Doc. No. 78-0945-06A0
June 14, 1993

CISCO SYSTEMS

Protocol Translator Configuration and Reference Errata

This document supplies corrections and additional information for the 9.0 version of the Cisco publication *Protocol Translator Configuration and Reference* dated April 1992. Keep this document with the *Protocol Translator Configuration and Reference* document for future reference.

Correction to Chapter 3, "Protocol Translator User Commands"

On page 3-6, in the section "The X.3 PAD Parameters," change the description of the parameter 4 (idle timer) values to the following:

Value	Description
0	No timer.
1	Do not delay before sending a packet in the absence of a data forwarding character. This is the default.
2-255	Delay time before sending a packet, in twentieths of a second.

On pages 3-18 and 3-43, the syntax of the **/route** argument is incorrectly given as follows:

/route: *path*

The correct form does not use the colon character, as follows:

/route *path*

Correction to Chapter 4, "System Configuration"

The following corrections apply to Chapter 4.

Correction to "Establishing the Privileged-Level Password"

On page 4-18, replace the last paragraph of the **enable password** description with the paragraphs that follow.

When you use the **enable** command at the console terminal, the EXEC does not prompt you for a password if the privileged mode password is not set. Additionally, if the enable password is not set and the line 0 (console line) password is not set, it is only possible to enter privileged mode on the console terminal. This feature allows you to use physical security rather than passwords to protect privileged mode if that is what you prefer to do.

If the enable password is not set and the line 0 (console) password is set, it is possible to enter privileged command mode either without entering a password at the console terminal or by entering the console line password when prompted while using any other line.

Correction to "Logging Messages to a UNIX Syslog Server"

Add the note that follows to the example on page 4-35.

Note: Many UNIX systems require a tab character to be used as the "white space" separator in the /etc/syslog.conf file. Use of a space character rather than a tab may cause the entry in /etc/syslog.conf to be ignored.

Correction to Chapter 5, "System Management"

On page 5-20, Table 5-9 indicates that the !P character means that the server received a *Protocol Unreachable* message. This should read "Server received *Port Unreachable* message."

Corrections to Chapter 12, "LAT Configuration and Management"

Extended access lists are now supported in the protocol translator on terminal lines. The following information applies to Chapter 12, "TCP/IP Configuration and Management," in the section titled "Restricting Terminal Connections."

Configuring Extended Access Lists

Extended access lists allow finer granularity in control of connections allowed to or from a specific protocol translator port. For example, users may be restricted to only making connections to the telnet port, or incoming access to a port may be restricted to "privileged" ports on the original host.

To define an extended access list, use the extended version of the **access-list** subcommand, as follows:

access-list *list* {**permit**|**deny**} *protocol source source-mask destination destination-mask* [*operator operand*] [**established**]

The argument *list* is an integer from 100 through 199 that you assign to identify one or more extended permit/deny conditions as an extended access list. Note that a list number in the range 100 to 199 distinguishes an extended access list from a standard access list. The condition keywords **permit** and **deny** determine whether the router allows or disallows a connection when a packet matches an access condition. The router stops checking the extended access list after a match occurs. All conditions must be met to make a match.

The argument *protocol* is one of the following keywords:

- **ip**
- **tcp**
- **udp**
- **icmp**

Use the keyword **ip** to match any Internet protocol, including TCP, UDP, and ICMP.

The argument *source* is an Internet source address in dotted-decimal format. The argument *source-mask* is a mask, also in dotted-decimal format, of source address bits to be ignored. The router uses the *source* and *source-mask* arguments to match the source address of a packet. For example, to match any address on a Class C network 192.31.7.0, the argument *source-mask* would be 0.0.0.255. The arguments *destination* and *destination-mask* are dotted-decimal values for matching the destination address of a packet.

To differentiate further among packets, you can specify the optional arguments *operator* and *operand* to compare destination ports, service access points, or contact names. Note that the **ip** and **icmp** protocol keywords do not allow port distinctions.

For the **tcp** and **udp** protocol keywords, the argument *operator* can be one of these keywords:

- **lt**—less than
- **gt**—greater than
- **eq**—equal
- **neq**—not equal

The argument *operand* is the decimal destination port for the specified protocol.

For the TCP protocol there is an additional keyword, **established**, that does not take an argument. A match occurs if the TCP datagram has the ACK or RST bits set, indicating an established connection. The nonmatching case is that of the initial TCP datagram to form a connection; the software goes on to other rules in the access list to determine whether a connection is allowed in the first place.

Note: After an access list is initially created, any subsequent additions (possibly entered from the terminal), are placed at the *end* of the list. In other words, you cannot selectively add or remove access lists command lines from an access list.

Controlling Line Access

To restrict incoming and outgoing connections between a particular terminal line or group of lines (into a Cisco device) and the addresses in an access list, use the **access-class** line configuration subcommand. Full command syntax for this command follows:

access-class *list* {**in**|**out**}
no access-class *list* {**in**|**out**}

This command restricts connections on a line or group of lines to certain Internet addresses.

The argument *list* is an integer from 1 through 199 that identifies a specific access list of Internet addresses.

The keyword **in** applies to incoming connections, such as virtual terminals. The keyword **out** applies to outgoing Telnet connections.

The **no access-class** line configuration subcommand removes access restrictions on the line for the specified connections.

Example 1:

The following example defines an access list that permits only hosts on network *192.89.55.0* to connect to the virtual terminal ports on the router.

```
access-list 12 permit 192.89.55.0  0.0.0.255
line 1 5
access-class 12 in
```

Use the **access-class** keyword **out** to define the access checks made on outgoing connections. (A user who types a host name at the router prompt to initiate a Telnet connection is making an outgoing connection.)

Note: Set identical restrictions on all the virtual terminal lines, because a user can connect to any of them.

Example 2:

The following example defines an extended access list that permits only telnet and rlogin.

```
access-list 101 permit tcp 0.0.0.0 0.0.0.0 0.0.0.0 255.255.255.255
eq 23
access-list 101 permit tcp 0.0.0.0 0.0.0.0 0.0.0.0 255.255.255.255
eq 513
!(implicit deny of everything else)
! public terminals can only telnet and rlogin line 1 20 access-class
101 out
!
```

Extended access-lists also can be used with **slip access-class** *list* [**in**|**out**].

Specifying Access Conditions

Add the text that follows to the section “Specifying Access Conditions” on page 12-15.

When both IP and LAT connections are allowed from a terminal line, and an IP access list is applied to that line with the **access-class** line subcommand, you also must create a LAT access list numbered the same if you want to allow any LAT connections from that terminal. This is because you can specify only one incoming and one outgoing access list number for each terminal line, and when checking LAT access lists, if the list specified does not exist, the system denies all LAT connections.

Corrections to Chapter 14, "XRemote Configuration and Management"

On page 14-1, in the first bulleted list, the third bullet incorrectly lists "EXEC commands for troubleshooting TN3270 operation" and should say "EXEC commands for troubleshooting XRemote operation."

This document is to be used in conjunction with the *Protocol Translator Configuration and Reference* publication.