPA750 series router.

set [*channel*] **ringback** *number* [*.subaddress*>]

Syntax Description

channel	(Optional) The ISDN B channel to which the ringback number applies. Can be 1 or 2. If no channel is specified, the ringback number applies to both channels.
ringback *number*	The number used by the remote router to make a callback to the CiscoPro CPA750 series router. Can consist of 1 to 32 digits. This number must include all the digits necessary for the remote router to complete a call to the CiscoPro CPA750 series router, for example area and access codes.
.subaddress	(Optional) Specifies a particular device on a multipoint ISDN line. Can consist of 1 to 10 digits.

Default

No ringback number is configured.

Command Mode

System level

Usage Guidelines

In addition to being the remote router's callback number, the ringback number has another function. To make a second-channel call, the CiscoPro CPA750 series router uses a combination of the number it used to make the first-channel call and the remote router's second-channel ringback number. For example, the CiscoPro CPA750 series router calls 555-1234 to reach the first channel of the remote router. If the second channel phone number is 555-5678, set the remote router's second-channel ringback number to 5678. The local router will use the prefix of the first number it called (555) plus the second channel's ringback number (5678) to make the second call.

Example

The following example sets the number that a remote router uses when making a callback to the CiscoPro CPA750 series router on the first ISDN B Channel:

```
Host> set 1 ringback 14155551234
```

set speed

To set the speed of data calls, use the **set speed** command.

set speed {56 | 64 | auto | voice}

Syntax Description

56	Outgoing calls are connected at 56 kbps. Incoming calls are connected at 56 kbps.
64	Outgoing calls are connected at 64 kbps. Incoming calls are connected at 64 kbps, unless Bearer Capability (BC) indicates the call is at 56 kbps. In this case, calls are connected at 56 kbps. Incoming Voice Bearer Capability (VBC) calls are connected at 56 kbps.
auto	Outgoing calls are attempted at 64 kbps. If unsuccessful, additional call attempts are made at 56 kbps. Incoming calls are connected at the speed indicated by BC and ISDN messages. Incoming VBC calls are connected at 56 kbps.
voice	Outgoing calls are made using VBC at 56 kbps. Incoming calls are accepted with VBC at 56 kbps.

Default

auto

Command Mode

Profile mode

Usage Guidelines

The **voice** keyword should only use ISDN switch types 5ESS or DMS.

Note The DMS switch type is also applicable for NI-1 switch types.

Example

The following example sets the speed for data calls to 64 kbps for profile 2503:

```
Host:2503> set speed 64
```

set spid

To enter a service profile identifier (SPID), use the **set spid** command.

set [*channel*] **spid** *spid-number*

Syntax Description

channel	(Optional) The ISDN B channel to which the SPID applies. If no channel is specified, the SPID applies to both channels.
spid *spid-number*	Number identifying the service to which you have subscribed. This values is assigned by the ISDN service provider and is usually a ten-digit telephone number with some extra digits. The SPID number can consist of 1 to 20 digits.

Default

No SPIDs are configured.

Command Mode

System level

Usage Guidelines

After using this command, use the **reboot** command to reboot the router. To delete a previously entered SPID, use the **set spid** command without the *spid-number* argument.

Examples

The following example sets the SPIDs for both B channels:

```
Host> set 1 spid 0408555123401
Host> set 2 spid 0405555123402
```

The following example deletes the SPID on the first B channel:

```
Host> set 1 spid
```

Related Commands

reboot

set switch

To configure the central office switch, use the **set switch** command.

set switch {5ess | dms }

Syntax Description

5ess	AT&T 5ESS
dms	Northern Telecom DMS-100
NI-1	National ISDN-1

Default

5ess

Command Mode

System level

Example

The following example configures the ISDN switch type as DMS:

```
Host> set switch dms
```

set timeout

To configure the amount of time the ISDN line will remain idle before disconnecting, use the **set timeout** command.

set [*channel*] **timeout** {*time* | **off** }

Syntax Description

channel	(Optional) The ISDN B channel to which the timeout parameters apply. Can be 1 or 2. If no B channel is specified, the timeout parameters apply to both B channels.
time	Time (in seconds) the ISDN line will remain idle before disconnecting. Can be between 1 and 32,767 seconds.
off	The ISDN line will not disconnect automatically.

Default

off

Command Mode

Profile mode

Example

The following example configures both ISDN B channels to disconnect after five minutes for profile 2503:

```
Host:2503> set 1 timeout 500
Host:2503> set 2 timeout 500
```

Related Commands

timeout

Set VoicePriority Mode

The set voiceprority mode cammand sets the voice priority mnode. It determines if the system will disconnect a B-channel assigned to a data call to allow a voice call.

set voicepriority {always|conditional|never|disable}

Syntax Description

always Sets voicepriority to be active under all circumstances.

conditional Sets voicepriority to disconnect the call under certain circumstances, but not under most.

never Disables voicepriority; data calls are never bumped for voice calls.

disable Sets ISDN so that only voice channels are available. This causes ISDN digital data (B channel) to be transmitted over the voice channel.

Default

always

Command Mode

Profile mode

Usage Guidelines

Voicepriority can be set in a variety of ways. Table 7-1 lists the settings and the modes they are active in.

Table 7-1 VoicePriority Modes

Inbound Calls			
Mode	**2 data channels destination A**	**1 data channel to destination A, 1 data channel to destination B**	**1 data channel to destination A—call offered in use[1]**
Always	Bump 1 data channel when inbound call is answered by going off-hook.	Bump 1 data channel when inbound call is answered by going off-hook.	Bump data call when inbound is answered.
Conditional	Bump 1 data channel when inbound call is answered by going off-hook.	No bump; ring busy	No bump; ring busy
Never	No bump; ring busy	No bump; ring busy	No bump; ring busy
Disable	Voice calls are handled as Data Over Voice calls (DOV).	Voice calls are handled as Data Over Voice calls (DOV).	

1. This case only applies when two SPIDs are in use.

Example

The following example configures voicepriority for conditional mode on the profile 2503:

```
Host:2503> set voicepriority conditional
```

show status

To display the current status of the ISDN line and both B channels, use the **show status** command.

show status

Syntax Description

This command contains no keywords or arguments.

Command Mode

System level or profile mode

Example

The following example shows output from the **show status** command:

```
Host:2503> show status

Status    01/03/1995 18:51:42                Connection Link
Line Status
  Line Activated
  Terminal Identifier Assigned
Port Status
  Ch: 1 56K Call In Progress                 7          2
  Ch: 2 56K Call In Progress                 7          1
```

timeout

To configure the parameters that specify when the ISDN line will be disconnected, use the **timeout** command. This is an expanded version of the **set timeout** command, which only allows you to specify duration.

timeout [*channel*] **[threshold** *data-rate*] **[duration** {*time* | **off**}] **[source** {**wan** | **lan** | **both**}]

Syntax Description

channel	(Optional) The ISDN B channel to which the timeout parameters apply. Can be 1 or 2. If no B channel is specified, the timeout parameters apply to both B channels.
threshold *data-rate*	(Optional) Data rate in kbps. If the data rate falls below the specified threshold for the specified duration, the ISDN line disconnects.
duration	(Optional) Length of time in seconds that the traffic must be below the threshold before the ISDN line is disconnected.
time	A number between 1 and 32,767.
off	The ISDN line will not disconnect automatically.
source	(Optional) Source of the traffic in reference to the threshold.
lan	Timeout parameters apply to packets received from the LAN.
wan	Timeout parameters apply to packets received from the ISDN line.
both	Timeout parameters apply to packets received from the interface that has the most traffic, LAN or ISDN.

Default

Channel 1—**threshold** 0, **duration off**, **source lan**
Channel 2—**threshold** 48, **duration off**, **source both**

Command Mode

Profile mode

Usage Guidelines

If the **set timeout** command is configured to off, this command does not apply.

Example

The following example configures both ISDN B channels to disconnect when traffic from either the LAN or the ISDN line falls below 64 kbps for 60 seconds:

```
Host:2503> timeout threshold 64 duration 60 source both
```

Related Commands

set timeout

CHAPTER 8

IP Commands

This chapter describes the commands used to configure IP routing, such as IP static routes, RIP, and IP filters.

reset ip filter

To delete an existing IP filter, use the **reset ip filter** command.

reset ip filter {*filter-id* | **all**}

Syntax Description

filter-id	(Optional) Clears the IP filter with this identification number, which was assigned by the router when the filter was created.
all	(Optional) Clears all IP filters.

Command Mode

Profile mode

Usage Guidelines

Use this command to delete IP filters that have been entered with the **set ip filter** command.

Examples

The following example deletes an IP filter with the identification number of 8 for profile 2503:

```
Host:2503> reset ip filter 8
```

The following example deletes all IP filters for profile 2503:

```
Host:2503> reset ip filter all
```

reset ip route

To delete an IP static route, use the **reset ip route** command.

reset ip route {all | destination *ip-address1* **[***/bits***] gateway** *ip-address2***}**

Syntax Description

all	Deletes all static routes.
destination *ip-address 1*	IP address of the network or host to which the packet is being sent in four-part dotted decimal format.
/bits	(Optional) Number of network bits in the destination network's IP address, counting from the left.
gateway *ip-address2*	IP address of the static route default gateway in four-part dotted decimal format.

Command Mode

Profile mode

Examples

The following example deletes a static route for profile 2503:

```
Host:2503> reset ip route destination 250.250.250.1 gateway 150.150.150.1
```

The following example deletes all static routes for profile 2503:

```
Host:2503> reset ip route all
```

Related Commands

set ip route

set gateway

Use the **set gateway** command to set a static default route pointing at the internal router profile's connection interface.

set gateway *ip-address*
set gateway 0.0.0.0

Syntax Description

ip-address	IP address of the internal profile's interface in four-part dotted decimal format.

Default

0.0.0.0

Command Mode

System level

Example

The following example configures a default static route to the internal profile's connection:

```
Host> set gateway 150.150.10.10
```

set ip address

To set the IP address for any connection, use the **set ip address** command. To delete the IP address for a connection, use this command with 0.0.0.0 as the IP address.

set ip address *ip-address*
set ip address 0.0.0.0

Syntax Description

ip-address	IP address for the interface in four-part dotted decimal format.

Default

0.0.0.0

Command Mode

Profile mode

Example

The following example configures profile 2503's connection with an IP address:

```
Host:2503> set ip address 150.150.10.17
```

set ip cost

To set the cost metric to the next destination, use the **set ip cost** command.

set ip cost *hops*

Syntax Description

hops	Number of routers between this router and the destination network.

Default

1

Command Mode

System level or profile mode

Usage Guidelines

Entering this command while in profile mode applies the cost to that profile's connection. Entering this command at the system level applies the cost to the internal profile.

Example

The following example configures profile 2503 with a cost parameter of 2:

```
Host:2503> set ip cost 2
```

set ip filter

To create an IP filter, use the **set ip filter** command.

set ip filter [*packet-type*] **{in | out}** [**source** [**not**] *ip-address1*] [**destination** [**not**] *ip-address2*] **{block | accept}**

Syntax Description

packet-type — (Optional) One of the following keywords corresponding to an IP packet type:

- **icmp**—ICMP packets.
- **icmpxrd**—ICMP packets, except redirect packets.
- **icmprd**—ICMP redirect packets.
- **tcp**—TCP packets.
- **tcpsyn**—TCP SYN (connection establishment) packets.
- **tcpxsyn**—TCP packets, except SYN.
- **udp**—UDP packets.

If no packet type is specified, the filter is applied to packets of any type.

in — Filters on incoming packets.

out — Filters on outgoing packets.

source *ip-address1* — (Optional) Filters all packets from this address.

Using the **source not ip-address1** keyword applies the filter to any packet that is not from the IP address specified in the command.

destination *ip-address2* — (Optional) Filters all packets destined for this address.

Using the **destination not ip-address2** keyword applies the filter to any packet that is not destined for the IP address specified in the command.

ip-address1...2 — IP address must be entered in the following format:

ip-address [/bits] [:low-port] [+ | –] [high-port]

- *ip-address*—The source or destination IP address. Use a 32-bit quantity in four-part dotted decimal format.
- */bits*—The number of significant bits in the IP address, counting from the left.
- *low-port*—The lowest port number that will be matched by the filter.
  If followed by + , all ports greater than this port will be matched by the filter.
  If followed by – , all ports between this port and the high port will be matched by the filter.
- *high-port*—The highest port number that will be matched by the filter.

Low port and high port arguments can only be used if the packet type is set to **tcp** or **udp**.

block	Prevents the packets defined in the filter from being sent on to the connection.
accept	Allows the packets defined in the filter to be sent on to the connection.

Default

No IP filters are configured.

Command Mode

System level or profile mode

Usage Guidelines

Entering this command while in profile mode applies the IP filter to that profile's connection. Entering this command at the system level applies the IP filter to the internal profile.

Examples

The following example configures profile 2503 with an IP filter that accepts incoming packets addressed to TCP port 25:

```
Host:2503> set ip filter tcp in 198.95.216.1:25 accept
```

The following example configures profile 2503 with an IP filter that blocks the establishment of outgoing TCP connections:

```
Host:2503> set ip filter tcpsyn out block
```

Related Commands

reset ip filter

set ip framing

To set the type of encapsulation used for IP packets, use the **set ip framing** command.

set ip framing {ethernet-ii | none}

Syntax Description

ethernet-ii	Number of routers between this router and the destination network. Use this keyword when connecting to a remote bridge.
none	Sets packet framing to Internet Protocol Control Protocol (IPCP). Use this keyword when using PPP.

Default

ethernet-ii

Command Mode

Profile mode.

Example

The following example configures profile 2503 for IPCP packet framing:

```
Host:2503> set ip framing none
```

set ip netmask

To set the subnet mask for an interface, use the **set ip netmask** command. To delete the subnet mask for an interface, enter this command with 0.0.0.0 as the IP address.

set ip netmask *subnet-mask*
set ip netmask 0.0.0.0

Syntax Description

subnet-mask	Subnet mask for the profile interface. Use a 32-bit quantity in four-part dotted decimal format.

Default

0.0.0.0 (This IP address applies the default subnet mask for Class A, B, and C networks.)

Command Mode

System level or profile mode

Usage Guidelines

Entering this command while in profile mode applies the cost to that profile's connection. Entering this command at the system level applies the cost to the internal profile.

Example

The following example configures the subnet mask for profile 2503:

```
Host:2503> set ip netmask 255.255.255.0
```

Related Commands

set subnet mask

set ip propagate

To set whether a route over the Ethernet interface is propagated in Routing Information Protocol (RIP) broadcast messages, use the **set ip propagate** command.

set ip propagate {on | off}

Syntax Description

on	Routes over the profile's interface will be propagated in RIP broadcast messages whenever the connection is active.
off	Routes over the profile's interface will not be propagated in RIP broadcast messages.

Default

on—(disabled)

Command Mode

System level or profile mode

Usage Guidelines

Entering this command while in profile mode applies the cost to that profile's connection. Entering this command at the system level applies the cost to the internal profile.

Example

The following example configures any route over the profile 2503 connection to be propagated in RIP broadcast messages:

```
Host:2503> set ip propagate on
```

set ip rip receive

To set whether RIP packets are received, use the **set ip rip receive** command.

set ip rip receive {on | off}

Syntax Description

on	RIP packets will be received on the profile's interface.
off	RIP packets will not be received on the profile's interface.

Default

on—(enabled)

Command Mode

System level or profile mode

Usage Guidelines

Entering this command while in profile mode applies the cost to that profile's connection. Entering this command at the system level applies the cost to the internal profile.

Example

The following example configures the connection for profile 2503 to block RIP packets:

```
Host:2503> set ip rip receive off
```

set ip rip update

To specify when RIP packets will be sent, use the **set ip rip update** command.

set ip rip update {periodic | demand | off}

Syntax Description

periodic	RIP packets are sent both periodically and whenever there is a change in the RIP table. Use this keyword for the LAN profile so that RIP information is passed to the LAN at regular intervals.
demand	RIP packets are sent both when the ISDN line first connects and when a change occurs in the RIP table. Use this keyword for WAN connections to avoid bringing up the ISDN line unnecessarily.
off	RIP packets are not sent.

Default

off—(Disabled)

Command Mode

System level or profile mode

Usage Guidelines

Entering this command while in profile mode applies the cost to that profile's connection. Entering this command at the system level applies the cost to the Internal profile.

Example

The following example configures profile 2503 for sending RIP packets on demand:

```
Host:2503> set ip rip update demand
```

set ip rip version

To specify which version of IP RIP (1 or 2) packets are used when sending RIP packets, use the **set ip rip version** command.

set ip rip version {1 | 2}

Syntax Description

1	RIP version 1 packets will be sent.
2	RIP version 2 packets will be sent.

Default

1

Command Mode

Profile mode

Example

The following example configures profile 2503 to send RIP version 2 packets:

```
Host:2503> set ip rip version 2
```

Related Commands

set ip route

set ip route

To define a static IP route, use the command **set ip route.**

set ip route destination *network-address* [*/bits*] **gateway** *next-hop* **[propagate {on | off}]** **[cost** *value*]

Syntax Description

destination *network-address*	Static route's destination network address.
/bits	(Optional) Number of network bits in the destination address, counting from the left. This information will be propagated only if RIP Version 2 is being used for RIP broadcasts.
gateway *next-hop*	IP address of the router that receives the packet for this network or host. This address must be in the same network as the IP address for the interface.
propagate {on | off}	(Optional) Whether the static route defined by this command will be propagated in RIP packets.
cost *value*	(Optional) Cost metric for the route.

Default

No static routes.

Command Mode

Profile mode

Example

The following example configures a static IP route for profile 2503:

```
Host:2503> set ip route destination 198.95.217.0 gateway 198.95.216.2 propagate on cost 2
```

Related Commands

reset ip route

set ip routing

To enable or disable IP routing, use the **set ip routing** command.

set ip routing {on | off}

Syntax Description

on	Enables IP routing on the profile's interface.
off	Disables IP routing on the profile's interface.

Default

Off—(Disabled)

Command Mode

Profile mode

Usage Guidelines

Any profile that has IP routing enabled must have a network address assigned with the **set ip address** command.

Example

The following example enables IP routing for profile 2503:

```
Host:2503> set ip routing on
```

Related Commands

set ip address

set subnet mask

To set the subnet mask for an interface, use the **set subnet mask** command. To delete the subnet mask for an interface, use this command with 0.0.0.0 as the IP address.

set subnet mask *subnet-mask*
set subnet mask 0.0.0.0

Syntax Description

subnet-mask	Subnet mask for the profile's interface in the form of an IP address.

Default

0.0.0.0 (This IP address applies the default subnet mask for Class A, B, and C networks.)

Command Mode

System level or profile mode

Usage Guidelines

Entering this command while in profile mode applies the cost to that profile's interface. Entering this command at the system level applies the cost to the internal profile.

Example

The following example configures the subnet mask for profile 2503:

```
Host:2503> set ip netmask 255.255.255.0
```

Related Commands

set ip netmask

show ip config

To display the IP configuration for one or all profiles, use the show ip configuration command.

show ip config [all]

Syntax Description

all (Optional) Displays IP configuration for all profiles.

Command Mode

System level or profile mode

Usage Guidelines

Use this command while in profile mode to display the IP configuration for that profile. Use this command at the system level or with the keyword **all** to display the IP configurations for all profiles.

Example

The following example shows the output of the **show ip configuration** command for profile 2503:

```
Host:2503> show ip configuration

Profile     Routing  Frame   IP Address   Netmask      RIP  TX  RX  Prop  Cost
-------------------------------------------------------------------------------
2503        ON       ETH2    1.1.1.6      255.0.0.0    V1   DEM ON  OFF   1
```

Table 8-1 describes the fields shown in the display.

Table 8-1 Show IP Configuration Field Descriptions

Field	Description
Profile	Profile that is being displayed. If you are in profile mode, this field displays the name of the profile.
Routing	Indicates if IP routing is enabled for the profile.
Frame	IP framing type used for the profile.
IP Address	IP address for the connection.
Netmask	IP netmask (subnet mask) used for the connection.
RIP	RIP version packets used for the profile.
TX	RIP update used for the profile—Off, Demand, or Periodic.
RX	RIP receive configuration for the profile—On or Off.
Prop	RIP propagate configuration for the profile—On or Off.
Cost	Cost metric of the route.

Related Commands

set user
set ip routing
set ip framing
set ip address
set ip netmask
set subnet mask
set ip rip version
set ip rip update
set ip rip receive
set ip propagate
set ip cost

show ip filter

To display the IP filters for one or all profiles, use the **show ip filter** command.

show ip filter [all]

Syntax Description

all	(Optional) Displays IP filters for all profiles.

Command Mode

System level or profile mode

Usage Guidelines

Use this command while in profile mode to display IP filters for that profile. Use this command at the system level or with the keyword **all** to display IP filters for all profiles.

Example

The following is a sample output of the **show ip filter** command for profile 2503:

```
Host:2503> show ip filter

Profile    ID   Dir   Type   Action     Addresses
-----------------------------------------------------------
2503       2    IN    IP     ACCEPT     DST 150.150.150.1/24
```

Table 8-2 describes the fields shown in the display.

Table 8-2 Show IP Filter Field Descriptions

Field	Description
Profile	Profile that is being displayed. If you are in profile mode, this field displays the name of the profile.
ID	The identification number assigned by the router when the filter is created.
Type	Packet type to which the filter applies. If no packet type is specified in the filter, IP is displayed.
Action	Indicates the action to be taken for packets that match the filter (block or accept).
Addresses	Destination and/or source addresses of the packets to which the filter applies.

Related Commands

set ip filter

show ip route

To display IP static routes for one or all profiles, use the **show ip route** command.

show ip route [all]

Syntax Description

all	(Optional) Displays IP static routes for all profiles.

Command Mode

System level or profile mode

Usage Guidelines

Use this command while in profile mode to display IP static routes for that profile. Use this command at the system level or with the keyword **all** to display IP static routes for all profiles.

Example

The following is a sample output of the **show ip route all** command:

```
Host> show ip route all

Profile   Type  Destination      Bits  Gateway    Prop  Cost   Source   Age
-------------------------------------------------------------------------------
JohnS     NET   150.150.217.0    24    1.1.1.5    ON    3      RIP      0
JohnS     NET   150.150.219.0    24    1.1.1.5    ON    3      RIP      0
JohnS     NET   150.150.216.0    24    1.1.1.5    ON    2      RIP      0
JohnS     NET   177.3.0.0        16    1.1.1.5    ON    3      RIP      0
Internal  NET   149.7.0.0        16    DIRECT     ON    1      DIRECT   0
```

Table 8-3 describes the fields shown in the display.

Table 8-3 Show IP Route Field Descriptions

Field	Description
Profile	Profile that is being displayed. If you are in profile mode, this field displays the name of the profile.
Type	Interface for the route; either NET or WAN.
Destination	Static route's destination address.
Bits	Number of bits in the destination address.
Gateway	Local-network gateway for the route.
Propagate	Indicates if the route is propagated in RIP packets.
Cost	Cost value for the route's destination address.
Source	Source of information about this route.
Age	Number of minutes the route remains in table without being updated.

Related Commands

set ip route

CHAPTER 9

Novell IPX Commands

This chapter describes the commands used to configure IPX routing, such as IPX static routes, RIP, SAP, and IPX service routes.

reset ipx route

To delete one or all static IPX routes for a profile, use the **reset ipx route** command.

reset ipx route {all | destination *network-number* **gateway** *network-address:node-address*}

Syntax Description

all	Deletes all static IPX routes for the profile.
destination *network-number*	The destination network number for the static route.
gateway *network-address:node-address*	The host address of the next router in the path to the destination network.

Command Mode

Profile mode

Related Commands

set ipx route

reset ipx service

To delete one or all static IPX service routes for a profile, use the **reset ipx service** command.

reset ipx service name {all | *service-name* **type** *service-type*}

Syntax Description

all	Deletes all static IPX service routes for the profile.
name *service-name*	Name of the service.
type *service-type*	Service type of the route. This is a hexadecimal number. Table 9-1 in the **set ipx service** section lists examples of service types.

Usage Guidelines

Use this command while in profile mode.

Example

The following example deletes all service routes for a profile:

```
reset ipx thissamplerouter all 0
```

set ipx framing

To set the frame type used by your IPX network, use the **set ipx framing** command.

set ipx framing {ethernet-ii | 802.3 | 802.2 | snap | none}

Syntax Description

ethernet-ii	Sets the IPX framing for Ethernet II type. This is a rarely used, older version of Ethernet.
802.3	Sets the IPX framing for IEEE type 802.3 framing. This framing is used with 10BaseT and AUI connections.
802.2	Sets the IPX framing for IEEE 802.2 framing. This framing is used with coaxial Ethernet cabling.
snap	Sets the IPX framing to Subnetwork Access Protocol (SNAP) framing. SNAP provides framing between a network entitiy in the subnetwork, and a network entity in the end system. SNAP provides data transfer, connection management, and quality of service selection.
none	Specifies IPXCP (Internetwork Packet Exchange Control Protocol) framing. Use the **none** keyword when you are connecting two IPX routers that are using PPP (Point-to-Point Protocol).

Default

Profiles created with the **set user lan** command—**802.3**
Profiles created with the **set user** command—**ethernet-ii**

Command Mode

Profile mode

Example

The following example sets the frame type to IPXCP for profile 2503:

```
Host:2503> set ipx framing none
```

set ipx netbios

To specify whether NetBIOS (Type 20) packets are forwarded on to the LAN, use the **set ipx netbios** command.

set ipx netbios {accept | block}

Syntax Description

accept	NetBIOS packets will be forwarded on to the LAN. Use the **accept** keyword when IPX routing is enabled and when using a NetBIOS protocol, such as Windows for Workgroups.
block	NetBIOS packets will not be forwarded on to the LAN.

Default

block

Command Mode

Profile mode

Example

The following example sets the profile 2503 to forward NetBIOS packets on to the LAN:

```
Host:2503> set ipx netbios accept
```

set ipx network

To set the IPX network address for a profile connection, use the **set ipx network address** command.

set ipx network *network-number*

Syntax Description

network-number	Number of the IPX network to which this profile connects. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range of 1 to FFFFFFFD. A network number of 0 instructs the router to attempt to learn the remote network address from incoming packets.

Default

0

Command Mode

Profile mode

Example

The following example sets the IPX network number for profile 2503:

```
Host:2503> set ipx network 3AAA
```

set ipx rip update

To specify when Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) packets will be sent, use the **set ipx rip update** command.

set ipx rip update {periodic | demand | off}

Syntax Description

periodic	RIP and SAP packets are sent both periodically and whenever there is a change in the RIP or SAP tables. Use this keyword for the LAN profile so that RIP and SAP information is passed to the LAN at regular intervals.
demand	RIP and SAP packets are sent both when the ISDN line first connects and when a change occurs in the RIP or SAP tables. Use this keyword for WAN connections to avoid bringing up the ISDN line unnecessarily.
off	RIP and SAP packets are not sent.

Default

periodic

Command Mode

Profile mode.

Example

The following example disables IPX RIP and SAP packets for the profile 2503:

```
Host:2503> set ipx rip update off
```

set ipx route

To enter a static router in a profile RIP table, use the **set ipx route** command.

set ipx route destination *network-number* [**gateway** *next-hop*] [**hops** *hops*] [**cost** *ticks*]

Syntax Description

destination *network-number*	Destination network number in the form of an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD.
gateway *network-node*	(Optional) The host address of the next router to which packets will be forwarded.
hops *hops*	(Optional) Number of routers between this router and the destination network. If this keyword is not used, the default is 1.
cost *ticks*	(Optional) Number of ticks (one-eighteenth of one second) to the destination network.

Default

No static IPX routes configured.

Command Mode

Profile mode

Example

The following example sets the ipx route to network 150, with four hops between the source and the destination router.

```
set ipx route destination 150 4
```

set ipx routing

To enable or disable routing for a profile interface, use the **set ipx routing** command.

set ipx routing {on | off}

Syntax Description

on	Enables IPX routing for the profile interface.
off	Disables IPX routing for the profile interface.

Default

off—(Disabled)

Command Mode

Profile mode

Example

The following example enables IPX routing for the profile 2503:

```
Host:2503> set ipx routing on
```

set ipx service

To add a service route to your network, use the **set ipx service** command:

set ipx service name *service-name* **type** *service-type* **address** *network-node-socket* [**hops** *hops*]

Syntax Description

all	Deletes all static IPX service routes for the profile.
name *service-name*	Name of the service destination; a 48-byte object name assigned to the server. The service name combined with the service type uniquely identifies a server on a network.
type *service-type*	Service type of the route; a hexadecimal number. Table 9-1 in the "Usage Guidelines" section lists examples of service types.
address *network-node-socket*	The address of the host on which the service resides. The address must be in the following format: • network—Destination network number in the form of an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. • node—MAC address of the host or server. • socket—The software structure serving as the communications endpoint on the network device.
hops *hops*	(Optional) Number of routers across which packets will be forwarded when being routed to the service.

Default

No service routes are configured.

Command Mode

Profile mode

Usage Guidelines

Table 9-1 lists some sample IPX SAP types. For more information about SAP types, contact Novell.

Table 9-1 Sample IPX SAP Services

Service Type (Hexadecimal)	Description
0	All SAP services; IPX defines server type 0 to be an unknown service.
1	User
2	User group
3	Print server queue
4	File server
5	Job server
7	Print server
9	Archive server
A	Queue for job servers
21	NAS SNA gateway
2D	Time Synchronization VAP
2E	Dynamic SAP
47	Advertising print server
4B	Btrieve VAP 5.0
4C	SQL VAP
7A	TES—NetWare for VMS
98	NetWare access server
9A	Named Pipes server
9E	Portable NetWare—UNIX
111	Test server
166	NetWare management (Novell's Network Management Station [NMS])
26A	NetWare management (NMS console)
FFF	Wildcard (any SAP service)

set ipx spoofing

To enable or disable ipx spoofing for IPX watchdog packets, use the **set ipx spoofing** command.

set ipx spoofing {*minutes* | **off**}

Syntax Description

minutes	Enables IPX spoofing for an idle ISDN connection for a specified number of minutes. The range is 1-32,000 minutes.
off	Disables IPX spoofing.

Default

off—(Disabled)

Command Mode

Profile mode

Usage Guidelines

IPX routing must be enabled for any profile on which you wish to enable spoofing.

Example

The following example enables spoofing for one hour on the profile 2503:

```
Host:2503> set ipx spoofing 60
```

Note IPX routing must be enabled for spoofing to function.

Related Commands

set ipx routing

show ipx config

To display IPX configurations for one or all profiles, use the **show ipx config** command.

show ipx config [all]

Syntax Description

all	(Optional) Displays IPX configurations for all filters.

Command Mode

System level or profile mode

Usage Guidelines

Use this command while in profile mode to display IPX configurations for that profile. Use this command at the system level to display IPX configurations for all profiles.

Sample Display

The following example shows the output from the **show ipx config all** command:

```
Host> show ipx config all

Profile      Routing  Frame     NetNum     Updates     Spoof(min)  NetBios
-------------------------------------------------------------------------
2503         ON       802.3     8889       Periodic    60          Block
Internal     ON       802.3     FFFF9      Periodic    0           Block
```

Table 9-2 describes the fields shown in the **show ipx config** display.

Table 9-2 Show IPX Config Field Descriptions

Field	Description
Profile	Profile with which IPX configuration is associated.
Routing	IPX routing enabled or disabled for the connection.
NetNum	Network number to which the connection is made.
Updates	RIP and SAP updates used for the connection—Off, Demand, or Periodic.
Spoof	Spoofing configuration for the connection—Off or number of minutes.
NetBios	NetBIOS packets blocked or accepted on the connection.

show ipx connections

To display information about all IPX connections, use the **show ipx connections** command.

show ipx connections

Syntax Description

This command has no arguments or keywords.

Command Mode

System level or profile mode

Usage Guidelines

This command will display information about all connections when used at the system level or when used while in profile mode.

Sample Display

The following example shows the output from the **show ipx connections** command:

```
Host> show ipx connections

Conn  #Chan  Routing  Address            InPkts    OutPkts  InErr  OutErr
-------------------------------------------------------------------------
2     1      ON       8889:40F902C34C    930434    470510   0      0
INT   1      ON       0FFFF9:40F902C34C  468384    931414   0      0
```

Table 9-3 describes the fields shown in the display.

Table 9-3 Show IPX Connections Field Descriptions

Field	Description
Conn	Connection number assigned by the router when the connection is established.
#Chan	ISDN B channel being used for the connection.
Routing	IPX routing enabled or disabled.
Address	Network and MAC to which the router is connected.
InPkts	Number of incoming packets.
OutPkts	Number of outgoing packets.
InErr	Number of incoming packets lost because of errors.
OutErr	Number of outgoing packets lost because of errors.

show ipx demand

To display IPX RIP and SAP packet statistics, use the **show ipx demand** command.

show ipx demand

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command at the system level for testing purposes.

Sample Display

The following example shows the output from the **show ipx demand** command:

```
Host> show ipx demand

IPX Demand Statistics
Input Requests                0      Output Requests               0
Input Acks                    0      Output Acks                   0
Input Response Pkts           0      Output Response Pkts          0
Input Fragments               0      Output Fragments              0
Reassembly Retries            0      Reassembly Timeouts           0
Retransmit Retries            0      Retransmit Timeouts           0
Pkt Too Short                 0      Duplicate Fragment            0
Bad Fragment Count            0      Bad Fragment Number           0
Bad Sequence Number           0      Timer Failure                 0
```

show ipx route

To display the current routing table with static and learned routes, use the **show ipx route** command.

show ipx route [all]

Syntax Description

all	(Optional) Displays routing tables for all profiles.

Command Mode

System level or profile mode

Usage Guidelines

Use this command while in profile mode to display only static RIP and SAP entries for that profile. Use this command at the system level to display the RIP routing table stored in RAM. Use this command with the all keyword to display all static and dynamic information of all active profiles.

Sample Display

The following example shows the output from the **show ipx route** command used at the system level:

```
4321> show ipx route

Destination     Gateway             Conn   Hops   Time   Flags
-------------------------------------------------------------
7200            8889:40F90056B2     2      3      8      3
7100            8889:40F90056B2     2      3      8      3
4300            8889:40F90056B2     2      3      8      3
4200            8889:40F90056B2     2      3      8      3
4100            8889:40F90056B2     2      3      8      3
5300            8889:40F90056B2     2      3      8      3
5200            8889:40F90056B2     2      3      8      3
6200            8889:40F90056B2     2      3      8      3
610             8889:40F90056B2     2      3      8      3
FF10            8889:40F90056B2     2      5      14     3
9090            8889:40F90056B2     2      2      5      3
0FFEE8          8889:40F90056B2     2      3      8      3
1968            8889:40F90056B2     2      3      8      3
```

Table 9-4 shows the fields displayed with the **show ipx route** command.

Table 9-4 Show IPX Route Field Descriptions

Field	Description
Destination	Route's destination network address.
Gateway	Route's local-network default gateway.
Conn	Route's connection number assigned by the router when the connection is established.
Hops	Number of routers to the destination network.
Time	Number of minutes between incoming RIP packets.
Flags	Number of internal flags (used for troubleshooting).

show ipx service

To display static service routes, use the **show ipx service** command.

show ipx service

Syntax Description

This command has no arguments or keywords.

Command Mode

System level or profile mode

Usage Guidelines

Use this command in profile mode to display static service routes for that profile only. Use this command at the system level to display service routes stored in RAM. Enter the **all** keyword either in profile mode or at the system level to display static and dynamic service information for all active profiles.

Example

The following display is sample output from the **show ipx service** command at the system level:

```
Host> show ipx service

Type  Conn  Hops  Time     Address                 Name
-------------------------------------------------------
4     2     3     1        091492:01:0451          ADMIN
4     2     3     1        0FF2:01:0451            BMW
4     2     5     1        2EB7F81C:01:0451        BENZ
4     2     3     1        09999250:01:0451        CHEVY
4     2     3     1        082468:01:0451          ENGIN
4     2     6     1        2F522FCB:01:0451        JEEP
4     2     4     1        2F51FD85:01:0451        JAGUAR
4     2     3     1        1968:01:0451            FORD
4     2     5     1        02502509:01:0451        VIPER
```

Table 9-5 shows the fields displayed by the **show ipx service** command.

Table 9-5 Show IPX Service Field Descriptions

Field	Description
Type	IPX service type.
Conn	Connection number (assigned by the router) of the service route.
Hops	Number of routers to the service.
Time	Time (in ticks) to the service.
Address	Network and node address of the service.
Name	Service name.

show ipx statistics

To display IPX, IPX RIP, and IPX SAP statistics, use the **show ipx statistics** command.

show ipx statistics

Syntax Description

This command has no arguments or keywords.

Command Mode

System level

Sample Display

The following example shows the output from the **show ipx statistics** command:

```
Host> show ipx statistics

IPX Statistics
Input Packets Total      1398664      Output Packets            14836
Packets Forwarded        1386933      Output Errors                 0
Packets No Route              20      Bad NetBIOS Packets           0
Packets Dropped                0      Packet Hops Exceeded          0
Packets Filtered               0      Packets TooShort              0
Input Packets: SAP:9094         RIP:2617         IPX:0          SPX:0
               NCP:0            NETBIOS:0                     IPXWAN:0

RIP Input Requests           305      Output Requests               0
RIP Input Responses         2312      Output Responses           5358
RIP Packets Filtered           0      Packets TooShort              0

SAP Input Packets           9094      SAP Output Packets         9478
SAP Packets Filtered           0      SAP Packets TooShort          0
SAP Table Entries             28      Lock Failed                   0
SAP Entries Added            418      Service Down Entries         56
SAP Entries Modified           8      Entries Timed Out           334
```

CHAPTER 10

Transparent Bridging Commands

This chapter describes the commands used to configure transparent bridging, such as filtering and address learning.

reset filter

To delete one or all user-defined bridge filters, use the **reset filter** command.

reset [*filter-id*] **filter** [**all**]

Syntax Description

filter-id	Deletes filters based on the identification number assigned to the filter when the filter is created with the **set filter** command.
all	Deletes all filters.

Note Use the **show filter** command to determine filter ID numbers.

Command Mode

System level or profile mode.

Examples

The following example deletes the filter with the identification number 4 from profile 2503:

```
Host:2503> reset 4 filter
```

The following example deletes all filters from profile 2503:

```
Host:2503> reset filter all
```

Related Commands

set filter

reset pattern

To delete one or all bridge filtering patterns, use the **reset pattern** command.

reset {*pattern-name* **pattern** | **pattern all**}

Syntax Description

pattern-name **pattern**	Deletes pattern based on the pattern name which was assigned with the set pattern command.
pattern all	Deletes all patterns.

Command Mode

System level

Example

The following example deletes a pattern called arp from profile 2503:

```
Host:2503> reset arp pattern
```

The following example deletes all patterns from profile 2503:

```
Host:2503> reset pattern all
```

Related Commands

set pattern

reset type

To delete one or all bridge type filters, use the reset type command.

reset type {*type* | **all**}

Syntax Description

type	Deletes a type filter based on the packet type defined with the set type command. Must be in the form of a four-digit hexadecimal number with no spaces between the digits.
all	Deletes all type filters.

Command Mode

System level

Examples

The following example deletes a type filter based on packet type:

```
Host> reset type 0806
```

The following example deletes all type filters:

```
Host> reset type all
```

Related Commands

set type

set filter

To create a user-defined bridge filter, use the **set filter** command.

set [*filter-id*] **filter** [*pattern-name*] **[block | accept] [demand | ignore]**

Syntax Description

filter-id	The filter ID argument is assigned by the router, and is not used to create a filter. It is used to modify existing filter configurations. To display filter IDs, use the **show filter** command.
pattern-name	Reference to pattern created with the **set pattern** command. Filters are composed of patterns. This argument can consist of 1 to 8 pattern names. If you are using more than one pattern in a filter, all patterns must use the same **(from)** value in the **set pattern** command.
block	Prevents packets that match the filter from being forwarded to the connection. Broadcast packets are forwarded. Although multiple filters can be defined, either as accept or block, the most recently defined filter determines which filters (either those set to block or those set to accept) are used.
accept	Prevents packets that match the filter from being forwarded to the connection. Broadcast packets are blocked. Although multiple filters can be defined, either as accept or block, the most recently defined filter determines which filters (either those set to block or those set to accept) are used.
demand	Packets that match the filter are counted in the threshold values that keep the ISDN line connected. Although multiple filters can be defined, either as demand or ignore, the most recently defined filter determines which filters (either those set to demand or those set to ignore) are used.
ignore	Packets that match the filter are counted in the threshold values that keep the ISDN line connected. Although multiple filters can be defined, either as demand or ignore, the most recently defined filter determines which filters (either those set to demand or those set to ignore) are used.

Default

No filters configured.

Command Mode

System level or profile mode

Usage Guidelines

Filters defined at the system level will be used by all profiles. Filters defined while in profile mode will be used by that profile only. Filters apply to both incoming and outgoing packets.

Example

The following example configures a filter that will be used by all profiles:

```
Host> set filter arp john demand
```

Related Commands

reset filter
set pattern

set mode

To configure packet forwarding for bridging, use the **set mode** command

set wan mode {any | only}
set lan mode {any | only}

Syntax Description

wan	Applies the configuration to packets received from the LAN and destined for the ISDN line.
lan	Applies the configuration to packets received from the ISDN line and destined for the LAN.
any	Packets with unknown destination addresses are forwarded to their destination.
only	Only packets with known destination addresses are forwarded to their destination.

Default

wan only
lan any

Command Mode

System level

Usage Guidelines

Addresses are learned either by enabling learning with the **set learn** command or by entering them manually with the **set address** command.

Note Broadcast and multicast packets are always forwarded unless filters are configured to block them.

Example

The following example configures the router to forward any packets with unknown destination addresses from the LAN to the ISDN line:

```
Host> set wan mode any
```

Related Commands

set address
set learn

set passthru

To configure packet bridging between ISDN connections, use the **set passthru** command.

set passthru {on | off}

Syntax Description

on	Enables individual remote routers to bridge to each other through the CiscoPro CPA750 series router.
off	Remote routers can only bridge to devices on the same LAN as the CiscoPro CPA750 series router.

Default

off-(Disabled)

Command Mode

System level.

Example

The following example enables individual remote routers to bridge to each other through the CiscoPro CPA750 series router:

```
Host> set passthru on
```

set pattern

To create a pattern that will be used in user-defined bridge filters, use the **set pattern** command.

set *pattern-name* **[offset** *bytes***] [from {beginning | typefield}]**
pattern {*hex-pattern* **|** *binary-pattern* **|** *decimal-pattern***}**

Syntax Description

pattern-name	Name of the pattern. Can consist of 1 to 7 characters.
offset *bytes*	Number of bytes from the pattern reference point that indicate where the pattern starts. Must be between 0 and 127. The **offset** value and the **pattern** value cannot be more than 128 bytes. If you do not enter a value, defaults to 0.
from	Pattern reference point, from where the **offset** value is counted. Can be **beginning** or **typefield**. If you do not enter one, the default is **beginning**.
beginning	The beginning of the packet.
typefield	The beginning of the packet typefield.
pattern	Value of the pattern. Must be between 1 and 6 bytes, separated by spaces.
hex-pattern	Bit or byte pattern in hexadecimal format. A wildcard in the form **X** can be used in place of a digit.
binary-pattern	Bit or byte pattern in binary format. Will be displayed in hexadecimal format with the **show pattern** command. A wildcard in the form **X** can be used in place of a digit.
decimal-pattern	Bit or byte pattern in decimal format. Will be displayed in hexadecimal format with the **show pattern** command.

Default

No patterns configured.

Command Mode

System level

Usage Guideline

Patterns can be used by all profiles.

Example

The following example sets the offset on the pattern test1 to 6 bytes:

```
host>set test1 off 6
```

The following example changes the pattern name from test1 to test2:

```
Host>set test1 pattern test2
```

Related Commands

reset pattern
set filter
show filter
show pattern

set type

To create a bridge filter based on packet type, use the **set type** command.

set type *packet-type* **[accept | block] [demand | ignore]**

Syntax Description

type *packet-type*	Ethernet packet type. Up to four hexadecimal digits with no spaces between digits.
accept	Only packets with this packet type are forwarded on to the connection. Although multiple type filters can be defined, either as accept or block, the most recently defined type filter determines which type filters (either those set to accept or those set to block) will be used.
block	Packets of this type is be forwarded on to the connection. Although multiple type filters can be defined, either as accept or block, the most recently defined type filter determines which type filters (either those set to accept or those set to block) are used.
demand	Only packets of this type are counted in the demand and timeout calculations that bring the ISDN line up and disconnect it. Although multiple type filters can be defined, either as demand or ignore, the most recently defined type filter determines which type filters (either those set to demand or those set to ignore) are used.
ignore	Packets of this type are not counted in the demand and timeout calculations that bring the ISDN line up and disconnect it. Although multiple type filters can be defined, either as demand or ignore, the most recently defined type filter determines which type filters (either those set to demand or those set to ignore) are used.

Default

No type filters configured.

Command Mode

System level or profile mode

Usage Guidelines

Type filters configured at the system level will be used by all profiles. Type filters configured at the profile level will be used by that profile only.

By default, type filters apply only to broadcast and multicast packets. If unicast filtering is enabled with the **set unicast filtering** command, type filters apply to broadcast, multicast, and unicast packets.

Type filtering is independent of Ethernet address filtering. Packets must match address filters and also type filters before being forwarded to or block from the ISDN line.

Example

The following example configures profile 2503 to prevent broadcast and multicast from activating the ISDN line (however, if the ISDN line already connected, the packets will be forwarded on to the line):

```
Host:2503> set type 1 accept
Host:2503> set type demand
```

There are no Ethernet packets of type 1, so this command will block all broadcast and multicast traffic because there are no Ethernet packet types of 1.

set unicast filtering

To enable or disable unicast filtering, use the **set unicast filtering** command.

set unicast {on | off}

Syntax Description

on	Enables unicast filtering.
off	Disables unicast filtering.

Default

off

Command Mode

System level

Usage Guidelines

Unicast filtering applies to type filters configured with the **set type** command and user-defined filters configured with the **set filter** command.

Example

The following example enables unicast filtering for the router:

```
Host> set unicast on
```

Related Commands

set type
set filter
show filter

show filter

To display user-defined filters, use the **show filter** command.

show [*filter-id*] **filter**

Syntax Description

filter-id	(Optional) The ID number assigned to the filter by the router. Displays that filter only, including all patterns that make up the filter.

Usage Guidelines

At the system level, this command displays all filters configured at the system level. In profile mode, this command displays filters configured at the system level and filters defined while in profile mode. This command also indicates whether unicast filtering is enabled.

Example

The following example shows output from the **show filter** command:

```
Host> show filter
Unicast Filtering     OFF
Filters
      1 Filter  BLOCK           arp
      3 Filter  ACCEPT  DEMAND  john
```

Related Commands

set filter
set unicast filtering

show pattern

To display all patterns configured with the **set pattern** command, use the **show pattern** command.

show [*pattern-name*] **pattern**

Syntax Description

pattern-name	(Optional) Displays a specific pattern by the name assigned with the set pattern command.

Command Mode

System level

Usage Guidelines

Patterns can be used by all profiles.

Example

The following example shows output from the **show pattern** command:

```
Host> show pattern
Patterns
Name    Offset  From       Pattern
board        0  BEGINNING  ff ff ff ff ff ff
arp          0  BEGINNING  12 34 56
start       44  TYPEFIELD  00 f9 00 12 34 56
end          3  TYPEFIELD  00 30
middle      10  BEGINNING  11 11
```

Table 10-1 defines the field shown in the display.

Table 10-1 Show Pattern Field Descriptions

Field	Description
Name	Name of the pattern.
Offset	Number of bytes from the pattern's reference point that the pattern starts.
From	Lists pattern starting reference point. Can be BEGINNING or TYPEFIELD.
Pattern	Byte pattern.

CHAPTER 11

PPP Commands

This chapter describes the commands used to configure Point-to-Point Protocol (PPP) parameters, such as call negotiation and authentication.

set ppp authentication

To set the PPP authentication that is performed for incoming and outgoing ISDN calls, use the **set ppp authentication** command.

set ppp authentication {*incoming* | *outgoing*} **[pap] [chap] [none]**

Syntax Description

incoming	Applies the authentication method to incoming packets. In system configuration, the optional authentication method will apply to both types of calls.
outgoing	(Optional) Applies the authentication method to outgoing packets. In a profile configuration, the authentication method will apply to both types of calls at the system level.
pap	(Optional) Enables Password Authentication Protocol (PAP) to be performed. You must have PAP host password configured with the **set ppp password** command and a User ID configured with the **set system name** command.
chap	(Optional) Enables the challenge Handshake Authentication Protocol (CHAP) authentication. You must have a CHAP host secret configured with the **set ppp password** command and a User ID configured with the **set system name** command.
none	(Optional) No authentication is performed.

Default

incoming chap
outgoing chap

Command Mode

System level or profile mode

Usage Guidelines

You can specify different authentication methods for incoming calls, where the CiscoPro CPA750 series router is the authenticator and outgoing calls, where the CiscoPro CPA750 series router will be authenticated by the remote router.

You may specify one, two, or all of the authentication options. They will be negotiated in the following order: **chap**, **pap**, **none**. If the **none** keyword is not specified and authentication fails, the call will be terminated.

Note This command has no effect on how the CiscoPro CPA750 series router responds to remote authentication requests. The CiscoPro CPA750 series router always responds to PAP or CHAP authentication requests. A client password or secret must be configured with the **set ppp password** command to make the authentication response succeed (unless a Null password or secret is being used by the peer).

Example

The following example sets the router to use incoming PAP authentication:

```
set ppp authentication incoming pap
```

The following example sets the router to use outgoing pap authentication:

```
set ppp authentication outgoing pap
```

Related Commands

set system name
set ppp password

Set PPP Callback Request/Reply

Use the set ppp callback request/reply command to set the callback mode for point-to-point encapsulation. This command ensures a level of callback security.

set ppp callback [{*request* | *reply*}{on|off|always}]

Syntax Description

request	Applies callback from the calling entity to a called entity.
reply	Applies callback from the called entity to a calling entity.
on	Enables callback.
off	Disables callback
always	Enables callback at all times.

Default

off-(Disabled)

Command Mode

Profile mode

Usage Guidelines

When the calling unit's request is set to On, the calling unit intiates a call back request. If the callback request is acknowledged by the called unit, the call will stay connected until either of the following occurs:

- The call is disconnected by the called unit, and the callback is made subsequently by the called unit.
- When the callback is acknowledged by the called unit, but the callback is not attempted by the called unit. This could happen if the called unit callback reply is set to Off for that profile, or the called unit is a product that does not support callback.
- If the calling unit request is set to always, the calling unit disconnects the call after the acknowledgement process. If the called unit reply is set to On or Always, then the called unit will make a callback to the calling unit.
- If the called unit reply is set to Always, the called unit will disconnect the original call. The called unit attempts a callback.

Example

The following example sets the profile to reply always:

```
Host> set ppp callback reply always
```

Related Commands

set number

set security

set ringback

show security

set ppp multilink

To configure the way that PPP packets are received from the ISDN line, use the **set ppp multilink** command.

set ppp multilink {on | off}

Syntax Description

on	Enables the router to reassemble any multilink PPP packets received from the ISDN line.
off	Disables the router from reassembling multilink PPP packets unless the remote router was requested by the remote router.

Default

on-(Enabled)

Command Mode

System level

Example

The following example configures the router to reassemble multilink PPP packets only when requested to do so by the remote router:

```
Host> set ppp multilink off
```

set ppp password

To configure the passwords used during PAP and CHAP PPP authentication, use the **set ppp password** command.

set ppp {password | secret} {host | client}

Syntax Description

password	Used for PAP authentication.
secret	Used for CHAP authentication.
host	Profile configurations used by the CiscoPro CPA750 series router to authenticate a remote router. The remote router's client password or secret must match the CiscoPro CPA750 series router's host password or secret.
client	System configurations used by the remote router to authenticate the CiscoPro CPA750 series router. The CiscoPro CPA750 series router's client password or secret must match the remote router's host password or secret.
password	Password or secret used for PPP authentication.

Default

No passwords or secrets are configured.

Command Mode

System level or profile mode

Usage Guidelines

Configure host passwords and secrets while in profile mode. Configure client passwords and secrets at the system level.

Example

The following example configures the router with a PAP client password:

Step 1 Enter the **set ppp password client** command:

```
Host> set ppp password client
```

Step 2 At the prompt, enter your client password. Your password will not be echoed on the terminal:

```
Enter new Password:
```

Step 3 At the prompt, reenter your client password for confirmation:

```
Re-Type new Password:
```

You have configured the CiscoPro CPA750 series router with a PAP client password.

The following example deletes the PAP client password:

Step 1 Enter the **set ppp password client** command:

```
Host> set ppp password client
```

Step 2 At the prompt, press Return:

```
Enter new Password: <Return>
```

Step 3 At the prompt, press Return again:

```
Re-Type new Password: <Return>
```

You have deleted the CiscoPro CPA750 series router PAP client password.

Related Commands

set ppp authentication

set ppp term count

To configure the number of times the router will send a terminate request packet without an answer before disconnecting the ISDN line, use the **set ppp term count** command.

set ppp term count *attempts*

Syntax Description

attempts	Number of times the router will send a terminate request packet without an answer before disconnecting the ISDN line. Must be between 1 and 100.

Default

2

Command Mode

System level

Example

The following example configures the router to send terminate request packets five times before disconnecting the ISDN line:

```
Host> set ppp term count 5
```

show negotiation

To display all negotiation parameters, use the show negotiation command.

show negotiation [all]

Syntax Description

all	(Optional) Use this keyword in profile mode to display system negotiation parameters and also profile negotiation parameters.

Command Mode

System level or profile mode

Usage Guidelines

In profile mode, this command displays only those parameters which can be configured by profile. Values are inherited from the profile template. Values that have been redefined from the template value are indicated with a *.

On the system level this command displays all system parameters.

Example

The following example shows output from the **show negotiation** command at the system level:

```
Host> show negotiation

System Parameters
   PPP Negotiation Parameters
      Integrity Interval        10
      Retry Count               10
      Retry Interval            3000
      Terminate Count           2
      Multilink                 ON

Profile Parameters
   Negotiated Parameters
      Connection   1            Virtual
      Connection   2  CPP  FRAGMENTED  COMPRESSED
```

CHAPTER 12

SNMP Commands

This chapter describes the commands used to configure System Network Management Protocol (SNMP) parameters, such as management station and traps.

reset snmp trap

To delete one or all of the configured trap hosts, use the **reset snmp trap** command.

reset snmp trap {*ip-address* | **all**}

Syntax Description

ip-address	IP address of the configured trap host in four part dotted-decimal notation.
all	Deletes all configured trap hosts.

Command Mode

System level.

Example

The following example deletes one trap host:

```
Host> reset snmp trap 150.150.50.25
```

Related Commands

set snmp trap host

set snmp contact

To enter the user name that is associated with all SNMP information that is forwarded to the trap host, use the **set snmp contact** command.

set snmp contact *contact-name*

Syntax Description

contact-name	User name that is associated with all SNMP information. Must be between 1 and 64 characters. If it includes spaces, the entire string of characters must be enclosed in quotation marks.

Command Mode

System level

Usage Guidelines

To delete the contact name, enter the command without the *contact-name* argument.

Example

The following example configures a contact name to be associated with SNMP information:

```
Host> set snmp contact "John Doe"
```

The following example deletes the contact name:

```
Host> set snmp contact
```

Related Commands

set snmp location
set snmp trap
set snmp trap host
show snmp

set snmp location

To configure the location name of the router that is associated with all SNMP information, use the **set snmp location** command.

set snmp location *location-name*

Syntax Description

location-name	Location name that is associated with all SNMP information. Must be between 1 and 64 characters. If it includes spaces, the entire string of characters must be enclosed in quotation marks.

Command Mode

System level

Usage Guidelines

To delete the contact name, enter the command without the *location-name* argument.

Example

The following example configures a location name to be associated with SNMP information:

```
Host> set snmp location "San Jose"
```

The following example deletes the location name:

```
Host> set snmp location
```

Related Commands

set snmp contact
set snmp trap
set snmp trap host
show snmp

set snmp trap

To configure when traps are sent to the network management station, use the **set snmp trap** command.

set snmp trap [coldstart {on | off}] [warmstart {on | off}] [linkup {on | off}] [linkdown {on | off}] [authenticationfail {on | off}]

Syntax Description

on	Traps are sent when any of the listed conditions (coldstart, warmstart, linkup, linkdown, or authentication failure) occurs.
off	Traps are not sent when any of the listed conditions (coldstart, warmstart, linkup, linkdown, or authentication failure) occurs.
coldstart	(Optional) Permanent storage is determined to be invalid. If this happens, the router automatically reverts to default values.
warmstart	(Optional) The router is rebooted, except when it sends a coldstart.
linkup	(Optional) A new connection is established. Does not apply to individual B channel establishment.
linkdown	(Optional) A connection is closed. Does not apply to individual B channels closing.
authenticationfail	(Optional) Authentication fails.

Default

Traps are never sent (all off).

Command Mode

System level

Example

The following example configures the router to send traps when the router is rebooted and when authentication fails:

```
Host> set snmp trap warmstart on authenticationfail on
```

Related Commands

set snmp contact
set snmp trap host
show snmp

set snmp trap host

To configure the router with the IP address of a network management station that receives SNMP traps, use the **set snmp trap host** command.

set snmp traphost *ip-address*

Syntax Description

ip-address	IP address of a network management station that receives the SNMP traps in four part dotted decimal notation. A maximum of eight different IP addresses can be entered with this command.

Default

0.0.0.0

Command Mode

System level

Example

The following example configures the router with the IP address of a network management station that will receive traps from the router:

```
Host> set snmp traphost 150.150.50.25
```

Related Commands

reset snmp trap host
set snmp contact
set snmp trap
show snmp

show snmp

To display SNMP configuration for the router, use the **show snmp** command.

show snmp

Command Mode

System level or profile mode

Example

The following example shows output from the **show snmp** command:

```
Host> show snmp

SNMP
Contact         John Doe
Location        San Jose
Trap            COLDSTART  OFF
Trap            WARMSTART  ON
Trap            LINKDOWN   OFF
Trap            LINKUP  OFF
Trap            AUTHENTICATIONFAIL  ON
Trap Host       150.150.50.25
Trap Host       150.150.30.35
```

Table 12-1 describes the fields shown in the display.

Table 12-1 Show SNMP Field Descriptions

Field	Description
Contact	Router's contact name.
Location	Router's location.
Coldstart	Indicates whether a trap is sent when permanent storage is determined to be invalid. Can be on or off.
Warmstart	Indicates whether a trap is sent when the unit is rebooted. Can be on or off.
Linkdown	Indicates whether a trap is sent when a connection closes. Can be on or off.
Linkup	Indicates whether a trap is sent when a connection opens. Can be on or off.
Authentication fail	Indicates whether a trap is sent when authentication fails. Can be on or off.
Trap Host	IP address(es) of management stations where traps are sent.

CHAPTER 13

DTMF Commands

This chapter documents dual tone multifrequency (DTMF) commands that apply to the basic telephone service interface on the CiscoPro CPA753. These configuration commands are entered from the telelphone keypad to enable a limited set of parameters. To enter DTMF commands you must first press the * key twice followed by the two digit designator for the command. After entering the command, press the # key to terminate the command. The following is an example of a DTMF command:

```
**sw#
```

After the command is terminated (with the # key) the CiscoPro CPA753 processes the command. If the command has been entered properly and is being processed the LED on the CiscoPro CPA753 will blink rapidly. If the command is entered in error, the phone will blink slowly, over an extended period of time.

Note These commands apply only to the CiscoPro CPA753. These commands should be performed before connecting the router to the ISDN line.

Caution Do not perform these commands on a terminal connected to the router. You must perform these commands on the telephone keypad of the device that is connected to the CiscoPro CPA753 through the basic telephone service port. The syntax follows the same convention as the other CiscoPro CPA750 series router software commands.

set dtmf directory number

To configure the basic telephone port with the ISDN directory numbers, use the set dtmf directory number command.

****03** [*channel*] *number* [**subaddress*]#

Syntax Description

*	Represents the * key on the telephone keypad.
channel	(Optional) ISDN B channel to which the directory number applies. Can be 1 or 2. Depending on your ISDN service provider, your line may be assigned one or two service profile identification (SPID). If no channel is specified, the directory number applies to both B channels.
number	The directory number assigned by the telephone company. Can consist of 1 to 20 digits.
.*subaddress*	(Optional) Subaddress of a device on a multipoint ISDN line. Can consist of 1 to 10 digits.
#	Represents the # key on the telephone keypad.

Default

No directory number is configured.

Command Mode

Telephone keyboard

Usage Guideline

This parameter must be configured to make analog-to-analog calls through the basic telephone service port. This should be configured before the ISDN line is connected.

Examples

Enter the following commands on the telephone keypad to set the directory numbers for both Channel 1 and Channel 2:

```
**03 1 5551234#
**02 2 5551235#
```

set dtmf gateway

To configure the basic telephone port with the Internal profile's default static route, use the set **dtmf gateway** command.

****06***octet1*octet2*octet3*octet3#*

Syntax Description

*	Represents the * key on the telephone keypad.
octet1...4	One octet of an IP address. Together, the four octets should make up the internal profile gateway address.
#	Represents the # key on the telephone keypad.

Default

0.0.0.0

Usage Guidelines

This parameter must be configured to route over the the basic telephone service port. Use this command on the telephone keypad. This should be configured before the ISDN line is connected.

Example

Enter the following command on the telephone keypad to configure the internal profile default gateway:

```
**06150*150*10*10#
```

Related Commands

set gateway

set dtmf ip address

To configure the basic telephone port with the internal profile IP address, use the set dtmf ip address command.

****05***octet1*octet2*octet3*octet3#*

Syntax Description

*	Represents the * key on the telephone keypad.
octet1...4	One octet of an IP address. Together, the four octets should make up the Internal profile's IP address.
#	Represents the # key on the telephone keypad.

Default

0.0.0.0

Command Mode

Telephone keyboard

Usage Guidelines

This parameter must be configured to route over the the basic telephone service port. This should be configured before the ISDN line is connected.

Example

Enter the following on the telephone keypad to configure the internal profile IP address:

```
**05150*150*10*17#
```

set dtmf ip netmask

To configure the basic telephone service port with the internal profile subnet mask, use the **set dtmf ip netmask** command.

****07***octet1*octet2*octet3*octet4#*

Syntax Description

*	Represents the * key on the telephone keypad.
octet1...4	One octet of an IP address. Together, the four octets should make up the internal profile's IP address.
#	Represents the # key on the telephone keypad.

Default

0.0.0.0 (This IP address applies the default subnet mask for Class A, B, and C networks.)

Command Mode

Telephone keyboard

Usage Guidelines

This parameter must be configured to route over the the basic telephone service port. This should be configured before the ISDN line is connected.

Example

Enter the following command on the telephone keypad to configure the internal profile subnet mask:

```
**07150*150*10*17#
```

set dtmf spid

To configure the basic telephone service port with the integrated services digital network service profile identification (ISDN SPID), use the **set dtmf spid** command.

****02**[*channel*] *spid-number*#

Syntax Description

*	Represents the * key on the telephone keypad.
channel	(Optional) The ISDN B channel to which the SPID applies. If no channel is specified, the SPID applies to both channels.
spid-number	Number identifying the service to which you have subscribed. This value is assigned by the ISDN service provider and is usually a ten-digit telephone number with some extra digits. Can consist of 1 to 20 digits.
#	Represents the # key on the telephone keypad.

Default

No SPIDs are configured.

Command Mode

Telephone keyboard

Usage Guidelines

This parameter must be configured to make analog-to-analog calls over the the basic telephone service port. This should be configured before the ISDN line is connected.

Examples

Enter the following on the telephone keypad to configure the basic telephone service port with the SPIDs for both B channels:

```
** 1 0408555123401#
**02 2 0405555123402#
```

set dtmf switch

To configure the basic telephone port with the central office integrated services digital network (ISDN) switch type, use the **set dtmf switch** command.

***switch-type#*

Syntax Description

*	Represents the * key on the telephone keypad.
switch-type	The switch type used by your ISDN line. Must be represented by 10 or 11: • 10—AT&T 5ESS • 11—Northern Telecom DMS-100 • 12—NI-1
#	Represents the # key on the telephone keypad.

Default

No switch configured.

Command Mode

Telephone keyboard

Usage Guidelines

This parameter must be configured to make analog-to-analog calls over the the basic telephone service port. This should be configured before the ISDN line is connected.

Example

Enter the following command on the telephone keypad to configure the basic telephone service port with the ISDN switch type 5ESS:

```
**10#
```

INDEX

Symbols

C

D

E

H

I

L

N

P

R

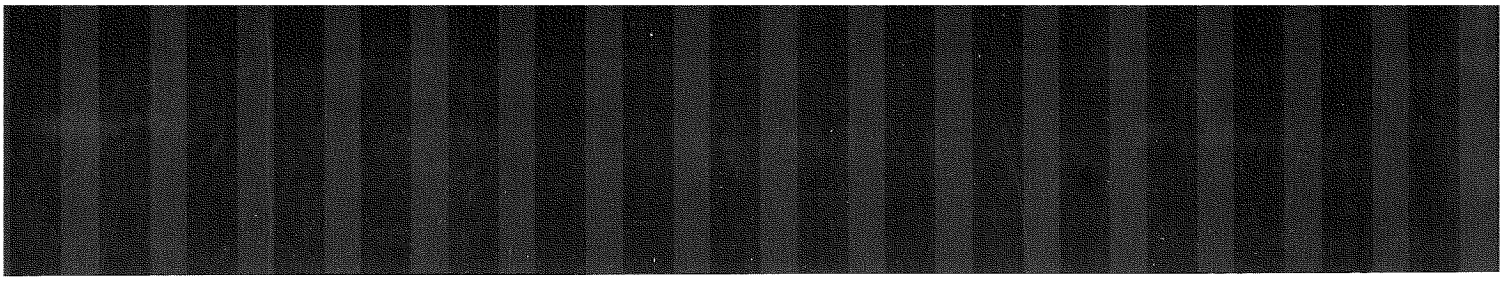
S

T

U

V

W



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
World Wide Web URL:
http://www.cisco.com

Contact your local reseller or, in North America, call 800 GO CISCO (462-4726). International customers, contact your local Cisco sales office.

CISCO SYSTEMS

Printed in the USA on recycled pape containing 10% post-consumer waste

78-2163-0
222-02247-0