Cisco IOS Bridging Command Reference

March 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT 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 OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco IOS IBM Networking Command Reference

About Cisco IOS Software Documentation

Last Updated: July 4, 2012

This document describes the objectives, audience, and conventions of Cisco IOS software documentation (including Cisco IOS XE software documentation) and how to access the documentation. Also included are resources for obtaining additional documentation, technical assistance, and other information from Cisco.

For information about the Cisco IOS CLI, see the *Using the Command-Line Interface in Cisco IOS Software* document.

Documentation Objectives

Cisco software documentation describes the concepts, tasks, and commands available to configure and maintain Cisco networking devices. Configuration examples are also provided.

Audience

Cisco software documentation is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the concepts, configuration and maintenance tasks, the relationship among tasks, or the Cisco software commands necessary to perform particular tasks. Cisco software documentation is also intended for those users experienced with Cisco software who need to know about new features, new configuration options, and new software characteristics in a current Cisco software release.

Documentation Conventions

In Cisco software documentation, the term *device* may be used to refer to various Cisco products, including routers, access servers, and switches. These and other networking devices that support Cisco software are shown interchangeably in figures and examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

Typographic Conventions

Convention	Description
^ or Ctrl	Both the **^** symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, that is enclosed within braces or square brackets indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem*.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

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

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Documentation, Resources, and Access

Cisco software documentation consists of the following.

Release Notes and Caveats	Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and select severity 3 (moderate) defects in released Cisco software. Review release notes before other documents to learn whether updates have been made to a feature.
Feature Modules	Cisco software features are documented in feature modules. Feature modules describe one feature or a group of related features that are supported on many different software releases and platforms. Feature modules provide conceptual and task-oriented descriptions of Cisco software features, as well as supporting examples. Your Cisco software release or platform may not support all the features documented in a feature module. See the feature information table at the end of the feature module for information about which features in that module are supported in your software release.
Configuration Guides	Configuration guides are provided by technology and release and comprise a set of individual feature modules relevant to the release and technology and, in certain cases, a particular device.
Command References	Command references are provided by technology only and comprise a set of relevant command pages, in alphabetical order. They provide detailed information about the commands used to configure the Cisco software features that are documented in the companion configuration guides. For each technology, there are one or more command references that support all Cisco software releases and that are updated at each standard release.
Supplementary Documents and Resources	• For information about all Cisco software commands, see the *Cisco IOS Master Command List, All Releases*, or use Command Lookup Tool. • For information about **debug** commands, see the *Cisco IOS Debug Command Reference*. • For information about system messages, use Error Message Decoder. • To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator. • To collaborate on and help shape Cisco documentation, use Cisco DocWiki.

The Cisco software configuration guides and command references support many different software releases and platforms. The Cisco software command references contain commands for Cisco software for all releases. Your Cisco software release or platform may not support all these technologies.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Accessing Cisco Software Documentation

For additional information about configuring and operating specific networking devices and to access all Cisco software documentation, go to the Cisco Product Selection web page on Cisco.com at the following location:

http://www.cisco.com/cisco/web/psa/default.html?mode=prod

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is released monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco software technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Using the Command-Line Interface in Cisco IOS Software

Last Updated: July 4, 2012

This document provides basic information about the command-line interface (CLI) in Cisco IOS software and how you can use some of the CLI features.

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface" module of the *Configuration Fundamentals Configuration Guide*.

For information about the software documentation, see the *About Cisco IOS Software Documentation* document.

Initially Configuring a Device

Initial configuration tasks differ by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at http://www.cisco.com/go/techdocs.

After you have performed the initial configuration and connected the device to your network, you can further configure the device either by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

You can change only two settings on a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600 baud.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

Note The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 Series Aggregation Services Router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

The table below contains common command modes, associated CLI prompts, and a brief description of how each mode can be used. It also describes how to access and exit each mode.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Device>`	Use the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, use the **enable** command.	`Device#`	Use the **disable** command or the **exit** command to return to user EXEC mode.	• Use **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, use the **configure terminal** command.	`Device(config)#`	Use the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, use the **interface** command.	`Device(config-if)#`	Use the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, use the **line vty** or **line console** command.	`Device(config-line)#`	Use the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, use the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` The # symbol represents the line number and increments at each prompt.	Use the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. • Perform password recovery when a Ctrl-Break sequence is used within 60 seconds of a power-on or reload.
Diagnostic (available only on Cisco ASR 1000 Series Routers)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS XE process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was issued, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS XE process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS XE CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS XE state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS XE software or other processes. • Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you use in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to display the commands that you can use while the device is in ROM monitor mode:

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate different command modes:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 1/1
Device(config-if)# ethernet
Device(config-line)# exit
Device(config)# end
Device#
```

Note A keyboard alternative to the **end** command is Ctrl-Z.

The Interactive Help Feature

The CLI includes an interactive Help feature. The table below describes the purpose of the CLI interactive Help commands.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the Help feature in any command mode.
?	Lists all commands available for a particular command mode.
*partial-command***?**	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial-command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the **help** commands:

help

```
Device> help
```

```
Help may be requested at any point in a command by entering a question mark '?'. If nothing
matches, the help list will be empty and you must backup until entering a '?' shows the
available options.
```

```
Two styles of help are provided:
```

```
1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.
```

```
2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Device# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

partial-command?

```
Device(config)# zo?
zone  zone-pair
```

partial-command<Tab>

```
Device(config)# we<Tab> webvpn
```

command ?

```
Device(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

command keyword ?

```
Device(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Command elements are the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific CLI conventions convey information about syntax and command elements. The table below describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of a branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Device(config)# ethernet cfm domain ?
  WORD  domain name
Device(config)# ethernet cfm domain dname ?
  level
Device(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Device(config)# ethernet cfm domain dname level 7 ?
  <cr>

Device(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>

Device(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
```

Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and you should set a password for these commands to prevent unauthorized use. Two types of passwords can be set: enable (not encrypted) and enable secret (encrypted). The following global configuration commands set these passwords:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can be 1 to 25 alphanumeric characters in length, and can start with a numeral. Spaces are also valid password characters; for example, "two words" is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a numeral for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

The Command History Feature

The command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, use the **terminal history size** command:

```
Device# terminal history size number
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, use the **history** command:

```
Device(config-line)# history [size number]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

  Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Use the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The command history feature is enabled by default. To disable this feature for a terminal session, use the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could can stand for **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples are from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, use the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. For example:

- Device(config)# **alias exec prt partition**
- Device(config)# **alias configure sb source-bridge**
- Device(config)# **alias interface rl rate-limit**

To display both default and user-created aliases, use the **show alias** command.

For more information about the **alias** command, see the *Cisco IOS Configuration Fundamentals Command Reference*.

The no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or to disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would use the **no ip routing** command. To re-enable IP routing, you would use the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode of the command-line interface.

The **no** form is documented in the command pages of Cisco software command references. The **default** form is generally documented in the command pages only when the **default** form performs a function different than that of the base and **no** forms of the command.

Command pages often include a "Command Default" section. The "Command Default" section documents the state of the configuration if the command is not used (for configuration commands) or the outcome of using the command if none of the optional keywords or arguments is specified (for EXEC commands).

The debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference*.

Caution Debugging is a high-priority and high-CPU-utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using the following three output modifiers, you can filter this output to show only the information that you want to see.

- **begin** *regular-expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular-expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular-expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Device# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

CLI Error Messages

You may encounter some error messages while using the CLI.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must use the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you use these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Device# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved.

```
Building configuration...
[OK]
Device#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- “Using the Cisco IOS Command-Line Interface” module of the *Configuration Fundamentals Configuration Guide*
- Cisco Support and Downloads (also search for documentation by task or product)

  http://www.cisco.com/cisco/web/support/index.html
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco software commands (requires Cisco.com user ID and password)

  http://tools.cisco.com/Support/CLILookup
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

IBM Networking Commands

access-expression

To define an access expression, use the **access-expression** command in interface configuration mode. To remove the access expression from the given interface, use the **no** form of this command.

access-expression {**in** | **out**} *expression*

no access-expression {**in** | **out**} *expression*

Syntax Description

in | **out**	Either **in** or **out** is specified to indicate whether the access expression is applied to packets entering or leaving this interface. You can specify both an input and an output access expression for an interface, but only one of each.
expression	Boolean access list expression, built as explained in the "Usage Guidelines" section.

Command Default

No access expression is defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in conjunction with the **access-list** command in interface configuration mode.

An access expression consists of a list of terms, separated by Boolean operators, and optionally grouped in parentheses.

An access expression term specifies a type of access list, followed by its name or number. The result of the term is either true or false, depending on whether the access list specified in the term permits or denies the frame.

Table 1 describes the terms that can be used.

Table 6 Access Expression Terms

Access Expression Term	Definition
lsap(2nn)	Subnetwork Access Protocol access list to be evaluated for this frame (Cisco 200 series).
type(2nn)	Subnetwork Access Protocol (SNAP) type access list to be evaluated for this frame (Cisco 200 series).
smac(7nn)	Access list to match the source MAC address of the frame (Cisco 700 series).
dmac(7nn)	Access list to match the destination MAC address of the frame (Cisco 700 series).
netbios-host(name)	NetBIOS-host access list to be applied on NetBIOS frames traversing the interface.
netbios-bytes(name)	NetBIOS-bytes access list to be applied on NetBIOS frames traversing the interface.

Access expression terms are separated by Boolean operators, as listed in Table 2.

Table 7 Boolean Operators for Access Expression Terms

Boolean Operators	Definitions
~ (called “not”)	Negates, or reverses, the result of the term or group of terms immediately to the right of the ~. Example: “~lsap (201)” returns FALSE if “lsap (201)” itself were TRUE.
& (called “and”)	Returns TRUE if the terms or parenthetical expressions to the left and right of the & both return TRUE. Example: “lsap (201) & dmac (701)” returns TRUE if both the lsap (201) and dmac (701) terms return TRUE.
| (called “or”)	Returns TRUE if the terms or parenthetical expressions either to the left or to the right of the | or both return TRUE. Example: “lsap (201) | dmac (701)” returns TRUE if either the lsap (201) or dmac (701) terms return TRUE, or if both return TRUE.

Terms can be grouped in parenthetical expressions. Any of the terms and operators can be placed in parentheses, similar to what is done in arithmetic expressions, to affect order of evaluation.

An “access-expression” type filter cannot exist with a “source-bridge” type filter on the same interface. The two types of filters are mutually exclusive.

Note The incorrect use of parentheses can drastically affect the result of an operation because the expression is read from left to right.

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

access-list

To configure the access list mechanism for filtering frames by protocol type or vendor code, use the **access-list** command in global configuration mode. To remove the single specified entry from the access list, use the **no** form of this command.

access-list *access-list-number* {**permit** | **deny**} {*type-code wild-mask* | *address mask*}

no access-list *access-list-number* {**permit** | **deny**} {*type-code wild-mask* | *address mask*}

Syntax Description

access-list-number	Integer that identifies the access list. If the *type-code* and *wild-mask* arguments are included, this integer ranges from 200 to 299, indicating that filtering is by protocol type. If the *address* and *mask* arguments are included, this integer ranges from 700 to 799, indicating that filtering is by vendor code.
permit	Permits the frame.
deny	Denies the frame.
type-code	16-bit hexadecimal number written with a leading 0x; for example, 0x6000. Specify either a Link Service Access Point (LSAP) type code for 802-encapsulated packets or a Subnetwork Access Protocol (SNAP) type code for SNAP-encapsulated packets. (LSAP, sometimes called SAP, refers to the type codes found in the DSAP and SSAP fields of the 802 header.)
wild-mask	16-bit hexadecimal number whose ones bits correspond to bits in the *type-code* argument. The *wild-mask* argument indicates which bits in the *type-code* argument should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be 0x0101 because these two bits are used for purposes other than identifying the SAP code.)
address	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. This field is used for filtering by vendor code.
mask	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. The ones bits in *mask* are the bits to be ignored in *address*. This field is used for filtering by vendor code. For source address filtering, the mask always should have the high-order bit set. This is because the IEEE 802 standard uses this bit to indicate whether a Routing Information Field (RIF) is present, not as part of the source address.

Command Default

No access list is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For a list of type codes, refer to Appendix: Ethernet Type Codes.

Examples

In the following example, the access list permits only Novell frames (LSAP 0xE0E0) and filters out all other frame types. This set of access lists would be applied to an interface via the **source-bridge input-lsap list** or **source-bridge input-lsap list** command (described later in this chapter).

```
access-list 201 permit 0xE0E0 0x0101
access-list 201 deny 0x0000 0xFFFF
```

Combine the DSAP/LSAP fields into one number to do LSAP filtering; for example, 0xE0E0—not 0xE0. Note that the deny condition specified in the preceding example is not required; access lists have an implicit deny as the last statement. Adding this statement can serve as a useful reminder, however.

The following access list filters out only SNAP type codes assigned to Digital Equipment Corporation (DEC) (0x6000 to 0x6007) and lets all other types pass. This set of access lists would be applied to an interface using the **source-bridge input-type-list** or **source-bridge output-type-list** command (described later in this chapter).

```
access-list 202 deny 0x6000 0x0007
access-list 202 permit 0x0000 0xFFFF
```

Note Use the last item of an access list to specify a default action; for example, to permit everything else or to deny everything else. If nothing else in the access list matches, the default action is to deny access; that is, filter out all other type codes.

Type code access lists will negatively affect system performance by greater than 30 percent. Therefore, we recommend that you keep the lists as short as possible and use wildcard bit masks whenever possible.

Related Commands

Command	Description
access-expression	Defines an access expression.
source-bridge input-address-list	Applies an access list to an interface configured for source-route bridging, and filters source-routed packets received from the device interface based on the source MAC address.
source-bridge input-lsap-list	Filters, on input, FDDI and IEEE 802-encapsulated packets that include the DSAP and SSAP fields in their frame formats.
source-bridge input-type-list	Filters SNAP-encapsulated packets on input.

Command	Description
source-bridge output-address-list	Applies an access list to an interface configured for SRB, and filters source-routed packets sent to the device interface based on the destination MAC address.
source-bridge output-lsap-list	Filters, on output, FDDI and IEEE 802-encapsulated packets that have DSAP and SSAP fields in their frame formats.
source-bridge output-type-list	Filters SNAP-encapsulated frames by type code on output.

access-list (extended-ibm)

To provide extended access lists that allow more detailed access lists, use the **access-list** command in global configuration mode. These lists allow you to specify both source and destination addresses and arbitrary bytes in the packet.

access-list *access-list-number* {**permit** | **deny**} *source source-mask destination destination-mask offset size operator operand*

Syntax Description

access-list-number	Integer from 1100 to 1199 that you assign to identify one or more **permit/deny** conditions as an extended access list. Note that a list number in the range from 1100 to 1199 distinguishes an extended access list from other access lists.
permit	Allows a connection when a packet matches an access condition. The Cisco IOS software stops checking the extended access list after a match occurs. All conditions must be met to make a match.
deny	Disallows a connection when a packet matches an access condition. The software stops checking the extended access list after a match occurs. All conditions must be met to make a match.
source	MAC Ethernet address in the form *xxxx.xxxx.xxxx.*
source-mask	Mask of MAC Ethernet source address bits to be ignored. The software uses the *source* and *source-mask* arguments to match the source address of a packet.
destination	MAC Ethernet value used for matching the destination address of a packet.
destination-mask	Mask of MAC Ethernet destination address bits to be ignored. The software uses the *destination* and *destination mask* arguments to match the destination address of a packet.
offset	Range of values that must be satisfied in the access list. Specified in decimal or in hexadecimal format in the form 0x*nn*. The offset is the number of bytes from the destination address field; it is not an offset from the start of the packet. The number of bytes you need to offset from the destination address varies depending on the media encapsulation type you are using.
size	Range of values that must be satisfied in the access list. Must be an integer from 1 to 4.

operator	Compares arbitrary bytes within the packet. Can be one of the following keywords: **lt**—less than **gt**—greater than **eq**—equal **neq**—not equal **and**—bitwise and **xor**—bitwise exclusive or **nop**—address match only
operand	Compares arbitrary bytes within the packet. The value to be compared to or masked against.

Command Default

No extended access lists are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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 list command lines from a specific access list.

An extended access list should not be used on FDDI interfaces that provide transit bridging.

There is not a **no** form for this command.

Note Due to their complexity, extended access lists should only be used by those who are very familiar with the Cisco IOS software. For example, to use extended access lists, it is important to understand how different encapsulations on different media would generally require different offset values to access particular fields.

Caution Do not specify offsets into a packet that are greater than the size of the packet.

Examples

The following example shows an extended access list. The first **access-list** command permits packets from MAC addresses 000c.1b*xx.xxxx* to any MAC address if the packet contains a value less than 0x55AA in the 2 bytes that begin 0x1e bytes into the packet. The seconds **access-list** command permits an NOP operation:

```
access-list 1102 permit 000c.1b00.0000 0000.00ff.ffff 0000.0000.0000
    ffff.ffff.ffff 0x1e 2 lt 0x55aa
access-list 1101 permit 0000.0000.0000 ffff.ffff.ffff 0000.0000.0000
    ffff.ffff.ffff
!
interface ethernet 0
 bridge-group 3 output-pattern 1102
```

The following is sample output from the **show interfaces crb** command for the access list configured above:

```
Device# show interfaces crb

Bridged protocols on Ethernet0/3:
clns  decnet  vines  apollo
novell  xns

Software MAC address filter on Ethernet0/3
Hash Len   Address         Matches   Act   Type
0x00: 0    ffff.ffff.ffff  0         RCV   Physical broadcast
0x00: 1    ffff.ffff.ffff  0         RCV   Appletalk zone
0x2A: 0    0900.2b01.0001  0         RCV   DEC spanning tree
0x49: 0    0000.0c36.7a45  0         RCV   Interface MAC address
0xc0: 0    0100.0ccc.cccc  48        RCV   CDP
0xc2: 0    0180.c200.0000  0         RCV   IEEE spanning tree
0xF8: 0    0900.07ff.ffff  0         RCV   Appletalk broadcast
```

Table 3 describes significant fields shown in the display.

Table 8 show interfaces crb Field Descriptions

Field	Description
Bridged protocols on…	List of the bridged protocols configured for the specified interface.
Software MAC address filter on…	Table of software MAC address filter information for the specified interface.
Hash	Hash key/relative position in the keyed list for this MAC-address entry.
Len	Length of this entry to the beginning element of this hash chain.
Address	Canonical (Ethernet ordered) MAC address.
Matches	Number of received packets matched to this MAC address.
Act	Action to be taken when that address is looked up; choices are to receive or discard the packet.
Type	MAC address type.

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
access-list (type-code-ibm)	Builds type-code access lists.
bridge-group output-pattern-list	Associates an extended access list with a particular interface.

access-list (standard-ibm)

To establish a MAC address access list, use the **access-list** command in global configuration mode. To remove access list, use the **no** form of this command.

access-list *access-list-number* {**permit** | **deny**} *address mask*

no access-list *access-list-number*

Syntax Description

access-list-number	Integer from 700 to 799 that you select for the list.
permit	Permits the frame.
deny	Denies the frame.
address mask	48-bit MAC addresses written as a dotted triple of four-digit hexadecimal numbers. The ones bits in the *mask* argument are the bits to be ignored in *address*.

Command Default

No MAC address access lists are established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring bridging access lists of type 700 may cause a momentary interruption of traffic flow.

Examples

The following example assumes that you want to disallow the bridging of Ethernet packets of all Sun workstations on Ethernet interface 1. Software assumes that all such hosts have Ethernet addresses with the vendor code 0800.2000.0000. The first line of the access list denies access to all Sun workstations, and the second line permits everything else. You then assign the access list to the input side of Ethernet interface 1.

```
access-list 700 deny 0800.2000.0000 0000.00FF.FFFF
access-list 700 permit 0000.0000.0000 FFFF.FFFF.FFFF
!
interface ethernet 1
 bridge-group 1 input-address-list 700
```

Related Commands

Command	Description
access-list (type-code-ibm)	Builds type-code access lists.

access-list (type-code-ibm)

To build type-code access lists, use the **access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-number* {**permit** | **deny**} *type-code wild-mask*

no access-list *access-list-number*

Syntax Description

access-list-number	User-selectable number from 200 to 299 that identifies the list.
permit	Permits the frame.
deny	Denies the frame.
type-code	16-bit hexadecimal number written with a leading "0x"; for example, 0x6000. You can specify either an Ethernet type code for Ethernet-encapsulated packets, or a destination service access point (DSAP)/source service access point (SSAP) pair for 802.3 or 802.5-encapsulated packets. Ethernet type codes are listed in the appendix "Ethernet Type Codes."
wild-mask	16-bit hexadecimal number whose ones bits correspond to bits in the *type-code* argument that should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be at least 0x0101 because these two bits are used for purposes other than identifying the SAP codes.)

Command Default

No type-code access lists are built.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Type-code access lists can have negatively affect system performance; therefore, keep the lists as short as possible and use wildcard bit masks whenever possible.

Access lists are evaluated according to the following algorithm:

- If the packet is Ethernet Type II or SNAP, the type-code field is used.
- If the packet is another type, then the LSAP is used.

Packets are treated according to the following algorithm:

- If the length/type field is greater than 1500, the packet is treated as an Advanced Research Projects Agency (ARPA) packet.
- If the length/type field is less than or equal to 1500, and the DSAP and SSAP fields are AAAA, the packet is treated using type-code filtering.
- If the length/type field is less than or equal to 1500, and the DSAP and SSAP fields are *not* AAAA, the packet is treated using Link Service Access Point (LSAP) filtering.

If the LSAP-code filtering is used, all SNAP and Ethernet Type II packets are bridged without obstruction. If type-code filtering is used, all LSAP packets are bridged without obstruction.

If you have both Ethernet Type II and LSAP packets on your network, you should set up access lists for both.

Examples

The following example shows how to permit only local-area transport (LAT) frames (type 0x6004) and filters out all other frame types:

```
access-list 201 permit 0x6004 0x0000
```

The following example shows how to filter out only type codes assigned to Digital Equipment Corporation (DEC) (0x6000 to 0x600F) and lets all other types pass:

```
access-list 202 deny 0x6000 0x000F
access-list 202 permit 0x0000 0xFFFF
```

Use the last item of an access list to specify a default action; for example, permit everything else or deny everything else. If nothing else in the access list matches, the default action is normally to deny access; that is, filter out all other type codes.

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.

adapter

To configure internal adapters, use the **adapter** command in internal LAN interface configuration submode. To remove an internal adapter, use the **no** form of this command.

adapter *adapter-number* [*mac-address*] [**hsma-partner** *hsma-mac-address*]

no adapter *adapter-number* [*mac-address*]

Syntax Description

adapter-number	Number in the range from 0 to 31 that uniquely identifies the internal adapter (relative adapter number) for all internal LANs of the same type on the Cisco Mainframe Channel Connection (CMCC) adapter. In Cisco Systems Network Architecture (CSNA), this value corresponds to the adapter number (ADAPNO) parameter defined in the Virtual Telecommunications Access Method (VTAM) Extended Communications Adapter (XCA) Major Node.
mac-address	(Optional) MAC address for this internal adapter. This is a hexadecimal value in the form *xxxx.xxxx.xxxx*.
hsma-partner	(Optional) Specifies a hot standby MAC address (HSMA) partner.
hsma-mac-address	(Optional) MAC address of the HSMA partner control adapter.

Command Default

No default behavior or values.

Command Modes

Internal LAN interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.3(3)	The **hsma-partner** keyword and *hsma-mac-address* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. Internal adapters are used to provide LAN gateway MAC addresses for the following CMCC adapter features: CSNA, Cisco Multipath Channel (CMPC), and TN3270 Server.

Up to 18 internal adapters can be configured on a CMCC adapter. Internal adapters are configured on internal LANs. The only limit to the number of internal adapters that you can configure on a single internal LAN is the limit of up to 18 total internal adapters per CMCC.

When an internal adapter configuration command is removed or an existing internal adapter is modified, the *mac-address* parameter is not required. In internal adapter configuration mode, the device prompt appears as follows:

```
Device(cfg-adap-type n-m)#
```

In this syntax, *type* is the internal LAN type, *n* is the LAN ID, and *m* is the adapter number.

HSMA is designed to allow redundant CMCC internal adapter MAC addresses in an Ethernet environment. Communication between the HSMA control adapters is used to ensure that only one of the adapters is active at a time.

Examples

The following example shows how to configure internal adapters 3 and 4 (with their corresponding MAC addresses) on the internal Token Ring LAN number 20, and internal adapter 1 on the internal Token Ring LAN number 10:

```
interface channel 1/2
 lan tokenring 20
  adapter 3 4000.7500.0003
  adapter 4 4000.7500.0004
 lan tokenring 10
  source-bridge 100 1 100
  adapter 1 4000.7500.1111
```

The following example shows how to configure internal adapter 9 to communicate with the HSMA partner at the MAC address 4043.3333.001a:

```
interface Channel1/2
 lan TokenRing 20
  source-bridge 310 3 100
  adapter 9 4043.1313.9009 hsma-partner 4043.3333.001a
 lan TokenRing 20
  source-bridge 319 9 100
  adapter 26 4043.1111.001a
   hsma enable
```

Related Commands

Command	Description
lan	Configures an internal LAN on a CMCC adapter interface and enters the internal LAN configuration mode.
name	Assigns a name to an internal adapter.
show extended channel hsma	Displays hot standby MAC address (HSMA) information
show extended channel lan	Displays the internal LANs and adapters configured on a CMCC adapter.
show extended channel llc2	Displays information about the LLC2 sessions running on CMCC adapter interfaces.
show extended channel connection-map llc2	Displays the number of active LLC2 connections for each SAP and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.
source-bridge	Configures an interface for SRB.

allocate lu

To assign logical unit (LU)s to a pool, use the **allocate lu** command in listen-point physical unit (PU) configuration submode. To remove LUs assigned to a pool, use the **no** form of this command.

allocate lu *lu-address* **pool** *poolname* **clusters** *count*

no allocate lu *lu-address* **pool** *poolname* **clusters** *count*

Syntax Description

lu-address	Starting number of the LOCADDR to which a cluster of LUs are to be allocated.
pool *poolname*	Pool name to which you want to allocate LUs. The pool name cannot exceed eight characters in length.
clusters *count*	Range of LUs in a cluster that are allocated to the specified pool. For example, if the **lu** keyword specifies the beginning of the LOCADDR number, the **cluster** keyword specifies the number of clusters to be included in the pool.

Command Default

No LUs are assigned to a pool.

Command Modes

Listen-point PU configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The following guidelines apply to the **allocate lu** command:

- The LUs assigned to a pool constitute a cluster. When multiple pools are configured, the LU ranges for different pools on the same PU must not overlap.
- A maximum of 255 LOCADDRs can be allocated to a pool. Configurations with invalid LOCADDRs are deleted. Overlapping LU ranges between different pools are invalid.
- The LOCADDR ranges must not overlap for multiple allocation statements and with existing ranges specified for client nailing statements.
- When LUs are allocated while LUs are in use, existing clients are allowed to complete their sessions unaffected.

Examples

In the following example, the starting LOCADDR is 10. Each cluster has 10 LOCADDRs, therefore 50 LOCADDRs are allocated to the pool name LOT1.

```
interface channel 0/2
 tn3270-server
 pool LOT1 cluster layout 4s1p
  listen-point 10.20.30.40
   pu PU1
    allocate lu 10 pool LOT1 clusters 5
```

As a result of this configuration, the following LOCADDRs are created in each cluster:

- Cluster 1
  - LOCADDR 10—Screen
  - LOCADDR 11—Screen
  - LOCADDR 12—Screen
  - LOCADDR 13—Screen
  - LOCADDR 14—Printer
- Cluster 2
  - LOCADDR 15—Screen
  - LOCADDR 16—Screen
  - LOCADDR 17—Screen
  - LOCADDR 18—Screen
  - LOCADDR 19—Printer

All of the LUs in these clusters are allocated to pool LOT1.

Related Commands

Command	Description
pool	Defines pool names for the TN3270 server and specifies the number of screens and printers in each logical cluster.
pu (TN3270)	Creates a PU entity that has its own direct link to a host and enters PU configuration mode.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

alps a1-map a2-map

To specify the A1 and A2 logical agent-set control unit (ASCU) identification information, use the **alps a1-map a2-map** command in Airline Product Set (ALPS) ASCU configuration submode. To remove the specification of the A1 and A2 logical ASCU identification information, use the **no** form of this command.

alps a1-map *a1-value* **a2-map** *a2-value*

no alps a1-map *a1-value* **a2-map** *a2-value*

Syntax Description

a1-value	A1 logical ASCU identification: • airline link control (ALC) range—Hexadecimal number in the range from 0 to 0xFF. • Unisys Terminal System (UTS) range—Hexadecimal number in the range from 0 to 0xFF.
a2-value	A2 logical ASCU identification: • ALC range—Hexadecimal number in the range from 0 to 0xFF. • UTS range—Hexadecimal number in the range from 0 to 0xFF.

Command Default

No A1 and A2 logical ASCU identification information is specified.

Command Modes

ALPS ASCU submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(2)T	The range values were modified.
12.0(5)T	The range values were modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies the A1 identification as 0x4C and the A2 identification as 0x20:

```
alps a1-map 4C a2-map 20
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps alias

To specify that an airline link control (ALC) agent-set control unit (ASCU) is to operate in nonpolling mode, and to specify the parent ASCU interchange address to which this ASCU is aliased, use the **alps alias** command in Airline Product Set (ALPS) ASCU configuration submode. To return the ASCU to polled mode, use the **no** form of this command.

alps alias *alias-interchange-address*

no alps alias *alias-interchange-address*

Syntax Description

alias-interchange-address	Specifies the interchange address of the polled (alias) ASCU with which to associate this non-polled ASCU. Valid range is between 41 and 7E, except 43, 44, 50 to 53, and 60.

Command Default

If you do not specify the **alps alias** command, the ASCU functions in normal polled mode. You must specify the **alps alias** command to enable non-polled handling.

Command Modes

ALPS ASCU configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to ALC ASCUs.

By default, an ALC ASCU cannot send data to a remote device until it is polled by that device. However, you can use this command to configure *non-polled* ALC ASCUs.

A non-polled ASCU must be associated with another, polled ASCU, known as the alias ASCU. When a remote device polls the alias ASCU, the device accepts data from that ASCU and from all non-polled ASCUs associated with that ASCU. The non-polled ASCUs present the same characteristics to the host as the alias ASCU, so the current ASCU configuration is maintained.

This command does not impact the ALC send path or the circuit management code.

Examples

The following example sets the ALC ASCU with interchange address 4B to operate in nonpolling mode and sets 42 as the alias interchange address:

```
alps ascu 4B
alps alias 42
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
show alps ascu	Displays the status of the ALPS ASCU.

alps ascu

To specify a physical agent-set control unit (ASCU) identity, use the **alps ascu** command in Airline Product Set (ALPS) ASCU configuration submode. To remove the ASCU from the interface and delete any messages queued for transmission to the ASCU or the network, use the **no** form of this command.

alps ascu *id*

no alps ascu *id*

Syntax Description

id	ASCU identification. Valid range is from 41 to 7E, except 43, 44, 50 to 53, and 60. The Unisys Terminal System (UTS) valid range is from 21 to 4F.

Command Default

No physical ASCU identity is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(2)T	This command was modified for UTS support.
12.1(2)T	The valid range values were modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If an ASCU already exists on the interface, the **alps ascu** command initiates the ALPS ASCU configuration submode for that ASCU. If the ASCU does not exist, an ASCU is created and the ALPS ASCU configuration submode is initiated.

Examples

The following example specifies the interchange address as 4B:

```
alps ascu 4B
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol is used on the serial interface.
encapsulation alc	Specifies that the P1024B airline link control (ALC) protocol is used on the serial interface.

alps auto-reset

To automatically reset a nonresponsive airline link control (ALC) agent-set control unit (ASCU) in the DOWN state, use the **alps auto-reset** command in Airline Product Set (ALPS) ASCU configuration submode. To disable the automatic reset, use the **no** form of this command.

alps auto-reset

no alps auto-reset

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic ASCU reset is disabled by default.

Command Modes

ALPS ASCU configuration submode

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to ALC ASCUs.

Examples

The following example shows how to configure automatic reset for all nonresponsive ASCUs in the DOWN state:

```
alps auto-reset
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
encapsulation alc	Specifies that the P1024B ALC protocol is used on the serial interface.

alps circuit

To specify an Airline Product Set (ALPS) circuit at the remote customer premises equipment (CPE) across a TCP/IP connection, use the **alps circuit** command in ALPS circuit configuration submode. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

alps circuit *name*

no alps circuit *name*

Syntax Description

name	Name given to identify an ALPS circuit.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Entering this command causes a circuit control block to be created. The command also initiates the ALPS circuit configuration submode. If the circuit already exists, the only action is the initiation of the ALPS circuit configuration submode.

Note that this command is used to statically create an ALPS circuit at the remote CPE. ALPS X.25 circuits (at the central CPE) are always dynamically created and are never created using this command.

Examples

The following example specifies the name of the ALPS circuit at the remote CPE as CKT1:

```
alps circuit CKT1
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps connection-type permanent

To specify that this circuit should be established when the circuit is enabled, use the **alps connection-type permanent** command in Airline Product Set (ALPS) circuit configuration submode. To remove the permanent activation behavior and return the behavior to the default dynamic activation, use the **no** form of this command.

alps connection-type permanent [*retry-timer*]

no alps connection-type permanent [*retry-timer*]

Syntax Description

retry-timer	(Optional) Specifies the maximum interval between consecutive attempts to establish a circuit in the event of a failure. The default for the retry timer is 30 seconds and the range is from 1 to 180 seconds.

Command Default

The default is 30 seconds.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that the circuit is established when enabled and that the customer premises equipment (CPE) will retry the connection every 30 seconds in the event of a failure:

```
alps connection-type permanent 30
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps default-circuit

To specify the Airline Product Set (ALPS) circuit that this agent-set control unit (ASCU) uses, use the **alps default-circuit** command in ALPS ASCU submode. To remove the default circuit specification, use the **no** form of this command.

alps default-circuit *name*

no alps default-circuit *name*

Syntax Description

name	Name given to identify an ALPS circuit on the remote customer premises equipment (CPE).

Command Default

No default behavior or values.

Command Modes

ALPS ASCU submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to specify that ALPS circuit to be used is CKT1:

```
alps default-circuit CKT1
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps enable-alarms ascu

To enable alarms for the Airline Product Set (ALPS) agent-set control unit (ASCU)s, use the **alps enable-alarms ascu** command in global configuration mode at the remote customer premises equipment (CPE). To disable alarms for the ALPS ASCUs, use the **no** form of this command.

alps enable-alarms ascu [*interface id*]

no alps enable-alarms ascu

Syntax Description

interface id	(Optional) ASCU identifier. Enable alarms for the specified ASCU.

Command Default

If no interface and interchange address combination is specified, then alarms (Syslog messages and SNMP traps) are enabled for all ALPS ASCUs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If an interface and interchange address combination is specified, then the alarms are enabled only for the ASCU matching that combination. Up to eight **alps enable-alarms ascu** commands can be entered to allow a set of ALPS ASCUs to be monitored. ALPS ASCU alarms are generated only at the remote CPE.

Examples

The following example enables alarms for ALPS ASCU 42 on serial interface 1:

```
alps enable-alarms ascu Serial1 42
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps enable-alarms circuit

To enable alarms for the Airline Product Set (ALPS) circuits, use the **alps enable-alarms circuit** command in global configuration mode. To remove the circuit definition from the configuration, use the **no** form of this command.

alps enable-alarms circuit [*name*]

no alps enable-alarms circuit [*name*]

Syntax Description

name	(Optional) Name given to identify an ALPS circuit on the remote customer premises equipment (CPE).

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a valid circuit name is specified, then the alarms are enabled only for the circuit matching the name. Up to eight **alps enable-alarms circuit** commands can be entered to allow a subset of ALPS circuits to be monitored. ALPS circuit alarms are generated at both the remote airline link control (ALC) CPE and the central (X.25) CPE.

Examples

The following example enables alarms for the ALPS circuit named CKT1:

```
alps enable alarms circuit CKT1
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps enable-alarms peer

To enable alarms for the Airline Product Set (ALPS) peers, use the **alps enable-alarms peer** command in global configuration mode. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

alps enable-alarms peer [*ip-address*]

no alps enable-alarms peer [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the remote peer for which alarms are enabled.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If an IP address is specified, then the alarms are enabled only for the remote peer matching the IP address. Up to eight **alps enable-alarms peer** commands can be entered to allow a set of ALPS peers to be monitored. ALPS peer alarms are generated at both the remote and the central customer premises equipment (CPE).

Examples

The following example enables alarms for the ALPS peer at IP address 172.22.0.91:

```
alps enable alarms peer 172.22.0.91
```

Related Commands

Command	Description
show alps peers	Displays the status of the ALPS partner peers.

alps enable-ascu

To move the previously defined agent-set control unit (ASCU) from the inactive poll list to the active poll list, use the **alps enable-ascu** command in Airline Product Set (ALPS) ASCU configuration submode. This move results in the protocol handler polling the ASCU and rendering it ready for handling terminal traffic. To remove the ASCU from the active poll list to the inactive poll list, use the **no** form of this command. This action prevents the ASCU from being polled, rendering it not ready for handling terminal traffic.

alps enable-ascu

no alps enable-ascu

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

ALPS ASCU submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example moves the ASCU to the active poll list:

```
alps enable-ascu
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps enable-circuit

To enable the circuit to be activated when data is received from an agent-set control unit (ASCU), use the **alps enable-circuit** command in Airline Product Set (ALPS) circuit configuration submode. To disable the circuit, use the **no** form of this command.

alps enable-circuit

no alps enable-circuit

Syntax Description

This command has no arguments or keywords.

Command Default

The circuit is disabled by default.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies the circuit to be activated when data is received from an ASCU:

```
alps enable-circuit
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps error-display

To specify where error messages about service availability or network problems are displayed, use the **alps error-display** command in Airline Product Set (ALPS) agent-set control unit (ASCU) configuration submode. To return to the default values, use the **no** form of this command.

alps error-display *number1 number2*

no alps error-display *number1 number2*

Syntax Description

number1	For P1024B airline link control (ALC), specifies the terminal address where these service messages are sent. Valid numbers are hexadecimal numbers in the range from 0x40 to 0x7F. The default address is 0x72. For P1024C Unisys Terminal System (UTS), specifies the screen line number where service messages are displayed. Valid numbers are hexadecimal numbers in the range from 0x00 to 0x7F. The default line number is 0x37.
number2	For P1024B ALC, specifies the screen line number where service messages are displayed. Valid numbers are hexadecimal numbers in the range from 0x40 to 0x7F. The default screen line number is 0x66. For P1024C UTS, specifies the column number where service messages are displayed. Valid numbers are hexadecimal numbers in the range from 0x00 to 0x7F. The default column number is 0x20.

Command Default

The default terminal address for P1024B ALC is 0x72.
The default screen line for P1024B ALC is 0x20.
The default line number for P1024C UTS is 0x37.
The default column number for P1024C UTS is 0x20.

Command Modes

ALPS ASCU submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that error messages are displayed at terminal address 6d, on screen line number 78:

```
alps error-display 6d 78
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps host-hld host-link

To enable Airline Product Set (ALPS) on the X.25 interface, use the **alps host-hld host-link** command in interface configuration mode. To disable ALPS on the X.25 interface, use the **no** form of this command.

alps host-hld *hld* **host-link** *number* {**ax25** [**damp-tmr** *value*] | **emtox** *x.121* [*pseudo-conv*]}
[**life-tmr** *value*] [**reply-tmr** *value*]

no alps host-hld *hld* **host-link** *number* {{**ax25** [**damp-tmr** *value*]} | {**emtox** *x.121* [*pseudo-conv*]}}
[**life-tmr** *value*] [**reply-tmr** *value*]

Syntax Description

hld	Host high-level designator. A hexadecimal number in the range from 1 to 7f7f.
number	Host-link identifier. A number in the range from 1 to 255.
ax25	Specifies airline X.25 implementation of X.25.
damp-tmr *value*	(Optional) Specifies the AX.25 permanent virtual circuit (PVC) damping timer. The *value* argument is the length of time that a PVC can be inactive before it is destroyed and the corresponding ALPS circuits are closed. The default is 10 seconds.
emtox	Specifies EMTOX implementation of X.25.
x.121	X.121 address of the EMTOX host (called address on calls to the EMTOX host).
pseudo-conv	(Optional) Specifies the pseudo-conversational format of EMTOX packets.
life-tmr *value*	(Optional) Specifies the maximum amount of time (in seconds) that a message may be queued for sending to the host X.25 system before it is discarded. The *value* argument is time (in seconds).
reply-tmr *value*	(Optional) Specifies the duration of the no-reply timer. If the X.2 line is idle for this duration, and the X.25 transmit window is full, then ALPS sends an X.25 reset message on the virtual circuit to reset the transmit/receive windows. The no-reply timer can be configured for 10 to 600 seconds.

Command Default

The default damping timer value is 10 seconds.
The default no-reply timer value is 60 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enable ALPS on the X.25 interface:

```
alps host-hld 1 host-link 1 emtox
```

alps hostlink

To specify information required to establish an X.25 virtual circuit at the central customer premises equipment (CPE), use the **alps hostlink** command in Airline Product Set (ALPS) circuit configuration submode. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

alps hostlink *number* {**ax25** *lcn* | **emtox** *x121-address*} [**winout** *val1*] [**winin** *val2*] [**ops** *val3*] [**ips** *val4*]

no alps hostlink *number* {**ax25** *lcn* | **emtox** *x121-address*} [**winout** *val1*] [**winin** *val2*] [**ops** *val3*] [**ips** *val4*]

Syntax Description

number	Interface at the host CPE. Decimal number in the range from 1 to 255.
ax25	Specifies airline X.25 implementation of X.25.
lcn	Local channel number for AX.25 connections.
emtox	Specifies EMTOX implementation of X.25.
x121-address	X.121 address for EMTOX connections. This is the X.121 calling address for X.25 call packets sent from the central CPE to the EMTOX host. This address is the source address in a call to the host.
winout *val1*	(Optional) Specifies the X.25 send window The *val1* argument is a decimal number in the range from 1 to 7.
winin *val2*	(Optional) Specifies the X.25 receive window. The *val2* argument is a decimal number in the range from 1 to 7.
ops *val3*	(Optional) Specifies the maximum output packet size. The *val3* argument is one of the following numbers: 128, 240, 256, 512, 1024, 2048, or 4096.
ips *val4*	(Optional) Specifies the maximum input packet size. The *val4* argument is one of the following numbers: 128, 240, 256, 512, 1024, 2048, or 4096.

Command Default

If no values are specified, the default values at the X.25-attached central CPE are used.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example establishes an X.25 virtual circuit at the central CPE. The configuration specifies airline X.25 implementation. The host CPE interface is 3, the local channel number for airline X.25 connections is 120, and the X.25 send window is 3.

```
alps hostlink 3 ax25 120 winout 3 winin 3
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

alps idle-timer

To specify (for dynamic circuits) the length of time that can elapse before an idle circuit is disabled, use the **alps idle-timer** command in Airline Product Set (ALPS) circuit configuration submode. To return to the default idle-timer value, use the **no** form of this command.

alps idle-timer *timer*

no alps idle-timer *timer*

Syntax Description

timer	Length of time that can elapse before an idle circuit is brought down. The range is from 10 to 600 seconds. The default is 60 seconds.

Command Default

The default length of time that can elapse before an idle circuit is brought down is 60 seconds.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that an idle circuit is maintained for 90 seconds before it is disabled:

```
alps idle-timer 90
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

alps keepalive

To enable TCP keepalives for Airline Product Set (ALPS) TCP peer connections, use the **alps keepalive** command in global configuration mode. A TCP keepalive request will be sent to the remote peer if the TCP connection to the remote peer is silent for a time period larger than the interval specified. The TCP connection to the ALPS host will be closed when a count equal to the retry count specified is missed consecutively. To disable keepalives for ALPS, use the **no** form of this command.

alps keepalive [**interval** *time*] [**retry** *count*]

no alps keepalive [**interval** *time*] [**retry** *count*]

Syntax Description

interval *time*	(Optional) Interval for keepalive requests. The *time* argument is the keepalive interval, in the range from 10 to 300 seconds. The default is 30 seconds.
retry *count*	(Optional) Indicates how many times keepalive requests will be sent before the connection is closed. The *count* argument is the retry count, in the range from 1 to 10. The default is three retries.

Command Default

The default keepalive interval is 30 seconds.
The default retry count is 3.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that a TCP keepalive request will be sent to the remote peer if the TCP peer connection is idle for 60 seconds. The connection will be closed after three consecutive keepalive requests are sent.

```
alps keepalive interval 60 retry 8
```

Related Commands

Command	Description
alps local-peer	Specifies the IP address of the local peer.

alps lifetime-timer

To specify how long messages can be queued in the Airline Product Set (ALPS) circuit queue awaiting transmission to the central customer premises equipment (CPE), use the **alps lifetime-timer** command in ALPS circuit configuration submode. To return to the default lifetime-timer value, use the **no** form of this command.

alps lifetime-timer *timer*

no alps lifetime-timer *timer*

Syntax Description

timer	Length of time, in seconds, that a message can be queued. The range is from 1 to 20 seconds. The default is 4 seconds.

Command Default

The default length of time that a message can be queued in the ALPS circuit queue is 4 seconds.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Messages that exceed the timer limit are discarded.

Examples

The following example specifies that a message remains in the ALPS circuit queue for no longer than 3 seconds:

```
alps lifetime-timer 3
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

alps local-hld remote-hld

To specify the local and remote high-level designator (HLD)s to use for this Airline Product Set (ALPS) circuit, use the **alps local-hld remote-hld** command in ALPS circuit configuration submode. To remove the definition from the configuration, use the **no** form of this command.

alps local-hld *loc-hld* **remote-hld** *rem-hld*

no alps local-hld *loc-hld* **remote-hld** *rem-hld*

Syntax Description

loc-hld	Local HLD to use for ALPS circuit. Hexadecimal number in the range from 1 to FFFF.
rem-hld	Remote HLD to use for ALPS circuit. Hexadecimal number in the range from 1 to FFFF.

Command Default

No default behavior or values.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(5)T	This command was modified and the **remote-hld** keyword was not applicable for mapping of airline traffic over IP (MATIP).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **remote-hld** keyword is not applicable for ALPS with MATIP.

Examples

The following example specifies the local HLD as 4B10:

```
alps local-hld 4B10
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive airline link control (ALC) ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

alps local-peer

To specify the IP address of the local peer, use the **alps local-peer** command in global configuration mode. To remove all subsequent Airline Product Set (ALPS) configuration commands from the device, use the **no** form of this command.

alps local-peer *ip-address* [**promiscuous**]

no alps local-peer *ip-address* [**promiscuous**]

Syntax Description

ip-address	IP address of the local peer.
promiscuous	(Optional) Keyword specified at the central customer premises equipment (CPE) to accept incoming TCP connections from any remote customer premises equipment (CPE).

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies the local peer IP address as 172.22.0.91 and specifies that the CPE accepts incoming TCP connections from any CPE:

```
alps local-peer 172.22.0.91 promiscuous
```

Related Commands

Command	Description
show alps peers	Displays the status of the ALPS partner peers.

alps matip-close-delay

To specify the interval between the closing and reopening of mapping of airline traffic over IP (MATIP) circuit connections, use the **alps matip-close-delay** command in Airline Product Set (ALPS) circuit configuration submode circuit submode command. To restore the definition to the default value, use the **no** form of this command.

alps matip-close-delay *time*

no alps matip-close-delay *time*

Syntax Description

time	Minimum number of seconds between the closing and reopening of an ALPS MATIP circuit. The range is from 1 to 90 seconds. The default is 10 seconds.

Command Default

The default value is 10 seconds.

Command Modes

ALPS circuit submode

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies a close delay time of 20 seconds:

```
alps matip-close-delay 20
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps max-msg-length

To specify maximum input message length, use the **alps max-msg-length** command in Airline Product Set (ALPS) agent-set control unit (ASCU) configuration submode. To return to the default maximum input message length, use the **no** form of this command.

alps max-msg-length *value*

no alps max-msg-length *value*

Syntax Description

value	Maximum input message length. The range is from 1 to 3840. The default is 962 characters.

Command Default

The default maximum input message length is 962 characters.

Command Modes

ALPS ASCU submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that the maximum length of a message is 1000 characters:

```
alps max-msg-length 1000
```

alps mpx

To specify the multiplexing and the agent-set control unit (ASCU) identification header for this circuit, use the **alps mpx** command in Airline Product Set (ALPS) ASCU configuration submode. To remove the definition from the configuration, use the **no** form of this command.

alps mpx {**group** | **single**} **hdr** {**a1a2** | **none**}

no alps mpx {**group** | **single**} **hdr** {**a1a2** | **none**}

Syntax Description

group	Specifies that multiple ASCUs will be multiplexed on the ALPS circuit. This setting is the default.
single	Specifies that only one ASCU will use this circuit.
hdr	Specifies the ASCU identification header for the circuit. The default is a1a2.
a1a2	ASCU identification via A1, A2.
none	No ASCU identification.

Command Default

The default for multiplexing is **group**.

The default header is a1a2.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(1)	This command was available for general release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **alps mpx group** command is specified, multiple ASCUs will be multiplexed on this ALPS circuit and the **none** option is not applicable. If the **alps mpx single** command is specified, then only one ASCU uses this ALPS circuit. If **alps mpx single hdr none** command is specified, the A1 and A2 ASCU identification information is not added to the front of data frames sent across this circuit, and it is assumed that it does not exist in frames received on this circuit. The exclusion of ASCU identification should be specified only when the EMTOX protocol is used.

Examples

The following example shows how to specify the multiplexing and the ASCU identification header:

```
alps mpx group hdr a1a2
```

alps n1

To specify the threshold of consecutive errors logged before an agent-set control unit (ASCU) is declared down, use the **alps n1** command in interface configuration mode. To reassert the default number of consecutive errors before declaring an ASCU down, use the **no** form of this command.

alps n1 *errors*

no alps n1 *errors*

Syntax Description

errors	Error count limit. The valid range is from 1 to 30 errors. The default for airline link control (ALC) is 30 errors. The default for Unisys Terminal System (UTS) is 10 errors.

Command Default

The default ALC error count is 30 errors.

The default UTS error count is 10 errors.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(2)T	The error ranges were modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The error count limit is a threshold value. If the ASCU state is UP and the error count threshold is exceeded, the ASCU state changes to DOWN and it is moved to the inactive poll. If alarms are enabled for the ASCU, a Syslog message is displayed and an Simple Network Management Protocol (SNMP) notification is sent to the SNMP network management station.

Examples

The following example specifies that an ASCU is declared down when the error count exceeds one:

```
alps n1 1
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps n2

To specify the number of polls that must be correctly replied to before an agent-set control unit (ASCU) is declared up, use the **alps n2** command in interface configuration mode. To reassert the default number of polls that must be correctly replied to before an ASCU is declared up, use the **no** form of this command.

alps n2 *polls*

no alps n2 *polls*

Syntax Description

polls	Number of polls that must be correctly replied to. The valid range is from 1 to 30 polls. The default is 1 poll.

Command Default

The default number of polls that must be correctly replied to is one.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the ASCU state is DOWN and the reply threshold is exceeded, the ASCU state changes to UP and the ASCU is moved to the active poll list. If alarms are enabled for the ASCU, a Syslog message is displayed and an Simple Network Management Protocol (SNMP) notification is sent to the SNMP management station.

Examples

The following example specifies that two polls must be correctly replied to before the ASCU is declared up:

```
alps n2 2
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
encapsulation uts	Specifies that the P1024C Universal Terminal Support (UTS) protocol will be used on the serial interface.

alps n3

To specify the maximum number of retransmissions of an unacknowledged output data message to an agent-set control unit (ASCU), use the **alps n3** command in interface configuration mode. To reassert the default, use the **no** form of this command.

alps n3 *value*

no alps n3 *value*

Syntax Description

value	Maximum number of times an unacknowledged output data message can be re-sent. When the number is exceeded, the output data message is dropped. The valid range is from 1 to 10 resends. The default is 3 resends.

Command Default

The default number of resends is three.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on 1026C interfaces.

Examples

The following example specifies that 6 is the maximum number of resends of an unacknowledged output data message to an ASCU:

```
alps n3 6
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
show alps ascu	Displays the status of the ALPS ASCU.

alps poll-pause

To set the minimum interval, in milliseconds, between two polls to the same agent-set control unit (ASCU), use the **alps poll-pause** command in interface configuration mode. To the default interval, use the **no** form of this command to revert.

alps poll-pause *milliseconds*

no alps poll-pause

Syntax Description

milliseconds	Minimum interval between polls, in milliseconds (ms). The valid range is from 10 to 1000 ms. The default interval is 50 ms.

Command Default

The default minimum interval is 50 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets a 200-ms minimum interval between polls:

```
alps poll-pause 200
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.

alps primary-peer

To specify the primary TCP peer and, optionally, a backup TCP peer for an Airline Product Set (ALPS) circuit, use the **alps primary-peer** command in ALPS circuit configuration submode. To remove the definition from the configuration, use the **no** form of this command.

alps primary-peer *ip-address* [**backup-peer** *ip-address*]

no alps primary-peer *ip-address* [**backup-peer** *ip-address*]

Syntax Description

ip-address	IP address specified in the **alps remote-peer** command.
backup-peer	(Optional) Backup TCP peer for the ALPS circuit.
ip-address	(Optional) IP address specified in the **alps remote-peer** command.

Command Default

No default behavior or values.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies a primary peer at IP address 172.22.0.91 and a backup peer at IP address 172.22.0.92:

```
alps primary-peer 172.22.0.91 backup-peer 172.22.0.92
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive airline link control (ALC) ASCU in the DOWN state.
show alps peers	Displays the status of the ALPS partner peers.

alps remote-peer

To specify the partner IP address for an Airline Product Set (ALPS) circuit, use the **alps remote-peer** command in global configuration mode. To remove the definition from the configuration, use the **no** form of this command.

alps remote-peer *ip-address* [**protocol** {**atp** | **matip**-**a**}] [**status-interval** *interval*] [**status-retry** *retries*] [**dynamic** [*inact-timer*] [**no-circuit** *no-circ-timer*]] [**tcp-qlen** [*number*]]

no alps remote-peer *ip-address* [**protocol** {*atp* | *matip-a*}] [**status-interval** *interval*] [**status-retry** *retries*] [**dynamic** [*inact-timer*] [**no-circuit** *no-circ-timer*]] [**tcp-qlen** [*number*]]

Syntax Description

ip-address	IP address of the peer.
protocol {**atp** | **matip**-**a**}	(Optional) Specifies the type of encapsulation for the connection. The following options are available: • ALPS Tunneling Protocol encapsulation. This encapsulation is the default. • mapping of airline traffic over IP (MATIP) Type A (conversational) encapsulation.
status-interval *interval*	(Optional) Specifies amount of time, in seconds, between sending of MATIP status messages. The messages verify the integrity of the TCP connection. Number of seconds between status messages. The range is from 0 to 300 seconds. The default value is 0 (off).
status-retry *retries*	(Optional) Specifies number of times to retry sending a MATIP status message before the peer connection is closed. Number of retries. The range is from 0 to 100 retries. The default value is 2.
dynamic *inact-timer*	(Optional) Allows the TCP connection to the host peer to be opened only when there is data to be transferred to the host reservation system. Length of inactivity, in seconds, after which the connection is closed. The range is from 0 to 300 seconds. The default is 30 seconds. A value of zero indicates that the timer is disabled.
no-circuit *no-circ-timer*	(Optional) Specifies amount of time, in seconds, that a peer will stay connected while no circuits are using the peer connection. This parameter is valid only if the dynamic parameter is first configured. Number of seconds before which the timer will expire. The range is from 0 to 3600 seconds. The default is 90 seconds.
tcp-qlen *number*	(Optional) Specifies the maximum length of a TCP queue for peer connections. Number of packets allowed in the TCP queue. The range is from 26 to 100 packets. The default is 50 packets.

Command Default

The default for the **status-interval** argument is 0 (off).
The default for the **status-retry** argument is 2.
The default for the **dynamic** argument is 30 seconds.
The default for the **no-circuit** argument is 90 seconds.
The default for the **tcp-qlen** argument is 50 packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(5)T	The **protocol**, **status-interval**, **status-retry** and the **no-circuit** keyword options were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the protocol option is configured for MATIP, the peer connection is dynamic.

When the protocol option is configured for ALPS Tunneling Protocol (ATP), the peer connection is permanent.

The **no-circuit** option within the dynamic keyword does not apply to permanent airline link control (ALC)/Universal Terminal Support (UTS) connections.

The **status-interval** and **status-retry** options apply only to the MATIP protocol.

Issuing the **no alps remote-peer** command does the following:

- Closes TCP connection.
- Notifies the partner TCP peer that this connection is closed.

Notifies the ALPS circuits using this TCP peer that the connection is closed.

Examples

The following example specifies a MATIP peer connection at IP address 10.22.0.92. Status messages will be sent every 9 seconds and will be resent twice before the connection is closed. The maximum TCP length is 30:

```
alps remote-peer 10.22.0.92 protocol matip-a status-interval 9 status-retry 2 tcp-qlen 30
```

Related Commands

Command	Description
alps local-peer	Specifies the IP address of the local peer.
show alps peers	Displays the status of the ALPS partner peers.

alps retry-option

To configure the customer premises equipment (CPE) to signal the agent-set control unit (ASCU) whenever an error is detected, use the **alps retry-option** command in Airline Product Set (ALPS) ASCU configuration submode. To reassert the default action of no retry, use the **no** form of this command.

alps retry-option {**resend** | **reenter**}

no alps retry-option

Syntax Description

resend	Specifies the retry option as resend. This option causes an indicator LED to signal the operator at the ASCU to resend data.
reenter	Specifies the retry option as reenter. This option causes a service message to signal the operator at the ASCU to reenter data.

Command Default

The default retry option is no retry.

Command Modes

ALPS ASCU submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is applicable only for P1024B automatic level control (ALC) interfaces; it is invalid on P1024C Unisys Terminal System (UTS) interfaces.

Examples

The following example specifies that an indicator LED signals the ASCU to resend data:

```
alps retry-option resend
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps service-msg data-drop

To specify where to retrieve the terminal address to be used when a service message is sent to an agent-set control unit (ASCU) as the result of a dropped data message, use the **alps service-msg data-drop** command in interface configuration mode. To remove the terminal address specification, use the **no** form of this command.

alps service-msg data-drop {**msg-term** | **config-term**}

no alps service-msg data-drop {**msg-term** | **config-term**}

Syntax Description

msg-term	Specifies that the service message will be sent to the terminal address of the dropped message.
config-term	Specifies that the service message terminal address is the same address configured in the **alps-error display** command.

Command Default

The **config-term option** is the default.
If this command is not configured and a data message is dropped from a terminal, the resulting service message is sent to the terminal specified in the **alps error-display** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to serial interfaces configured with airline link control (ALC) encapsulation only.

Examples

The following example specifies that service messages resulting from dropped data messages are sent to the terminal address of the dropped message:

```
alps service-msg data-drop msg-term
```

Related Commands

Command	Description
alps error-display	Specifies where error messages about service availability or network problems are displayed.
encapsulation alc	Specifies that the P1024B ALC protocol is used on the serial interface.

alps service-msg format

To specify the protocol format of service messages sent from the device to an agent-set control unit (ASCU), use the **alps service-msg format** command in interface configuration mode. To remove the protocol format specification, use the **no** form of this command.

alps service-msg format {**sita** | **apollo**}

no alps service-msg format {**sita** | **apollo**}

Syntax Description

sita	Specifies the sita protocol format.
apollo	Specifies the apollo protocol format.

Command Default

The default protocol format is **sita**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to serial interfaces configured with automatic level control (ALC) encapsulation only.

Examples

The following example specifies the apollo protocol format:

```
alps service-msg format apollo
```

Related Commands

Command	Description
encapsulation alc	Specifies that the P1024B airline link control (ALC) protocol is used on the serial interface.

alps service-msg status-change

To specify that service messages for Airline Product Set (ALPS) circuit status changes be sent to agent-set control unit (ASCU)s on the serial interface, use the **alps service-msg status-change** command in interface configuration mode. To send service messages for ALPS circuit status changes only when airline link control (ALC) data messages are dropped, use the **no** form of this command.

alps service-msg status-change

no alps service-msg status-change

Syntax Description

This command has no arguments or keywords.

Command Default

The default is on. Unless the **no** form of this command is configured, unsolicited service messages are sent to all ASCUs multiplexed on the mapping of airline traffic over IP (MATIP) session when the following ALPS circuit events occur:

- MATIP session status change
- ASCU status change

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to serial interfaces configured with ALC encapsulation only.

If the **no** form of this command is configured, service messages for ALPS circuit status changes are sent only when airline link control (ALC) data messages are dropped.

Examples

The following example specifies that unsolicited service messages resulting from ALPS circuit status changes be sent to ASCUs on the serial interface:

```
alps service-msg status-change
```

Related Commands

Command	Description
encapsulation alc	Specifies that the P1024B ALC protocol is used on the serial interface.

alps service-msg-interval

To specify the interval between consecutive transmissions of service messages from the remote customer premises equipment (CPE) to the agent-set control unit (ASCU), use the **alps service-msg-interval** command in Airline Product Set (ALPS) circuit configuration submode. To remove the definition from the configuration, use the **no** form of this command.

alps service-msg-interval *seconds*

no alps service-msg-interval *seconds*

Syntax Description

seconds	Interval, in seconds, between consecutive sendings of service messages from the remote CPE to the ASCU. The range is from 1 to 20 seconds. The default interval is 4 seconds.

Command Default

The default interval between consecutive sendings of service messages from the remote CPE to the ASCU is 4 seconds.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The “PLEASE RETRY” message is sent only to ASCUs that use circuits with a dynamic connection type.

Examples

The following example specifies an interval of 3 seconds between sending service messages from the CPE to the ASCU:

```
alps service-msg-interval 3
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
alps service-msg-list	Defines the service message list to be used for this circuit.

alps service-msg-list

To define the service message list to be used for this circuit, use the **alps service-msg-list** command in Airline Product Set (ALPS) circuit configuration submode. To remove the list from the circuit configuration, thus issuing no service messages until another list is configured, use the **no** form of this command.

alps service-msg-list *list*

no alps service-msg-list *list*

Syntax Description

list	The service message list to be used for this circuit. The valid numbers are from 1 to 8.

Command Default

No default behavior or values.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that message list 1 is used for this circuit:

```
alps service-msg-list 1
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive airline link control (ALC) ASCU in the DOWN state.
alps service-msg-interval	Specifies the interval between consecutive transmissions of service messages from the remote CPE to the agent-set control unit (ASCU).

alps service-msg-list number

To define the service message identity and its contents for a service message list, use the **alps service-msg-list number** command in global configuration mode. To remove a service message number from the service message list configuration, use the **no** form of this command.

alps service-msg-list *list* **number** *number message*

no alps service-msg-list *list* **number** *number message*

Syntax Description

list	Service message list to be used for this circuit. Valid numbers are from 1 to 8.
number	List number. Valid numbers are from 1 to 8.
message	Contents of a service message. Maximum number of characters allowed in a service message is 32. **Note** Configuring the *message* argument with a value of $OFF$ disables this particular service message.

Command Default

The default service message is used if no service message list number is specified.

Table 9 shows the default service message text strings.

Table 9 Service Message Default Text Strings

Message Number	Event	Text String
1	ALPS circuit to host is opened.	CONNECTION UP
2	X.25 virtual circuit at the host is cleared.	DISC BY THE HOST
3	X.25 interface at the host is down.	HOST ISOLATED
4	No response from the host device when trying to establish a connection.	NETWORK PROBLEM
5	Connection to host was disconnected because of inactivity.	READY TO CONNECT
6	Network is congested.	CONGESTION
7	Network congestion has cleared.	PLEASE PROCEED
8	Network operator has disabled the path to the host.	DISC BY NET OPERAT

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.1(2)T	The OFF option was added to the *message* argument and the maximum service message length was increased to 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To disable a particular service message, configure the *message* argument with a value of OFF.

Examples

The following example specifies the text of message list 1, message number 2:

```
alps service-msg-list 1 number 2 "Turn off the terminal NOW."
```

The following example disables service message 3 from list 1:

```
alps service-msg-list 1 number 3 $OFF$
```

Related Commands

Command	Description
alps service-msg list	Defines the service message list to be used for this circuit.

alps servlim

To specify the number of polls of the agent-set control unit (ASCU) UP list allowed between two successive polls of the ASCU DOWN list, use the **alps servlim** command in interface configuration mode. To reassert the default number of cycles through the normal (active) poll list allowed before the slow poll list is processed, use the **no** form of this command.

alps servlim *polls*

no alps servlim *polls*

Syntax Description

polls	Number of polls of the ASCU UP list. The valid range is from 1 to 512 polls. The default is 30 polls.

Command Default

The default number of polls of the ASCU UP list allowed between two successive polls of the ASCU DOWN list is 30 polls.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that five polls of the ASCU UP list are allowed between two successive polls of the ASCU DOWN list.

```
alps servlim 5
```

Related Commands

Command	Description
alps n1	Specifies the threshold of consecutive errors logged before an ASCU is declared down.
alps n2	Specifies the number of polls that must be correctly replied to before an ASCU is declared up.
alps t1	Specifies the timeout delay between polling and response.
alps t2	Specifies the timeout delay between receipt of the first character of an IP sequence solicited by a poll and receipt of a GA sequence.

alps t1

To specify the timeout delay between polling and response, use the **alps t1** command in interface configuration mode. To reassert the default poll timeout value of 0.5 seconds, use the **no** form of this command.

alps t1 *delay*

no alps t1 *delay*

Syntax Description

delay	Timeout delay, in seconds, between polling and response. The valid range is from 1 to 20-tenths of a second (0.1 to 2 seconds). The default is 5-tenths of a second (0.5 second).

Command Default

The default timeout delay between polling and response is 5-tenths of a second (0.5 second).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.1(2)T	The range for the timeout delay was extended.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies a 0.5-second timeout delay between polling and response:

```
alps t1 5
```

Related Commands

Command	Description
alps n1	Specifies the threshold of consecutive errors logged before an agent-set control unit (ASCU) is declared down.
alps n2	Specifies the number of polls that must be correctly replied to before an ASCU is declared up.
alps servlim	Specifies the number of polls of the ASCU UP list allowed between two successive polls of the ASCU DOWN list.
alps t2	Specifies the timeout delay between receipt of the first character of an IP sequence solicited by a poll and receipt of a Go Ahead (GA) sequence.

Command	Description
encapsulation alc	Specifies that the P1024B airline link control (ALC) protocol is used on the serial interface.
encapsulation uts	Specifies that the P1024C UTS protocol is used on the serial interface.

alps t2

To specify the timeout delay between receipt of the first character of an I/P sequence solicited by a poll and receipt of a Go Ahead (GA) sequence, use the **alps t2** command in interface configuration mode. To reassert the default timeout value of 6 seconds, use the **no** form of this command.

alps t2 *delay*

no alps t2 *delay*

Syntax Description

delay	Timeout delay, in seconds, between receipt of first character of an I/P sequence solicited by a poll and receipt of GA sequence. The valid range is from 1 to 10 seconds. The default is 6 seconds.

Command Default

The default timeout delay between receipt of first character of an I/P sequence solicited by a poll and receipt of GA sequence is 6 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies a timeout delay of 8 seconds between receipt of the first character of an I/P sequence solicited by a poll and receipt of a GA sequence:

```
alps t2 8
```

Related Commands

Command	Description
alps n1	Specifies the threshold of consecutive errors logged before an agent-set control unit (ASCU) is declared down.
alps n2	Specifies the number of polls that must be correctly replied to before an ASCU is declared up.
alps servlim	Specifies the number of polls of the ASCU UP list allowed between two successive polls of the ASCU DOWN list.
alps t1	Specifies the timeout delay between polling and response.

alps translate

To map an X.121 address to an IP address of a remote peer, use the **alps translate** command in interface configuration mode. To remove mapping from the configuration, use the **no** form of this command.

alps translate *x.121-address ip-address*

no alps translate *x.121-address ip-address*

Syntax Description

x.121-address	X.121 address to be mapped to an IP address of a remote peer.
ip-address	IP address of the remote peer.

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The X.121 address is compared to the Called Address on inbound X.25 call packets to determine if the call should be accepted. The X.121 address may have an asterisk (*) at the end to indicate “all X.121 addresses prefixed with the address before the *.”

Examples

The following example maps all X.121 addresses prefixed with the address 88845 to the remote peer IP address 172.22.0.90:

```
alps translate 88845* 172.22.0.90
```

Related Commands

Command	Description
encapsulation x25	Specifies operation of a serial interface as an X.25 device.

alps update-circuit

To update one or more Airline Product Set (ALPS) circuits, use the **alps update-circuit** command in user EXEC or privileged EXEC mode. If a circuit name is specified, then only that circuit will be updated; otherwise, all circuits will be updated.

alps update-circuit [*name*]

Syntax Description

name	(Optional) Specifies name of the circuit to update.

Command Default

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **alps update-circuit** command is issued for a circuit that is using the ALPS Tunneling Protocol (ATP) protocol, the circuit will be closed and reopened.

If the **alps update-circuit** command is issued for a circuit that is using the mapping of airline traffic over IP (MATIP) protocol, a configuration update will be sent in the form of a MATIP Session Open command.

The **alps update-circuit** command is effective only for ALPS circuits that are enabled and active (opening or opened state).

There is not a **no** form for this command.

Examples

The following example specifies that circuit 1 has been updated:

```
Device# alps update-circuit CKT-1
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive airline link control (ALC) agent-set control unit (ASCU) in the DOWN state.

Command	Description
alps enable-circuit	Enables the circuit to be activated when data is received from an ASCU.
show alps circuits	Displays the status of the ALPS circuits.

asp addr-offset

To configure an asynchronous port to send and receive polled asynchronous traffic through a block serial tunnel (BSTUN), use the **asp addr-offset** command in interface configuration mode. To disable the traffic flow through a BSTUN, use the **no** form of this command.

asp addr-offset *address-offset*

no asp addr-offset

Syntax Description

address-offset	Location of the address byte within the polled asynchronous frame being received. The range is from 0 to 255. The default value is 0.

Command Default

No polled asynhronous protocol group is defined within the frame of the address byte.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **asp addr-offset** *address-offset* command to specify the offset from the start of the frame where the address byte is located. This command is applicable only when the asynchronous-generic protocol is specified on an interface using a combination of the **bstun protocol-group** command in global configuration mode and the **bstun group** command in interface configuration mode.

Interfaces configured to run the asynchronous-generic protocol have the following configuration:

- baud rate set to 9600 bps
- 8 data bits
- no parity
- 1 start bit
- 1 stop bit

If different line configurations are required, use the **rxspeed** command, **txspeed** command, **databits** command, **stopbits** command, and **parity line** command in the global configuration mode to change the line attributes. The addresses of the alarm panels must be used in the address field of the **bstun route address** command in the interface configuration mode

Examples

The following example shows that the fifth byte in the polled asynchronous frame contains the device address:

```
Device(config)# interface Serial 3/0
Device(config-if)# physical-layer async
Device(config-if)# encapsulation bstun
Device(config-if)# asp addr-offset 5
Device(config-if)# end
```

Related Commands

Command	Description
asp role	Specifies whether the device is acting as the primary end of the polled asynchronous link or the secondary end of the polled asynchronous link connected to the serial interface, and whether the attached remote device is a security alarm control station.
asp rx-ift	Specifies a time period that, by expiring, signals the end of one frame being received and the start of the next.
bstun group	Specifies the BSTUN group to which the interface belongs.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

asp broadcast-addr

To specify the address byte that asynchronous serial protocols (ASP) use to broadcast packets from their remote stations, use the **asp broadcast-addr** command in interface configuration mode. To disable asynchronous broadcast, use the **no** form of this command.

asp broadcast-addr *address*

no asp broadcast-addr

Syntax Description

address	Broadcast address in hexadecimal format. The range is from 0 to 0xff.

Command Default

No broadcast address is defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(3)T	This command was modified. Support was extended to enable the ASP broadcast mask to transmit packets as broadcasts.

Usage Guidelines

Use the **asp broadcast-addr** command to specify the address byte that Asynchronous Serial Protocols (ASP) use to broadcast packets. All packets that are to be broadcast are copied and sent to all peers defined on the serial interface. The broadcast addresses identify the packets transmitted to all remote devices in the same Block Serial Tunnel (BSTUN) group.

For example, the address values configured using the **bstun route** command can be 01, 02, 03, and so on. If the address value is configured using the **asp broadcast-addr ff** command, the packets received are considered as a broadcast. These packets are transmitted to all remote devices in that BSTUN group.

Note A broadcast-mask value of ff identifies all packets as broadcasts. Therefore, all address bytes in the range 0x00 to 0xff are classified as broadcasts.

Examples

The following example shows how to configure an asynchronous broadcast address using the address ff:

```
Device(config)# interface Serial 3/0
Device(config-if)# asp broadcast-addr ff
Device(config-if)# end
```

Related Commands

Command	Description
asp eof-char	Specifies an EOF character for the asynchronous generic application that is used to end ASP transmissions.
asp ignore-sequence-number	Instructs a device to ignore the ASP sequence numbers that are used to synchronize ASP traffic between head-end and tail-end devices.
asp sof-char	Specifies an SOF character for the asynchronous generic application.
brdcast-address-mask	Allows the configuration of multiple address masks.

asp brdcast-address-mask

To specify the bit or bits in the address byte that the asynchronous serial protocols (ASP) use to broadcast packets from their remote stations, use the **asp brdcast-address-mask** command in interface configuration mode. To disable the bit or bits in the address byte that the ASP uses to broadcast packets, use the **no** form of this command.

asp brdcast-address-mask *address*

no asp brdcast-address-mask

Syntax Description

address	Broadcast address in hexadecimal format. The range is from 0 to 0xff.

Command Default

No address masks are configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(3)T	This command was modified. Support was extended to enable the ASP broadcast mask to transmit packets as broadcasts.

Usage Guidelines

This command will force the ASP to take an ASP asynchronous character and mask it to check if it is a valid broadcast address mask. The broadcast address mask is predetermined; for example, you can set up your network such that any address above 0x7f is a broadcast address mask. Broadcast addresses identify packets that are transmitted to all remote devices in the same block serial tunnel (BSTUN) group.

For example, use the **asp brdcast-address-mask 80** command to set up the network such that any address beyond 0x7f is a broadcast address. The broadcast address is logically anded with the address byte. If the resulting value is not zero, the address is considered as a broadcast.

Note A broadcast-mask value of 0xff identifies all packets as broadcasts. Therefore, all address bytes in the range 0x00 to 0xff are classified as broadcasts.

Examples

The following example shows the configuration of ASP address broadcast mask 30 on the Serial interface:

```
Device(config)# interface Serial 0/0
Device(config-if)# asp brdcast-address-mask 30
Device(config-if)# end
```

Related Commands

Command	Description
asp addr-offset	Configures an asynchronous port to send and receive polled asynchronous traffic through a BSTUN.
asp broadcast-addr	Specifies the address that an asynchronous generic application uses to broadcast packets from its remote stations.
asp role	Allows configuration of multiple address masks.

asp dcd always

To specify that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when the serial interface starts, use the **asp dcd always** command in interface configuration mode. To specify that DSR and DCD are to be asserted when the HAYES AT connect message is sent to the point of sale (POS) device, use the **no** form of this command.

asp dcd always

no asp dcd always

Syntax Description

This command has no arguments or keywords.

Command Default

The **asp dcd always** command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For APOS, the device always functions as the DCE. If the **asp dcd always** command is enabled, then both DSR and DCD will be asserted when the serial interface is started.

If the **asp dcd always** command is disabled, then DSR and DCD are asserted when the HAYES AT connect message is sent to the POS device. When the connection to the POS device is terminated, DSR and DCD are de-asserted.

Some POS devices require that the DSR and DCD work independently, and that DSR be asserted when the serial interface starts and DCD be asserted when the connect message is sent. This requires a modified cable to disconnect the DTR and DSR connection in both directions, and on the DB25 side of the connector tying the DTE's output DTR to the DTE's input DSR.

If the **asp dcd always** command is disabled, then DSR and DCD are asserted when the HAYES AT connect message is sent to the POS device. When the connection to the POS device is terminated, DSR and DCD are de-asserted. For devices using modified cables that require that DCD be asserted only where there is a connection to the host, the **asp dcd always** command should be disabled.

Examples

The following example configures the **asp dcd always** command:

```
asp dcd always
```

Related Commands

Command	Description
asp direct	Disables dial mode and automatically activate the peer connection.
asp enq	Configures how the device sends ENQ(0x05) messages to the terminal.
asp retries	Specifies the number of times a packet will be resent before the connection with the terminal is disconnected.
asp send ack	Enables the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests.
asp timer	Customizes the ASP timers.

asp direct

To disable dial mode and automatically activate the peer connection, use the **asp direct** command in interface configuration mode. To enable dial mode, use the **no** form of this command.

asp direct

no asp direct

Syntax Description

This command has no arguments or keywords.

Command Default

The **asp direct** command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **asp direct** command is enabled, the connect timer is used to reactivate the connection if the peer connection goes down.

Examples

The following example configures the **asp direct** command:

```
asp direct
```

Related Commands

Command	Description
asp dcd always	Specifies that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when traffic starts to the serial interface.
asp enq	Configures how the device sends ENQ(0x05) messages to the terminal.
asp retries	Specifies the number of times a packet will be resent before the connection with the terminal is disconnected.
asp send ack	Enables the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests.
asp timer	Customizes the ASP timers.

asp enq

To configure how the device sends ENQ(0x05) messages to the terminal, use the **asp enq** command in interface configuration mode. To restore the default method of sending of ENQ messages to the terminal to initiate sessions, use the **no** form of this command.

asp enq {**disable** | **delay** *milliseconds*}

no asp enq {**disable** | **delay**}

Syntax Description

disable	Disables the device from sending ENQ messages to the terminal to initiate sessions.
delay	Configures a delay between the sending of a connect message and the ENQ message.
milliseconds	Duration of the delay in milliseconds. Allowed values are from 1 to 1000.

Command Default

By default, ENQ messages are sent to the terminal.
milliseconds: 10 milliseconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **asp enq disable** command should be enabled only if the terminal the device is connecting to does not require ENQ messages as part of the session flow.

The **delay** keyword can be used to slow responses in dialed networks.

Examples

The following example specifies that ENQ messages be sent 500 milliseconds after the connect message is sent:

```
asp enq delay 500
```

Related Commands

Command	Description
asp dcd always	Specifies that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when traffic starts to the serial interface.
asp direct	Disables dial mode and automatically activate the peer connection.
asp retries	Specifies the number of times a packet will be resent before the connection with the terminal is disconnected.
asp send ack	Enables the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests.
asp timer	Customizes the ASP timers.

asp eof-char

To specify an end-of-frame (EOF) character for asynchronous serial protocols (ASP) to use to end ASP transmissions, use the **asp eof-char** command in interface configuration mode. To remove a previously configured EOF character, use the **no** form of this command.

asp eof-char *eof-character*

no asp eof-char

Syntax Description

eof-character	EOF character in hexadecimal format. The range is from 0 to ff.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **asp eof-char** command is enabled, asynchronous serial protocols (ASP) stops receiving characters when it receives the specified EOF character. When the **asp eof-char** command is disabled, ASP continues to receive characters until the RX-IFT timer expires.

Examples

The following example sets 3e as the EOF character:

```
asp eof-char 3e
```

Related Commands

Command	Description
asp broadcast-addr	Specifies the address that an asynchronous generic application uses to broadcast packets from its remote stations.
asp ignore-sequence-number	Instructs a device to ignore the ASP sequence numbers that are used to synchronize ASP traffic between head-end and tail-end devices.
asp sof-char	Specifies an SOF character for the asynchronous generic application.

asp ignore-sequence-number

To instruct a device to ignore the asynchronous serial protocols (ASP) sequence numbers that are used to synchronize ASP traffic between head-end and tail-end devices, use the **asp ignore-sequence-number** command in interface configuration mode. To instruct a device to use the ASP sequence numbers to validate ASP traffic, use the **no** form of this command.

asp ignore-sequence-number

no asp ignore-sequence-number

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled. The ASP sequence numbers are used to validate ASP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **asp ignore-sequence-number** command should be enabled when there is not a one-to-one correspondence between commands from the head-end device and commands from the tail-end device.

When the **asp ignore-sequence-number** command is disabled, ASP validates the sequence numbers.

Examples

The following example instructs the device to ignore ASP sequence numbers:

```
asp ignore-sequence-number
```

Related Commands

Command	Description
asp broadcast-addr	Specifies the address that an asynchronous application uses to broadcast packets from its remote stations.
asp eof-char	Specifies an EOF character for the asynchronous generic application to use to end ASP transmissions.
asp sof-char	Specifies an SOF character for the asynchronous generic application.

asp retries

To specify the number of times a packet will be resent before the connection with the terminal is disconnected, use the **asp retries** command in interface configuration mode. To reset the number of asynchronous serial protocols (ASP) retries to its default value, use the **no** form of this command.

asp retries *number*

no asp retries

Syntax Description

number	Number of times a packet will be resent before the connection with the terminal is disconnected. Allowed values are from 1 to 10.

Command Default

number: 4

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures ten ASP retries:

```
Device(config-if)# asp retries 10
```

Related Commands

Command	Description
asp dcd always	Specifies that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when traffic starts to the serial interface.
asp direct	Disables dial mode and automatically activate the peer connection.
asp enq	Configures how the device sends ENQ(0x05) messages to the terminal.
asp send ack	Enables the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests.
asp timer	Customizes the ASP timers.

asp role

To specify that the device is the primary end or the secondary end of the polled asynchronous link that is connected to a serial interface and that the attached remote device is a security alarm control station, use the **asp role** command in interface configuration mode. To remove the specification, use the **no** form of this command.

asp role {**primary** | **secondary**}

no asp role

Syntax Description

primary	Specifies the device as the primary end of the polled asynchronous link connected to the serial interface, and the attached remote devices are alarm panels.
secondary	Specifies the device as the secondary end of the polled asynchronous link connected to the serial interface, and the attached remote device is a security alarm control station.

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command configures the interface as primary or secondary to the device on which asynchronous serial protocol (ASP) is configured. Configure the interface connected to the alarm console as the secondary device and the interface connected to the alarm panel as the primary device. The addresses of the alarm panels must be used in the address field of the **bstun route address** command in the interface configuration mode.

Examples

The following example shows how to specify the device as the primary end of the link:

```
Device(config)# interface Serial 3/0
Device(config-if)# asp role primary
Device(config-if)# end
```

Related Commands

Command	Description
asp brdcast-address-mask	Allows the configuration of multiple address masks.
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

asp rx-ift

To specify a time period that, by expiring, signals the end of one frame being received and the start of the next, use the **asp rx-ift** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

asp rx-ift *interframe-timeout*

no asp rx-ift

Syntax Description

interframe-timeout	Number of milliseconds between the end of one frame being received and the start of the next frame. The default timeout value is 40 milliseconds.

Command Default

The default timeout value is 40 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The interframe timeout is useful when different baud rates are used between the device and the alarm console or alarm panel. For example, you might set an interframe timeout of 6 ms if the polled asynchronous protocol is running at 9600 bps, but set the value to 40 ms if the protocol is running at 300 bps.

This command applies only when the asynchronous-generic protocol has been specified on an interface using a combination of the **bstun protocol-group** global configuration command and the **bstun group** interface configuration command.

Interfaces configured to run the asynchronous-generic protocol have their baud rate set to 9600 bps, use 8 data bits, no parity, 1 start bit, and 1 stop bit. If different line configurations are required, use the **rxspeed**, **txspeed**, **databits**, **stopbits**, and **parity** line configuration commands to change the line attributes.

The addresses of the alarm panels should be used in the address field of the **bstun route address** interface configuration command.

Examples

The following example sets the interframe timeout value to 6 ms because the polled asynchronous protocol is running at 9600 bps:

```
asp rx-ift 6
```

Related Commands

Command	Description
asp addr-offset	Configures an asynchronous port to send and receive polled asynchronous traffic through a BSTUN tunnel.
asp role	Specifies whether the device is acting as the primary end of the polled asynchronous link or as the secondary end of the polled asynchronous link connected to the serial interface, and whether the attached remote device is a security alarm control station.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

asp send ack

To enable the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests, use the **asp send ack** command in interface configuration mode. To disable the sending of ACK messages, use the **no** form of this command.

asp send ack

no asp send ack

Syntax Description

This command has no arguments or keywords.

Command Default

The **asp send ack** command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **asp send ack** command is enabled, an acknowledgement is immediately sent when the device receives a packet. If the **asp send ack** command is disabled, an acknowledgement is not sent until the device receives a response from the host.

Examples

The following example configures the **asp send ack** command:

```
asp send ack
```

Related Commands

Command	Description
asp dcd always	Specifies that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when traffic starts to the serial interface.
asp direct	Disables dial mode and automatically activate the peer connection.
asp enq	Configures how the device sends ENQ(0x05) messages to the terminal.
asp retries	Specifies the number of times a packet will be resent before the connection with the terminal is disconnected.
asp timer	Customizes the ASP timers.

asp sof-char

To specify a start-of-frame (SOF) character, use the **asp sof-char** command in interface configuration mode. To remove a previously configured SOF character, use the **no** form of this command.

asp sof-char *address*

no asp sof-char

Syntax Description

address	SOF character in hexadecimal format. The range is from 0 to ff.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **asp sof-char** command is enabled, asynchronous serial protocols (ASP) ignores any characters received prior to the specified SOF character. When the **asp sof-char** command is disabled, ASP receives all characters.

Examples

The following example sets d9 as the SOF character:

```
asp sof-char d9
```

Related Commands

Command	Description
asp broadcast-addr	Specifies the address that an asynchronous generic application uses to broadcast packets from its remote stations.
asp eof-char	Specifies an EOF character for the asynchronous generic application to use to end ASP transmissions.
asp ignore-sequence-number	Instructs a device to ignore the ASP sequence numbers that are used to synchronize ASP traffic between head-end and tail-end devices.

asp timer

To customize the asynchronous serial protocols (ASP) timers, use the **asp timer** command in interface configuration mode. To reset the ASP timers to their default values, use the **no** form of this command.

asp timer {**rsp** *rsp-time* | **rx** *rx-time* | **host** *host-time* | **connect** *connect-time*}

no asp timer {**rsp** | **rx** | **host** | **connect**}

Syntax Description

rsp	Duration the device will wait for a response to a packet before resending.
rsp-time	Allowed values are from 1 to 30 seconds.
rx	Duration the device will wait for the entire packet to be received, beginning when the STX(0x02) character is received.
rx-time	Allowed values are from 10 to 60 seconds.
host	Duration the device will wait for a response packet from the host, beginning when the terminal request is forwarded to APIP
host-time	Allowed values are from 10 to 120 seconds.
connect	Duration the device will wait for the peer connection to activate when in dial mode, beginning when the device receives a dial string.
connect-time	Allowed values are from 1 to 30 seconds.

Command Default

rsp-time: 7 seconds
rx-time: 15 seconds
host-time: 60 seconds
connect-time: 8 seconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the RSP timer to 30 seconds, the RX timer to 60 seconds, the host timer to 120 seconds and the connect timer to 30 seconds:

```
asp timer rsp 30
asp timer rx 60
asp timer host 120
asp timer connect 30
```

bridge acquire

To forward any frames for stations that the system has learned about dynamically, use the **bridge acquire** command in global configuration mode. To disable the behavior, use the **no** form of this command.

bridge *bridge-group* **acquire**

no bridge *bridge-group* **acquire**

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.

Defaults

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When using the command default, the Cisco IOS software forwards any frames from stations that it has learned about dynamically. If you use the **no** form of this command, the bridge stops forwarding frames to stations it has dynamically learned about through the discovery process and limits frame forwarding to statically configured stations. That is, the bridge filters out all frames except those whose sourced-by or destined-to addresses have been statically configured into the forwarding cache. The **no** form of this command prevents the forwarding of a dynamically learned address.

Examples

The following example shows how to prevent the forwarding of dynamically determined source and destination addresses:

```
no bridge 1 acquire
```

Related Commands

Command	Description
bridge address	Filters frames with a particular MAC-layer station source or destination address.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge address

To filter frames with a particular MAC-layer station source or destination address, use the **bridge address** in global configuration mode. To disable the filtering of frames, use the **no** form of this command.

bridge *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface*]

no bridge *bridge-group* **address** *mac-address*

Syntax Description

bridge-group	Bridge group number. It must be the same number specified in the **bridge protocol** command argument.
mac-address	48-bit hardware address written as a dotted triple of four-digit hexadecimal numbers such as that displayed by the **show arp** command in EXEC mode, for example, 0800.cb00.45e9. It is either a station address, the broadcast address, or a multicast destination address.
forward	Frame sent from or destined to the specified address is forwarded as appropriate.
discard	Frame sent from or destined to the specified address is discarded without further processing.
interface	(Optional) Interface specification, such as Ethernet 0. It is added after the **forward** or **discard** keyword to indicate the interface on which that address can be reached.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Any number of addresses can be configured into the system without a performance penalty.

Note MAC addresses on Ethernet are “bit-swapped” when compared with MAC addresses on Token Ring and FDDI. For example, address 0110.2222.3333 on Ethernet is 8008.4444.CCCC on Token Ring and FDDI. Access lists always use the canonical Ethernet representation. When using different media and building access lists to filter on MAC addresses, remember this point. Note that when a bridged packet traverses a serial link, it has an Ethernet-style address.

Examples

The following example shows how to enable frame filtering with MAC address 0800.cb00.45e9. The frame is forwarded through Ethernet interface 1:

```
bridge 1 address 0800.cb00.45e9 forward ethernet 1
```

The following example shows how to disable the ability to forward frames with MAC address 0800.cb00.45e9:

```
no bridge 1 address 0800.cb00.45e9
```

Related Commands

Command	Description
bridge acquire	Forwards any frames for stations that the system has learned about dynamically.
bridge-group input-address-list	Assigns an access list to a particular interface.
bridge-group output-address-list	Assigns an access list to a particular interface for filtering the MAC destination addresses of packets that would ordinarily be forwarded out that interface.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge bitswap-layer3-addresses

To enable transparent bridging or source-route translational bridging or IP Advanced Research Projects Agency (ARPA) between canonical and noncanonical media types, use the **bridge bitswap-layer3-addresses** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

bridge *bridge-group* **bitswap-layer3-addresses**

no bridge *bridge-group* **bitswap-layer3-addresses**

Syntax Description

bridge-group	Bridge group number.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3(5) T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command “bit-swaps” (to and from noncanonical format) the hardware addresses that are embedded in layer 3 of ARP and Reverse Address Resolution Protocol (RARP) frames. This function enables IP communication between Token Ring and non-Token Ring media in a transparent-bridging environment. Because transparent bridging views the source-route bridge domain as a Token Ring media, enabling this command for a transparent bridge group also enables this function for source-route translational bridging (SR/TLB).

The user must ensure the frames are small enough to be sent on all media types because there is no end to end bridging protocol to negotiate the largest frame size.

There is no attempt to reformat ARP frames between ARP and Subnetwork Access Protocol (SNAP) formats.

Examples

The following example shows how to enable bit-swapping of addresses to and from noncanonical form in a transparent-bridged environment:

```
no ip routing
!
interface ethernet 0
 bridge-group 1
!
interface token-ring 0
 bridge-group 1
!
!
bridge 1 protocol ieee
bridge 1 bitswap-layer3-addresses
```

bridge bridge

To enable the bridging of a specified protocol in a specified bridge group, use the **bridge bridge** command in global configuration mode. To disable the bridging of a specified protocol in a specified bridge group, use the **no** form of this command.

bridge *bridge-group* **bridge** *protocol*

no bridge *bridge-group* **bridge** *protocol*

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.
protocol	Any of the supported routing protocols. The default is to bridge all of these protocols.

Defaults

Bridge every protocol.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When integrated routing and bridging (IRB) is enabled, the default route/bridge behavior in a bridge group is to bridge all protocols. You need not use the **bridge bridge** command to enable bridging.

You can use the **no bridge bridge** command to disable bridging in a bridge group so that it does not bridge a particular protocol. When you disable bridging for a protocol in a bridge group, routable packets of this protocol are routed when the bridge is explicitly configured to route this protocol, and nonroutable packets are dropped because bridging is disabled for this protocol.

Note Packets of nonroutable protocols, such as local-area transport (LAT), are bridged only. You cannot disable bridging for the nonroutable traffic.

Examples

The following example shows how to disable bridging of IP in bridge group 1:

```
no bridge 1 bridge ip
```

Related Commands

Command	Description
bridge irb	Enables the Cisco IOS software to route a given protocol between routed interfaces and bridge groups or to route a given protocol between bridge groups.
bridge protocol	Defines the type of Spanning Tree Protocol.
bridge route	Enables the routing of a specified protocol in a specified bridge group.

bridge circuit-group pause

To configure the interval during which transmission is suspended in a circuit group after circuit group changes take place, use the **bridge circuit-group pause** command in global configuration mode.

bridge *bridge-group* **circuit-group** *circuit-group* **pause** *milliseconds*

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command argument.
circuit-group	Number of the circuit group to which the interface belongs.
milliseconds	Forward delay interval. It must be a value in the range from 0 to 10000 ms.

Defaults

The default forward delay interval is 0.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Circuit-group changes include the addition or deletion of an interface and interface state changes.

There is not a **no** form for this command.

Examples

The following example shows how to set the circuit group pause to 5000 ms:

```
bridge 1 circuit-group 1 pause 5000
```

Related Commands

Command	Description
bridge circuit-group source-based	Uses just the source MAC address for selecting the output interface.
bridge-group circuit-group	Assigns each network interface to a bridge group.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge circuit-group source-based

To use just the source MAC address for selecting the output interface, use the **bridge circuit-group source-based** command in global configuration mode. To remove the interface from the bridge group, use the **no** form of this command.

bridge *bridge-group* **circuit-group** *circuit-group* **source-based**

no bridge *bridge-group* **circuit-group** *circuit-group* **source-based**

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.
circuit-group	Number of the circuit group to which the interface belongs.

Defaults

No bridge-group interface is assigned.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For applications that depend on the ordering of mixed unicast and multicast traffic from a given source, load distribution must be based on the source MAC address only. The **bridge circuit-group source-based** command modifies the load distribution strategy to accommodate such applications.

Examples

The following example uses the source MAC address for selecting the output interface to a bridge group:

```
bridge 1 circuit-group 1 source-based
```

Related Commands

Command	Description
bridge circuit-group pause	Configures the interval during which transmission is suspended in a circuit group after circuit group changes take place.
bridge-group circuit-group	Assigns each network interface to a bridge group.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge cmf

To enable constrained multicast flooding (CMF) for all configured bridge groups, use the **bridge cmf** command in global configuration mode. To disable constrained multicast flooding, use the **no** form of this command.

bridge cmf

no bridge cmf

Syntax Description

This command has no arguments or keywords.

Defaults

CMF is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enable CMF for all configured bridge groups:

```
bridge cmf
```

Related Commands

Command	Description
clear bridge multicast	Clears transparent bridging multicast state information.
show bridge multicast	Displays transparent bridging multicast state information.

bridge crb

To enable the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router, use the **bridge crb** command in global configuration mode. To disable the feature, use the **no** form of this command.

bridge crb

no bridge crb

Syntax Description

This command has no arguments or keywords.

Defaults

Concurrent routing and bridging is disabled. When concurrent routing and bridging has been enabled, the default behavior is to bridge all protocols that are not explicitly routed in a bridge group.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When concurrent routing and bridging is first enabled in the presence of existing bridge groups, it command generates a **bridge route** configuration command for any protocol for which any interface in the bridge group is configured for routing. This precaution applies only when concurrent routing and bridging is not already enabled, bridge groups exist, and the **bridge crb** command is encountered.

Once concurrent routing and bridging has been enabled, you must configure an explicit **bridge route** command for any protocol that is to be routed on interfaces in a bridge group (in addition to any required protocol-specific interface configuration).

Examples

The following command shows how to enable concurrent routing and bridging:

```
bridge crb
```

Related Commands

Command	Description
bridge route	Enables the routing of a specified protocol in a specified bridge group.

bridge domain

To establish a domain by assigning it a decimal value from 1 and 10, use the **bridge domain** command in global configuration mode. To return to a single bridge domain by choosing domain zero (0), use the **no** form of this command.

bridge *bridge-group* **domain** *domain-number*

no bridge *bridge-group* **domain**

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol ieee** command. The **dec** keyword is not valid for this command.
domain-number	Domain ID number you choose. The default domain number is zero; this is the domain number required when communicating to IEEE bridges that do not support this domain extension.

Defaults

Single bridge domain. The default domain number is 0.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco has implemented a proprietary extension to the IEEE spanning-tree software in order to support multiple spanning-tree domains. You can place any number of routers within the domain. The routers in the domain, and only those routers, will then share spanning-tree information.

Use this feature when multiple routers share the same cable, and you want to use only certain discrete subsets of these routers to share spanning-tree information with each other. This function is most useful when running other applications, such as IP User Datagram Protocol (UDP) flooding, that use the IEEE Spanning Tree Protocol. It can also be used to reduce the number of global reconfigurations in large bridged networks.

Caution Use multiple spanning-tree domains with care. Because bridges in different domains do not share spanning-tree information, bridge loops can be created if the domains are not carefully planned.

Note This command works only when the bridge group is running the IEEE Spanning Tree Protocol.

Examples

The following example shows how to place bridge group 1 in bridging domain 3. Only other routers that are in domain 3 will accept spanning-tree information from this router.

```
bridge 1 domain 3
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge forward-time

To specify the forward delay interval for the Cisco IOS software, use the **bridge forward-time** command in global configuration mode. To return to the default interval, use the **no** form of this command.

bridge *bridge-group* **forward-time** *seconds*

no bridge *bridge-group* **forward-time** *seconds*

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.
seconds	Forward delay interval. It must be a value in the range from 10 to 200 seconds. The default is 30 seconds.

Defaults

30-second delay.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The forward delay interval is the amount of time the software spends listening for topology change information after an interface has been activated for bridging and before forwarding actually begins.

Each bridge in a spanning tree adopts the **hello-time**, **forward-time**, and **max-age** parameters of the root bridge, regardless of its individual configuration.

Examples

The following example shows how to set the forward delay interval to 60 seconds:

```
bridge 1 forward-time 60
```

Related Commands

Command	Description
bridge-group subscriber-trunk	Specifies that an interface is at the upstream point of traffic flow.
bridge max-age	Changes the interval the bridge will wait to hear BPDUs from the root bridge.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge hello-time

To specify the interval between hello bridge protocol data units (BPDUs), use the **bridge hello-time** command in global configuration mode. To return the default interval, use the **no** form of this command.

bridge *bridge-group* **hello-time** *seconds*

no bridge *bridge-group* **hello-time**

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.
seconds	Interval from 1 to 10 seconds. The default is 1 second.

Defaults

1 second.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Each bridge in a spanning tree adopts the **hello-time**, **forward-time**, and **max-age** parameters of the root bridge, regardless of its individual configuration.

Examples

The following example shows how to set the interval to 5 seconds:

```
bridge 1 hello-time 5
```

Related Commands

Command	Description
bridge forward-time	Specifies the forward delay interval for the Cisco IOS software.
bridge max-age	Changes the interval the bridge will wait to hear BPDUs from the root bridge.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge irb

To enable the Cisco IOS software to route a given protocol between routed interfaces and bridge groups or to route a given protocol between bridge groups, use the **bridge irb** command in global configuration mode. To disable the feature, use the **no** form of this command.

bridge irb

no bridge irb

Syntax Description

This command has no arguments or keywords.

Defaults

Integrated routing and bridging (IRB) is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

IRB is supported for transparent bridging, but not for source-route bridging. IRB is supported on all interface media types except X.25 and ISDN bridged interfaces.

Examples

The following shows how to enable integrated routing and bridging:

```
bridge irb
```

Related Commands

Command	Description
bridge bitswap-layer3-addresses	Enables the bridging of a specified protocol in a specified bridge group.
bridge route	Enables the routing of a specified protocol in a specified bridge group.
interface bvi	Creates the BVI that represents the specified bridge group to the routed world and links the corresponding bridge group to the other routed interfaces.
show interfaces irb	Displays the configuration for each interface that has been configured for integrated routing or bridging.

bridge lat-service-filtering

To specify local-area transport (LAT) group-code filtering, use the **bridge lat-service-filtering** command in global configuration mode. To disable the use of LAT service filtering on the bridge group, use the **no** form of this command.

bridge *bridge-group* **lat-service-filtering**

no bridge *bridge-group* **lat-service-filtering**

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.

Defaults

LAT service filtering is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command informs the system that LAT service advertisements require special processing.

Examples

The following example specifies that LAT service announcements traveling across bridge group 1 require some special processing:

```
bridge 1 lat-service-filtering
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge max-age

To change the interval the bridge will wait to hear Bridge Protocol Data Unit (BPDU)s from the root bridge, use the **bridge max-age** command in global configuration mode. To return to the default interval, use the **no** form of this command.

bridge *bridge-group* **max-age** *seconds*

no bridge *bridge-group* **max-age**

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.
seconds	Interval the bridge will wait to hear BPDUs from the root bridge. It must be a value in the range from 10 to 200 seconds. The default is 15 seconds.

Defaults

15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Each bridge in a spanning tree adopts the **hello-time**, **forward-time**, and **max-age** parameters of the root bridge, regardless of its individual configuration. If a bridge does not receive BPDUs from the root bridge within this specified interval, it considers the network to be changed and will recompute the spanning-tree topology.

Examples

The following example increases the maximum idle interval to 20 seconds:

```
bridge 1 max-age 20
```

Related Commands

Command	Description
bridge forward-time	Specifies the forward delay interval for the Cisco IOS software.
bridge-group subscriber-trunk	Specifies that an interface is at the upstream point of traffic flow.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge multicast-source

To configure bridging support to allow the forwarding, but not the learning, of frames received with multicast source addresses, use the **bridge multicast-source** command in global configuration mode. To disable this function on the bridge, use the **no** form of this command.

bridge *bridge-group* **multicast-source**

no bridge *bridge-group* **multicast-source**

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you need to bridge Token Ring over another medium, remote source-route bridging (RSRB) is recommended.

Examples

The following example allows the forwarding, but not the learning, of frames received with multicast source addresses:

```
bridge 2 multicast-source
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge priority

To configure the priority of an individual bridge, or the likelihood that it will be selected as the root bridge, use the **bridge priority** command in global configuration mode.

bridge *bridge-group* **priority** *number*

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.
number	The lower the number, the more likely the bridge will be chosen as root. When the IEEE Spanning Tree Protocol is enabled, the *number* argument ranges from 0 to 65535 (default is 32768). When the Digital Spanning Tree Protocol is enabled, the *number* argument ranges from 0 to 255 (default is 128).

Defaults

When the IEEE Spanning Tree Protocol is enabled on the router: 32768
When the Digital Spanning Tree Protocol is enabled on the router: 128

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When two bridges tie for position as the root bridge, an interface priority determines which bridge will serve as the root bridge. Use the **bridge-group priority** command in interface configuration mode to control an interface priority.

There is not a **no** form for this command.

Examples

The following example establishes this bridge as a likely candidate to be the root bridge:

```
bridge 1 priority 100
```

Related Commands

Command	Description
bridge-group priority	Sets an interface priority.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge protocol

To define the type of Spanning Tree Protocol, use the **bridge protocol** command in global configuration mode. To delete the bridge group, use the **no** form of this command with the appropriate keywords and arguments.

bridge *bridge-group* **protocol** {**dec** | **ibm** | **ieee** | **vlan-bridge**}

no bridge *bridge-group* **protocol** {**dec** | **ibm** | **ieee** | **vlan-bridge**}

Syntax Description

bridge-group	Number in the range from 1 to 255 that you choose to refer to a particular set of bridged interfaces. Frames are bridged only among interfaces in the same group. You will use the group number you assign in subsequent bridge configuration commands.
dec	Digital Spanning Tree Protocol.
ibm	IBM Spanning Tree Protocol.
ieee	IEEE Ethernet Spanning Tree Protocol.
vlan-bridge	VLAN-Bridge Spanning Tree Protocol.

Defaults

No Spanning Tree Protocol is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(1)T	The **ibm** and **vlan-bridge** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The routers support two Spanning Tree Protocols: the IEEE 802.1 standard and the earlier Digital Spanning Tree Protocol upon which the IEEE standard is based. Multiple domains are supported for the IEEE 802.1 Spanning Tree Protocol.

Note The IEEE 802.1D Spanning Tree Protocol is the preferred way of running the bridge. Use the Digital Spanning Tree Protocol only for backward compatibility.

Examples

The following example shows bridge 1 as using the Digital Spanning Tree Protocol:

```
bridge 1 protocol dec
```

Related Commands

Command	Description
bridge domain	Establishes a domain by assigning it a decimal value from 1 to 10.
bridge-group	Assigns each network interface to a bridge group.

bridge protocol ibm

To create a bridge group that runs the automatic spanning-tree function, use the **bridge protocol ibm** command in global configuration mode. To cancel the previous assignment, use the **no** form of this command.

bridge *bridge-group* **protocol ibm**

no bridge *bridge-group* **protocol ibm**

Syntax Description

bridge-group	Number in the range from 1 to 9 that refers to a particular set of bridged interfaces.

Defaults

No bridge group is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies bridge 1 to use the automatic spanning-tree function:

```
bridge 1 protocol ibm
```

Related Commands

Command	Description
show source-bridge	Displays the current source bridge configuration and miscellaneous statistics.
source-bridge spanning (automatic)	Enables the automatic spanning-tree function for a specified group of bridged interfaces.
source-bridge spanning (manual)	Enables use of spanning explorers.

bridge route

To enable the routing of a specified protocol in a specified bridge group, use the **bridge route** command in global configuration mode. To disable the routing of a specified protocol in a specified bridge group, use the **no** form of this command.

bridge *bridge-group* **route** *protocol*

no bridge *bridge-group* **route** *protocol*

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.
protocol	One of the following protocols: • **appletalk** • clns • decnet • ip • **ipx**.

Defaults

No default bridge group or protocol is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	The following values for the *protocol* argument were removed: • **apollo** • **vines** • **xns**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, AppleTalk and IP are routed on bridge group 1:

```
bridge crb
bridge 1 protocol ieee
bridge 1 route appletalk
bridge 1 route ip
```

Related Commands

Command	Description
bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge subscriber-policy

To bind a bridge group with a subscriber policy, use the **bridge subscriber-policy** command in global configuration mode. To disable the subscriber bridge group feature, use the **no** form of this command.

bridge *bridge-group* **subscriber-policy** *policy*

no bridge *bridge-group* **subscriber-policy** *policy*

Syntax Description

bridge-group	Bridge group number, in the range from from 1 to 256, specified in the **bridge protocol** command.
policy	Subscriber policy number in the range from 1 to 100.

Defaults

Table 5 shows the default values that are applied if no forward or filter decisions have been specified for the subscriber policy:

Table 10 Packet Default Values

Packet	Upstream
ARP	Permit
Broadcast	Deny
CDP	Deny/Disable
Multicast	Permit
Spanning Tree Protocol	Deny/Disable
Unknown Unicast	Deny

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Standard access lists can coexist with the subscriber policy. However, subscriber policy will take precedence over the access list by being checked first. A packet permitted by the subscriber policy will be checked against the access list if it is specified. A packet denied by subscriber policy will be dropped with no further access list checking.

Examples

The following example forms a subscriber bridge group using policy 1:

```
bridge 1 subscriber-policy 1
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.
show subscriber-policy	Displays the details of a subscriber policy.
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

bridge-group

To assign each network interface to a bridge group, use the **bridge-group** command in interface configuration mode. To remove the interface from the bridge group, use the **no** form of this command.

bridge-group *bridge-group*

no bridge-group *bridge-group*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.

Defaults

No bridge group interface is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can bridge on any interface, including any serial interface, regardless of encapsulation. Bridging can be configured between interfaces on different cards, although the performance is lower compared with interfaces on the same card. Also note that serial interfaces must be running with high-level data link control (HLDC), X.25, or Frame Relay encapsulation.

Note Several modifications to interfaces in bridge groups, including adding interfaces to bridge groups, will result in any Token Ring or FDDI interfaces in that bridge group being re initialized.

Examples

In the following example, Ethernet interface 0 is assigned to bridge group 1, and bridging is enabled on this interface:

```
interface ethernet 0
 bridge-group 1
```

Related Commands

Command	Description
bridge-group cbus-bridging	Enables autonomous bridging on a ciscoBus2 controller.
bridge-group circuit-group	Assigns each network interface to a bridge group.
bridge-group input-pattern-list	Associates an extended access list with a particular interface in a particular bridge group.
bridge-group output-pattern-list	Associates an extended access list with a particular interface.
bridge-group spanning-disabled	Disables the spanning tree on a given interface.

bridge-group aging-time

To set the length of time that a dynamic entry can remain in the bridge table from the time the entry was created or last updated, use the **bridge-group aging-time** command in global configuration mode. To return to the default aging-time interval, use the **no** form of this command.

bridge-group *bridge-group* **aging-time** *seconds*

no bridge-group *bridge-group* **aging-time**

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
seconds	Aging time, in the range from 10 to 1000000 seconds. The default is 300 seconds.

Defaults

300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If hosts on a bridged network are likely to move, decrease the aging time to enable the bridge to adapt quickly to the change. If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time and thus reduce the possibility of flooding when the hosts send again.

Examples

The following example sets the aging time to 200 seconds:

```
bridge-group 1 aging-time 200
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

bridge-group cbus-bridging

To enable autonomous bridging on a ciscoBus2 controller, use the **bridge-group cbus-bridging** command in interface configuration mode. To disable autonomous bridging, use the **no** form of this command.

bridge-group *bridge-group* **cbus-bridging**

no bridge-group *bridge-group* **cbus-bridging**

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.

Defaults

Autonomous bridging is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Normally, bridging takes place on the processor card at interrupt level. When autonomous bridging is enabled, bridging takes place entirely on the ciscoBus2 controller, substantially improving performance.

You can enable autonomous bridging on Ethernet, FDDI (FCIT) and High-Speed Serial Interface (HSSI) interfaces that reside on a ciscoBus2 controller. Autonomous bridging is not supported on Token Ring interfaces, regardless of the type of bus in use.

To enable autonomous bridging on an interface, first define that interface as part of a bridge group. When a bridge group includes both autonomously and normally bridged interfaces, packets are autonomously bridged in some cases, but bridged normally in others. For example, when packets are forwarded between two autonomously bridged interfaces, those packets are autonomously bridged. But when packets are forwarded between an autonomously bridged interface and one that is not, the packet must be normally bridged. When a packet is flooded, the packet is autonomously bridged on autonomously bridged interfaces, but must be normally bridged on any others.

Note In order to maximize performance when using a ciscoBus2 controller, use the **bridge-group cbus-bridging** command to enable autonomous bridging on any Ethernet, FDDI, or HSSI interface.

Note You can filter by MAC-level address on an interface only when autonomous bridging is enabled on that interface; autonomous bridging disables all other filtering and priority queueing.

Examples

In the following example, autonomous bridging is enabled on Ethernet interface 0:

```
interface ethernet 0
 bridge-group 1
 bridge-group 1 cbus-bridging
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

bridge-group circuit-group

To assign each network interface to a bridge group, use the **bridge-group circuit-group** command in interface configuration mode. To remove the interface from the bridge group, use the **no** form of this command.

bridge-group *bridge-group* **circuit-group** *circuit-group*

no bridge-group *bridge-group* **circuit-group** *circuit-group*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
circuit-group	Circuit group number. The range is from 1 to 9.

Defaults

No bridge group interface is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Circuit groups are primarily intended for use with High-Speed Serial Interface (HSSI)-encapsulated serial interfaces. They are not supported for packet-switched networks such as X.25 or Frame Relay. Circuit groups are best applied to groups of serial lines of equal bandwidth, but can accommodate mixed bandwidths.

Note You must configure bridging before you configure a circuit group on an interface.

Examples

In the following example, Ethernet interface 0 is assigned to circuit group 1 of bridge group 1:

```
interface ethernet 0
 bridge-group 1 circuit-group 1
```

Related Commands

Command	Description
bridge circuit-group pause	Configures the interval during which transmission is suspended in a circuit group after circuit group changes take place.
bridge circuit-group source-based	Uses just the source MAC address for selecting the output interface.

bridge-group input-address-list

To assign an access list to a particular interface, use the **bridge-group input-address-list** command in interface configuration mode. This access list is used to filter packets received on that interface based on their MAC source addresses. To remove an access list from an interface, use the **no** form of this command.

bridge-group *bridge-group* **input-address-list** *access-list-number*

no bridge-group *bridge-group* **input-address-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the **access-list** command. It must be in the range from 700 to 799.

Defaults

No access list is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example assumes you want to disallow the bridging of Ethernet packets of all Sun workstations on Ethernet interface 1. Software assumes that all such hosts have Ethernet addresses with the vendor code 0800.2000.0000. The first line of the access list denies access to all Sun workstations, and the second line permits everything else. You then assign the access list to the input side of Ethernet interface 1.

```
access-list 700 deny 0800.2000.0000 0000.00FF.FFFF
access-list 700 permit 0000.0000.0000 FFFF.FFFF.FFFF
!
interface ethernet 1
 bridge-group 1 input-address-list 700
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge address	Filters frames with a particular MAC-layer station source or destination address.
bridge-group output-address-list	Assigns an access list to a particular interface for filtering the MAC destination addresses of packets that would ordinarily be forwarded out that interface.

bridge-group input-lat-service-deny

To specify the group codes by which to deny access upon input, use the **bridge-group input-lat-service-deny** command in interface configuration mode. To remove this access condition, use the **no** form of this command.

bridge-group *bridge-group* **input-lat-service-deny** *group-list*

no bridge-group *bridge-group* **input-lat-service-deny** *group-list*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
group-list	List of local-area transport (LAT) service groups. Single numbers and ranges are permitted. Ranges are specified with a dash between the first and last group numbers in the range. Specify a zero (0) to disable the LAT group code for the bridge group.

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This command prevents the system from bridging any LAT service advertisement that has any of the specified groups set.

Examples

The following example causes any advertisements with groups 6, 8, and 14 through 20 to be dropped:

```
interface ethernet 0
 bridge-group 1 input-lat-service-deny 6 8 14-20
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-lat-service-permit	Specifies the group codes by which to permit access upon input.
bridge-group output-lat-service-deny	Specifies the group codes by which to deny access upon output.

bridge-group input-lat-service-permit

To specify the group codes by which to permit access upon input, use the **bridge-group input-lat-service-permit** command in interface configuration mode. To remove this access condition, use the **no** form of this command.

bridge-group *bridge-group* **input-lat-service-permit** *group-list*

no bridge-group *bridge-group* **input-lat-service-permit** *group-list*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
group-list	local-area transport (LAT) service groups. Single numbers and ranges are permitted. Specify a zero (0) to disable the LAT group code for the bridge group.

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This command causes the system to bridge only those service advertisements that match at least one group in the group list specified by the *group-list* argument.

If a message specifies group codes in both the deny and permit list, the message is not bridged.

Examples

The following example bridges any advertisements from groups 1, 5, and 12 through 14:

```
interface ethernet 1
 bridge-group 1 input-lat-service-permit 1 5 12-14
```

Related Commands

Command	Description
bridge-group input-lat-service-deny	Specifies the group codes by which to deny access upon input.
bridge-group output-lat-service-permit	Specifies the group codes by which to permit access upon output.

bridge-group input-lsap-list

To filter IEEE 802.2-encapsulated packets on input, use the **bridge-group input-lsap-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **input-lsap-list** *access-list-number*

no bridge-group *bridge-group* **input-lsap-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This access list is applied to all IEEE 802.2 frames received on that interface prior to the bridge-learning process. Subnetwork Access Protocol (SNAP) frames must also pass any applicable Ethernet type-code access list.

Examples

The following example specifies access list 203 on Ethernet interface 1:

```
interface ethernet 1
 bridge-group 3 input-lsap-list 203
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group output-lsap-list	Filters IEEE 802-encapsulated packets on output.

bridge-group input-pattern-list

To associate an extended access list with a particular interface in a particular bridge group, use the **bridge-group input-pattern-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **input-pattern-list** *access-list-number*

no bridge-group *bridge-group* **input-pattern-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned using the extended **access-list** command. Specify a zero (0) to disable the application of the access list on the interface.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

The following command applies access list 1101 to bridge group 3 using the filter defined in group 1:

```
interface ethernet 0
bridge-group 3 input-pattern-list 1101
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group output-pattern-list	Associates an extended access list with a particular interface.

bridge-group input-type-list

To filter Ethernet- and Subnetwork Access Protocol (SNAP)-encapsulated packets on input, use the **bridge-group input-type-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **input-type-list** *access-list-number*

no bridge-group *bridge-group* **input-type-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

For SNAP-encapsulated frames, the access list is applied against the 2-byte Type field given after the destination service access point (DSAP)/source service access point (SSAP)/Organizationally Unique Identifier (OUI) fields in the frame.

This access list is applied to all Ethernet and SNAP frames received on that interface prior to the bridge learning process. SNAP frames must also pass any applicable IEEE 802 DSAP/SSAP access lists.

Examples

The following example shows how to configure a Token Ring interface with an access list that allows only the local-area transport (LAT) protocol to be bridged:

```
interface tokenring 0
 ip address 131.108.1.1 255.255.255.0
 bridge-group 1
 bridge-group 1 input-type-list 201
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group output-type-list	Filters Ethernet- and SNAP-encapsulated packets on output.

bridge-group lat-compression

To reduce the amount of bandwidth that local-area transport (LAT) traffic consumes on the serial interface by specifying a LAT-specific form of compression, use the **bridge-group lat-compression** command in interface configuration mode. To disable LAT compression on the bridge group, use the **no** form of this command.

bridge-group *bridge-group* **lat-compression**

no bridge-group *bridge-group* **lat-compression**

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Compression is applied to LAT frames being sent out the router through the interface in question.

LAT compression can be specified only for serial interfaces. For the most common LAT operations (user keystrokes and acknowledgment packets), LAT compression reduces LAT's bandwidth requirements by nearly a factor of two.

Examples

The following example compresses LAT frames on the bridge assigned to group 1:

```
bridge-group 1 lat-compression
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

bridge-group output-address-list

To assign an access list to a particular interface for filtering the MAC destination addresses of packets that would ordinarily be forwarded out that interface, use the **bridge-group output-address-list** command in interface configuration mode. To remove an access list from an interface, use the **no** form of this command.

bridge-group *bridge-group* **output-address-list** *access-list-number*

no bridge-group *bridge-group* **output-address-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command.

Defaults

No access list is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example assigns access list 703 to Ethernet interface 3:

```
interface ethernet 3
 bridge-group 5 output-address-list 703
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge address	Filters frames with a particular MAC-layer station source or destination address.
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-address-list	Assigns an access list to a particular interface.

bridge-group output-lat-service-deny

To specify the group codes by which to deny access upon output, use the **bridge-group output-lat-service-deny** command in interface configuration mode. To cancel the specified group codes, use the **no** form of this command.

bridge-group *bridge-group* **output-lat-service-deny** *group-list*

no bridge-group *bridge-group* **output-lat-service-deny** *group-list*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
group-list	List of local-area transport (LAT) groups. Single numbers and ranges are permitted.

Defaults

No group codes are assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This command causes the system to not bridge onto this output interface any service advertisements that contain groups matching any of those in the group list.

Examples

The following example prevents bridging of LAT service announcements from groups 12 through 20:

```
interface ethernet 0
 bridge-group 1
 bridge-group 1 output-lat-service-deny 12-20
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.

Command	Description
bridge-group input-lat-service-deny	Specifies the group codes by which to deny access upon input.
bridge-group output-lat-service-permit	Specifies the group codes by which to permit access upon output.

bridge-group output-lat-service-permit

To specify the group codes by which to permit access upon output, use the **bridge-group output-lat-service-permit** command in interface configuration mode. To cancel specified group codes, use the **no** form of this command.

bridge-group *bridge-group* **output-lat-service-permit** *group-list*

no bridge-group *bridge-group* **output-lat-service-permit** *group-list*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
group-list	local-area transport (LAT) service advertisements.

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This command causes the system to bridge onto this output interface only those service advertisements that match at least one group in the specified group code list.

Note If a message matches both a deny and a permit condition, it will not be bridged.

Examples

The following example allows only LAT service announcements from groups 5, 12, and 20 on this bridge:

```
interface ethernet 0
 bridge-group 1 output-lat-service-permit 5 12 20
```

Related Commands

Command	Description
bridge-group input-lat-service-permit	Specifies the group codes by which to permit access upon input.
bridge-group output-lat-service-deny	Specifies the group codes by which to deny access upon output.

bridge-group output-lsap-list

To filter IEEE 802-encapsulated packets on output, use the **bridge-group output-lsap-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **output-lsap-list** *access-list-number*

no bridge-group *bridge-group* **output-lsap-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Subnetwork Access Protocol (SNAP) frames must also pass any applicable Ethernet type-code access list. This access list is applied just before sending out a frame to an interface.

For performance reasons, specify both input and output type code filtering on the same interface.

Access lists for Ethernet- and IEEE 802-encapsulated packets affect only bridging functions. Such access lists cannot be used to block frames with protocols that are being routed.

Packets bearing an 802.2 LSAP of 0xAAAA qualify for LSAP filtering because they are inherently in 802.3 format. However, because they also carry a Type field, they are matched against any Type filters. Therefore, if you use Link Service Access Point (LSAP) filters on an interface that may bear SNAP-encapsulated packets, you must explicitly permit 0xAAAA.

Examples

The following example specifies access list 204 on Ethernet interface 0:

```
interface ethernet 0
 bridge-group 4 output-lsap-list 204
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-lsap-list	Filters IEEE 802.2-encapsulated packets on input.

bridge-group output-pattern-list

To associate an extended access list with a particular interface, use the **bridge-group output-pattern-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **output-pattern-list** *access-list-number*

no bridge-group *bridge-group* **output-pattern-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Extended access list number you assigned using the extended **access-list** command. Specify a zero (0) to disable the application of the access list on the interface.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

The following example filters all packets sent by bridge group 3 using the filter defined in access list 1102:

```
interface ethernet 0
 bridge-group 3 output-pattern-list 1102
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-pattern-list	Associates an extended access list with a particular interface in a particular bridge group.

bridge-group output-type-list

To filter Ethernet- and Subnetwork Access Protocol (SNAP)-encapsulated packets on output, use the **bridge-group output-type-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **output-type-list** *access-list-number*

no bridge-group *bridge-group* **output-type-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group. This access list is applied just before sending out a frame to an interface.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

The following example specifies access list 202 on Ethernet interface 0:

```
interface ethernet 0
 bridge-group 2 output-type-list 202
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-type-list	Filters Ethernet- and SNAP-encapsulated packets on input.

bridge-group path-cost

To set a different path cost, use the **bridge-group path-cost** command in interface configuration mode. To choose the default path cost for the interface, use the **no** form of this command.

bridge-group *bridge-group* **path-cost** *cost*

no bridge-group *bridge-group* **path-cost** *cost*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
cost	Relative cost of using the path. Path cost can range from 1 to 65535, with higher values indicating higher costs. This range applies regardless of whether the IEEE or Digital Spanning Tree Protocol has been specified.

Defaults

The default path cost is computed from the interface's bandwidth setting. The following are IEEE default path cost values. The Digital path cost default values are different.

- Ethernet—100
- 16-Mb Token Ring—62
- FDDI—10
- HSSI—647
- MCI/SCI Serial—647

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By convention, the path cost is 10000/data rate of the attached LAN (IEEE), or 100000/data rate of the attached LAN (Digital), in megabits per second.

Examples

The following example changes the default path cost for Ethernet interface 0:

```
interface ethernet 0
 bridge-group 1 path-cost 250
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

bridge-group priority

To set an interface priority, use the **bridge-group priority** command in interface configuration mode. The interface priority is used to select the designated port for this bridge-group on the connected media. One designated port on each medium is needed to compute the spanning tree.

bridge-group *bridge-group* **priority** *number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
number	Priority number ranging from 0 to 255 (Digital), or 0 to 64000 (IEEE). The default is 32768 if IEEE Spanning Tree Protocol is enabled on the router or 128 if Digital Spanning Tree Protocol is enabled on the router.

Defaults

When the IEEE Spanning Tree Protocol is enabled on the router: 32768
When the Digital Spanning Tree Protocol is enabled on the router: 128

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The lower the number, the more likely it is that the bridge on the interface will be chosen as the root.

There is not a **no** form for this command.

Examples

The following example increases the likelihood that the root bridge will be the one on Ethernet interface 0 in bridge group 1:

```
interface ethernet 0
 bridge-group 1 priority 0
```

The following example shows the **bridge-group priority** help information for 9-bit port number size:

```
Router(config-if)# bridge-group 1 priority ?
<0-255> increments of 2 for IEEE or vlan-bridge, others 1
```

The following example shows the **bridge-group priority** help information for 10-bit port number size:

```
Router(config-if)# bridge-group 1 priority ?
<0-255> increments of 4 for IEEE or vlan-bridge, others 1
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
bridge priority	Configures the priority of an individual bridge, or the likelihood that it will be selected as the root bridge.

bridge-group spanning-disabled

To disable the spanning tree on a given interface, use the **bridge-group spanning-disabled** command in interface configuration mode. To enable the spanning tree on a given interface, use the no form of this command.

bridge-group *bridge-group* **spanning-disabled**

no bridge-group *bridge-group* **spanning-disabled**

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from of 1 to 255.

Defaults

Spanning tree is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To enable transparent bridging on an interface, use the **bridge protocol** command to specify the type of Spanning Tree Protocol to be used. The **bridge-group spanning-disabled** command can be used to disable that spanning tree on that interface.

When a *loop-free* path exists between any two bridged subnetworks, you can prevent Bridge Protocol Data Unit (BPDU)s generated in one transparent bridging subnetwork from impacting nodes in the other transparent bridging subnetwork, yet still permit bridging throughout the bridged network as a whole.

For example, when transparently bridged LAN subnetworks are separated by a WAN, you can use this command to prevent BPDUs from traveling across the WAN link. You would apply this command to the serial interfaces connecting to the WAN in order to prevent BPDUs generated in one domain from impacting nodes in the remote domain. Because these BPDUs are prevented from traveling across the WAN link, using this command also has the secondary advantage of reducing traffic across the WAN link.

Note In order to disable the spanning tree, you must make sure that no parallel paths exist between transparently bridged interfaces in the network.

Examples

In the following example, the spanning tree for the serial interface 0 is disabled:

```
interface serial 0
 bridge-group 1 spanning-disabled
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge-group sse

To enable the Cisco silicon switching engine (SSE) switching function, use the **bridge-group sse** command in interface configuration mode. To disable SSE switching, use the **no** form of this command.

bridge-group *bridge-group* **sse**

no bridge-group *bridge-group* **sse**

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following shows how to enable SSE switching:

```
bridge-group 1 sse
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.

bridge-group subscriber-loop-control

To enable loop control on virtual circuits associated with a bridge group, use the **bridge-group subscriber-loop-control** command in interface configuration mode. To disable loop control, use the **no** form of this command.

bridge-group *bridge-group* **subscriber-loop-control**

no bridge-group *bridge-group* **subscriber-loop-control**

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.

Defaults

Loop control is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following shows how to enable loop control on virtual circuits associated with bridge group 1:

```
bridge-group 1 subscriber-loop-control
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.
bridge subscriber-policy	Binds a bridge group with a subscriber policy.
show subscriber-policy	Displays the details of a subscriber policy.
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

bridge-group subscriber-trunk

To specify that an interface is at the upstream point of traffic flow, use the **bridge-group subscriber-trunk** command in interface configuration mode. To remove the specification and reset the interface to a non trunking port, use the **no** form of this command.

bridge-group *bridge-group* **subscriber-trunk**

no bridge-group *bridge-group* **subscriber-trunk**

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.

Defaults

The interface is set to a non-trunking port.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets bridge group 1 as the upstream point of traffic flow:

```
bridge-group 1 subscriber-trunk
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.
bridge subscriber-policy	Binds a bridge group with a subscriber policy.
show subscriber-policy	Displays the details of a subscriber policy.
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

bsc char-set

To specify the character set used by the Bisync support feature in this serial interface as either EBCDIC or ASCII, use the **bsc char-set** command in interface configuration mode. To cancel the character set specification, use the **no** form of this command.

bsc char-set {**ascii** | **ebcdic**}

no bsc char-set {**ascii** | **ebcdic**}

Syntax Description

ascii	ASCII character set.
ebcdic	EBCDIC character set. This character set is the default.

Defaults

EBCDIC

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command specifies that the ASCII character set will be used:

```
bsc char-set ascii
```

bsc contention

To specify an address on a contention interface, use the **bsc contention** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc contention *address*

no bsc contention

Syntax Description

address	Address assigned to contention interface. The range is from 1 to 255. The default is 0x01.

Defaults

The default address is 0x01 to accommodate backward compatibility to the previous point-to-point contention implementation.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command specifies address 20 on the remote device:

```
bsc contention 20
```

Related Commands

Command	Description
bsc dial-contention	Specifies a router at the central site as a central router with dynamic allocation of serial interfaces.

bsc dial-contention

To specify a router at the central site as a central router with dynamic allocation of serial interfaces, use the **bsc dial-contention** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc dial-contention *timeout*

no bsc dial-contention

Syntax Description

timeout	Amount of time (in seconds) the interface can sit idle before it is returned to the idle interface pool. The range is from 2 to 30 seconds. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A timeout value is configurable to ensure that an interface does not get locked out because of a device outage during sending of data.

Examples

The following command defines a dial-in interface at the central site with an idle timeout of 10 seconds:

```
bsc dial-contention 10
```

Related Commands

Command	Description
bsc contention	Specifies an address on a contention interface.

bsc host-timeout

To detect deactivation of devices at the host, use the **bsc host-timeout** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

bsc host-timeout *interval*

no host-timeout *interval*

Syntax Description

interval	Timeout interval within which a poll or select for a control unit must be received. If this interval expires, the remote router is sent a teardown peer signal. The range is from 30 to 3000 deciseconds. The default is 600 deciseconds (60 seconds).

Defaults

The default interval is 600 deciseconds (60 seconds).

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to detect deactivation of devices at the host. If the host is told to deactivate or not poll a device, time will be required for the signal to propagate the network and get the remote end from polling. The timeout can be used to fine-tune the delay in detecting the host outage. The remote peer will stop polling the control unit that has timed out in the interval one to two times the configured timeout value.

Examples

The following example shows how to configure a timeout of 500 deciseconds:

```
bsc host-timeout 500
```

Related Commands

Command	Description
bsc secondary	Specifies that the router is acting as the secondary end of the Bisync link connected to the serial interface, and the attached remote device is a Bisync control station.
bstun group	Specifies the BSTUN group to which the interface belongs.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.

bsc pause

To specify the interval, to the tenth of a second, between starts of the polling cycle, use the **bsc pause** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc pause *time*

no bsc pause *time*

Syntax Description

time	Interval in tenths of a second. The default value is 30 (that is, 30 tenths of a second, or 3 seconds). The maximum time is 255 tenths of a second (25.5 seconds).

Defaults

30 tenths of a second (3 seconds)

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command sets the interval to 20 tenths of a second (2 seconds):

```
bsc pause 20
```

bsc poll-timeout

To specify the timeout, in tenths of a second, for a poll or select sequence, use the **bsc poll-timeout** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc poll-timeout *time*

no bsc poll-timeout *time*

Syntax Description

time	Time in tenths of a second. The default value is 30 (that is, 30 tenths of a second, or 3 seconds).

Defaults

30 tenths of a second (3 seconds).

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command sets the interval to 20 tenths of a second (2 seconds):

```
bsc poll-timeout 20
```

bsc primary

To specify that the router is acting as the primary end of the Bisync link connected to the serial interface, and that the attached remote devices are Bisync tributary stations, use the **bsc primary** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc primary

no bsc primary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Bisync support feature in the serial interface uses the address of the incoming encapsulation for reply.

Examples

The following example specifies the router as the primary role:

```
bsc primary
```

Related Commands

Command	Description
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

bsc retries

To specify the number of retries performed before a device is considered to have failed, use the **bsc retries** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc retries *retries*

no bsc retries *retries*

Syntax Description

retries	Number of retries before a device fails. The default is 5.

Defaults

Five retries.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This commands was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command sets the retry count to 10:

```
bsc retries 10
```

bsc secondary

To specify that the router is acting as the secondary end of the Bisync link connected to the serial interface, and the attached remote device is a Bisync control station, use the **bsc secondary** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc secondary

no bsc secondary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Bisync support feature in this serial interface uses the address of the poll or selection block in the framing encapsulation. It also generates an end of transmission (EOT) frame preceding each Bisync poll and selection.

Examples

The following example specifies the router as the secondary role:

```
bsc secondary
```

Related Commands

Command	Description
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

bsc servlim

To specify the number of cycles of the active poll list that are performed between polls to control units in the inactive poll list, use the **bsc servlim** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc servlim *servlim-count*

no bsc servlim *servlim-count*

Syntax Description

servlim-count	Number of cycles. The range is from 1 to 50. The default is 3.

Defaults

Three cycles.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command sets the number of cycles to 2:

```
bsc servlim 2
```

bsc spec-poll

To set specific polls, rather than general polls, used on the host-to-router connection, use the **bsc spec-poll** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc spec-poll

no spec-poll

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **bsc spec-poll** command when a router is connected to a host, and only when that host issues specific polls rather than general polls. Tandem hosts that poll ATM cash machines are typically configured to use specific polls rather than general polls.

Configuring a downstream (control-unit/device connected) router to support specific polling has no effect.

Examples

The following commands configure serial interface 0 to use specific poll:

```
interface serial 0
 description Connection to host.
 encapsulation bstun
 bstun group 1
 bsc secondary
 bsc spec-poll
 bsc char-set ebcdic
 bstun route all tcp 10.10.14.122
```

bstun group

To specify the block serial tunnel (BSTUN) group to which the interface belongs, use the **bstun group** command in interface configuration mode. To remove the interface from the BSTUN group, use the **no** form of this command.

bstun group *group-number*

no bstun group *group-number*

Syntax Description

group-number	BSTUN group to which the interface belongs.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Each BSTUN-enabled interface must be placed in a BSTUN group that was previously defined by the **bstun protocol-group** command. Packets travel only between BSTUN-enabled interfaces that are in the same group.

Examples

The following example specifies that serial interface 1 belongs to the previously defined protocol group 1:

```
interface serial 1
 encapsulation bstun
 bstun group 1
```

Related Commands

Command	Description
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
encapsulation bstun	Configures BSTUN on a particular serial interface.

bstun keepalive-count

To define the number of times to attempt a peer connection before declaring the peer connection to be down, use the **bstun keepalive-count** command in global configuration mode. To cancel the definition, use the **no** form of this command.

bstun keepalive-count *count*

no bstun keepalive-count

Syntax Description

count	Number of connection attempts. The range is from 2 to 10 retries.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The following example sets the number of times to retry a connection to a peer to 4:

```
bstun keepalive-count 4
```

Related Commands

Command	Description
bstun remote-peer-keepalive	Enables detection of the loss of a peer.

bstun lisnsap

To configure a service access point (SAP) on which to listen for incoming calls, use the **bstun lisnsap** command in global configuration mode. To cancel the SAP on which to listen, use the **no** form of this command.

bstun lisnsap *sap-value*

no bstun lisnsap

Syntax Description

sap-value	SAP on which to listen for incoming calls. The default is 04.

Defaults

The default SAP value is 04.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Changes to the **bstun lisnsap** command configuration will not take effect until after the router has been reloaded.

Examples

The following example shows how to configure SAP for listening:

```
bstun lisnsap
```

Related Commands

Command	Description
bstun route (Frame Relay)	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer over Frame Relay.
frame-relay map bstun	Configures BSTUN over Frame Relay for passthrough.
frame-relay map llc2	Configures BSTUN over Frame Relay when using Bisync local acknowledgment.

bstun peer-map-poll

To map the state of the peer to polling, use the **bstun peer-map-poll** command in global configuration mode. To disable mapping of the peer state to polling and map to the received status messages, use the **no** form of this command.

bstun peer-map-poll

no bstun peer-map-poll

Syntax Description

This command has no arguments or keywords.

Defaults

The received status messages are mapped to polling.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **bstun peer-map-poll** command to map the peer state to polling. If you configure this command, Bisync-to-IP protocol (BIP) activates polling when the BIP tunnel becomes active and stops polling when the tunnel connection is terminated. When the peer state-to-polling is not mapped, BIP waits for the host to issue an "active" status message across the BIP tunnel before polling the Automated Teller Machine (peer) device and polling is stopped when an "inactive" status message is received across the tunnel or the tunnel connection is terminated.

Related Commands

Command	Description
bstun peer-name	Enables the BSTUN function.
bstun reconnect-interval	Set the amount of time for the system to wait before trying to reconnect to a peer.
show bstun	Displays the current status of STUN connections.

bstun peer-name

To enable the block serial tunnel (BSTUN) function, use the **bstun peer-name** command in global configuration mode. To disable the function, use the **no** form of this command.

bstun peer-name *ip-address*

no bstun peer-name *ip-address*

Syntax Description

ip-address	Address by which this BSTUN peer is known to other BSTUN peers that are using the TCP transport.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The IP address defines the address by which this BSTUN peer is known to other BSTUN peers that are using the TCP transport. If this command is unconfigured or the **no** form of this command is specified, all BSTUN routing commands with IP addresses are deleted. BSTUN routing commands without IP addresses are not affected by this command.

Examples

The following example enables the BSTUN function:

```
bstun peer-name 10.10.254.201
```

Related Commands

Command	Description
bstun protocol-group	Defines a BSTUN group and the protocol it uses.

bstun protocol-group

To define a block serial tunnel (BSTUN) group and the protocol it uses, use the **bstun protocol-group** command in global configuration mode. To delete the BSTUN group, use the **no** form of this command.

bstun protocol-group *group-number protocol*

no bstun protocol-group *group-number protocol*

Syntax Description

group-number	BSTUN group number. Valid numbers are decimal integers in the range from 1 to 255.
protocol	Block serial protocol, selected from the following: • **adplex** • **adt-poll-select** • **adt-vari-poll** • **apos** • **async-generic** • **bsc** • **bsc-local-ack** • **diebold** • **mdi** • mosec • gddb

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.3(2)T	The **apos** keyword was added as a Block serial protocol.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **rxspeed**, **txspeed**, **databits**, **stopbits**, and **parity** line configuration commands must be set to match the device they are communicating with.

Interfaces configured to run the Adplex protocol should set the baud rate set to 4800 bps, use 8 data bits, 1 start bit, 1 stop bit, and use even parity.

Interfaces configured to run the adt-vari-poll and adt-poll-select protocols should set their baud rate set to 600 bps, use 8 data bits, 1 start bit, 1.5 stop bits, and use even parity.

Interfaces configured to run the MDI protocol should set their baud rate set to 4800 bps, 7 data bits, 1 start bit, 2 stop bits, and use odd parity. The MDI protocol allows alarm panels to be sent to the MDI alarm console.

Examples

The following example defines BSTUN group 1, specifies that it uses the Bisync protocol, and indicates that frames will be locally acknowledged:

```
Router(config)# bstun protocol-group 1 bsc-local-ack
```

Related Commands

Command	Description
bstun group	Specifies the BSTUN group to which the interface belongs.

bstun reconnect-interval

To set the amount of time for the system to wait before trying to reconnect to a peer, use the **bstun reconnect-interval** command in global configuration mode. To return to the default setting, use the **no** form of the command.

bstun reconnect-interval *time-value*

no bstun reconnect-interval *time-value*

Syntax Description

time-value	Amount of time (in seconds). The range is from 1 to 600 seconds. The default is 60 seconds.

Defaults

60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to Block Serial Tunneling (BSTUN) route Bisync-to-IP (BIP) connections that are defined as active.

Examples

In the following example, the system is configured to wait 300 seconds before trying to reestablish a peer connection:

```
bstun reconnect-interval 300
```

Related Commands

Command	Description
bstun route (BIP)	Specifies how frames will be forwarded from a BSTUN interface to a remote host over an IP network.

bstun remote-peer-keepalive

To enable detection of the loss of a peer, use the **bstun remote-peer-keepalive** command in global configuration mode. To disable detection, use the **no** form of this command.

bstun remote-peer-keepalive *seconds*

no bstun remote-peer-keepalive

Syntax Description

seconds	Keepalive interval, in seconds. The range is from 1 to 300 seconds. The default is 30 seconds.

Defaults

30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the remote peer keepalive interval is set to 60 seconds:

```
bstun remote-peer-keepalive 60
```

Related Commands

Command	Description
bstun keepalive-count	Defines the number of times to attempt a peer connection before declaring the peer connection to be down.

bstun route

To define how frames will be forwarded from a block serial tunnel (BSTUN) interface to a remote BSTUN peer, use the **bstun route** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

bstun route {**all** | **address** *address-number*} {**tcp** *ip-address* | **interface serial** *number*}

no bstun route {**all** | **address** *address-number*} {**tcp** *ip-address* | **interface serial** *number*}

Syntax Description

all	All BSTUN traffic received on the input interface is propagated, regardless of the address contained in the serial frame.
address	Serial frame that contains a specific address is propagated.
address-number	Poll address, a hexadecimal number from 01 to FF (but not all values are valid). The reply address to be used on the return leg is calculated from the configured poll address.
tcp	TCP encapsulation is used to propagate frames that match the entry.
ip-address	IP address of the remote BSTUN peer.
interface serial	High-level data link control (HLDC) encapsulation is used to propagate the serial frames.
number	Serial line to an appropriately configured router on the other end.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the ADplex protocol is specified in the **bstun protocol-group** command, ADplex device addresses are limited to the range from 1 to 127 because ADplex alarm panels invert the device address in the ADplex frame when responding to alarm console commands.

When the adt-poll-select protocol is specified in the **bstun protocol-group** command, routes for specific addresses cannot be specified on the downstream router (connected to the alarm panel) because no address field is provided within frames that are sent back to the alarm console. The only way to route traffic back to the alarm console is to use the **bstun route all** form of the **bstun route** command. This is also true for the diebold protocol and any other protocol supported by the asynchronous-generic protocol group that does not include a device address in the frame.

When the adt-vari-poll protocol is specified in the **bstun protocol-group** command, ADT device addresses are limited to the range from 0 to 255, and address 0 is reserved for use as a broadcast address for adt-vari-poll only. If address 0 is specified in the **bstun route address** form of the **bstun route** command, the address is propagated to all configured BSTUN peers.

It is possible to use both the **all** and the **address** keywords on different **bstun route** commands on the same serial interface. When this is done, the **address** specifications take precedence; if none of these match, then the **all** specification is used to propagate the frame.

Examples

In the following example, all BSTUN traffic received on serial interface 0 is propagated, regardless of the address contained in the serial frame:

```
bstun route all interface serial 0
```

bstun route (BIP)

To specify how frames will be forwarded from a Block Serial Tunneling (BSTUN) interface to a remote host over an IP network, use the **bstun route** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bstun route {**address** *cu-address*} {**bip** *ip-address*} {**fport** *port-number*} {**lport** *port-number* | **passive**} [**tcp-queue-max**] [**transparent**]

no bstun route {**address** *cu-address*} {**bip** *ip-address*} {**fport** *port-number*} {**lport** *port-number* | **passive**} [**tcp-queue-max**] [**transparent**]

Syntax Description

address	Propagates serial frames that contain a specific address.
cu-address	Control unit poll address for the Bisync end station. This address is a hexadecimal number from 01 to FF.
bip	Specifies that the Bisync-to-IP (BIP) translation form of TCP is to be used for propagating the frames that match the entry.
ip-address	Specifies the IP address of the remote BIP host computer.
fport	Indicates that a foreign or remote port number is either being listened on or connected from.
port-number	Specifies the foreign port number. The port number range is from 1025 to 32000.
lport	Indicates that a local port is being sourced from this router, and represents a specific control unit.
port-number	Specifies a local port number. The port number range is from 1025 to 32000.
passive	Indicates that an outbound connection will not be attempted. Instead, the system listens on port number 1963 for any connection requests from the host computer.
tcp-queue-max	(Optional) Sets the maximum size of the outbound TCP queue. The default is 100 packets.
transparent	(Optional) Specifies the method of sending text on a defined route. The default is nontransparent bisync text.

Defaults

The default is 100 packets.
The default is nontransparent bisync text.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The remote or foreign IP address and port number are required for all connection types.

The user selects the connection type by either configuring a unique local port or by using the **passive** keyword. If the **passive** keyword is used, the foreign port must be unique and the system does not attempt an outbound connection but instead listens on port number 1963 for any connection requests from the host computer. If the **active** keyword is configured (that is, if a local port is configured), the system attempts an outbound connection but also listens for the connection to be established inbound.

The *cu-address* argument is the control unit poll address for the Bisync end station. This address is a hexadecimal number from 01 to FF. Valid addresses vary depending on the setting of the **bsc char-set** interface configuration command.

The TCP queue length, an optional configuration parameter, defaults to 100 packets.

By default, the method of sending text on a defined route is to use nontransparent Bisync text. To send in transparent Bisync text, specify the optional **transparent** keyword.

Examples

In the following example, BSTUN traffic with the control unit address C5 is routed to and from the host computer specified by the IP address 192.168.60.100:

```
bstun route address C5 bip 192.168.60.100 fport 2000 lport 3005
```

Related Commands

Command	Description
bstun group	Specifies the BSTUN group to which the interface belongs.
bstun peer-name	Enables the BSTUN function.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.

bstun route (Frame Relay)

To define how frames will be forwarded from a Block Serial Tunneling (BSTUN interface to a remote BSTUN peer over Frame Relay, use the **bstun route** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

bstun route {**all** | **address** *cu-address*} **interface serial** *number* [**dlci** *dlci rsap*] [**priority** *priority*]

no bstun route {**all** | **address** *cu-address*} **interface serial** *number* [**dlci** *dlci rsap*] [**priority** *priority*]

Syntax Description

all	All BSTUN traffic received on the input interface is propagated, regardless of the address contained in the serial frame.
address	Serial frames that contain a specific address are propagated.
cu-address	Control unit address for the Bisync end station.
interface serial *number*	Specify a serial interface on which Frame Relay encapsulation is used to propagate serial frames.
dlci *dlci*	(Optional) Data-link connection identifier to be used on the Frame Relay interface.
rsap	(Optional) Remoteservice access point (SAP), to be used when initiating an Logical Link Control (LLC)2 session. This argument is configurable only if the interface group number supports local acknowledgment.
priority *priority*	(Optional) Priority port to be used for this LLC2 session. Configurable only if the interface group number supports local acknowledgment.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how toexample shows how to configure BSTUN over Frame Relay. All BSTUN traffic is propagated to serial interface 0 regardless of the address contained in the serial frame:

```
bstun route all interface serial 0 dlci 16
```

bstun route all apip

To define how asynchronous point of sale-to-IP conversion (APIP) frames will be forwarded from a block serial tunnel (BSTUN) interface to an APIP remote peer, use the **bstun route all apip** command in interface configuration mode. To disable the forwarding of APIP frames, use the **no** form of this command.

bstun route all apip *ip-address* [**fport** *port*] [**tcp-queue-max** *size*] [**header** {**vo** | **v1** | **v2**}] [**alternate** *ip-address2* [**dialstring** *phone-number*]]

no bstun route all apip *ip-address* [**fport**] [**tcp-queue-max**] [**header**]

Syntax Description

ip-address	The IP address of the BSTUN peer.
fport	(Optional) Specifies the port number of the remote (foreign) device.
port	(Optional) The remote port number.
tcp-queue-max	(Optional) Customizes the size of the TCP queue.
size	(Optional) The size of the TCP queue.
header	(Optional) Customizes the APIP header version.
v0	(Optional) A two-byte header that includes the header length in the length field.
v1	(Optional) A two-byte header that excludes the header length in the length field.
v2	(Optional) A four-byte header that excludes the header length from the length field.
alternate	(Optional) Specifies an alternate BSTUN peer.
ip-address2	(Optional) The IP address of the BSTUN peer.
dialstring	(Optional) Specifies that the router connects to the alternate BSTUN peer only when it receives the dial string from the POS device. If the connection to the alternate peer fails, a “No Carrier” message is sent to the POS device. If the dial string received from the POS device does not match the configured dial string on the router, then the router connects to the primary BSTUN peer. If the connection to the primary peer fails, a “No Carrier” message is sent to the POS device.
phone-number	(Optional) Dial string sent from the POS device to the router.

Defaults

The **bstun route all apip** command is disabled by default.
port: 10550
size: 100
The default APIP header version is **v0**.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(4)T1	The **alternate** and **dialstring** keywords and *ip-address2* and *phone-number* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There are 2 options for configuring an alternate BSTUN peer: automatic and manual.

- Automatic: Specified by configuring the **alternate** *ip-address2* option. In this situation, if the router is unable to connect to the primary BSTUN peer, the router automatically attempts to connect to the alternate BSTUN peer. The router does not notify the POS device until either the router connects to one of the BSTUN peers or the both connection attempts fail.
- Manual: Specified by configuring the **alternate** *ip-address2* **dialstring** *phone-number* option. In this situation, the router only attempts to connect to the alternate BSTUN peer if the dial string recieved from the POS device matches the dial string specified by the *phone-number* argument. If the connection to the primary peer fails, a “No Carrier” message is sent to the POS device.

Examples

The following example shows a complete APIP configuration. The **bstun route all apip** command is configured such that the primary BSTUN peer is at IP address 10.122.2.1 and the alternate peer is at IP address 10.122.2.2. The router only attempts to connect to the alternate BSTUN peer if the POS device sends it the dialstring 4085555309.

```
bstun peer-name 10.122.2.10
bstun protocol-group 20 apos
bstun remote-peer-keepalive 100
bstun keepalive-count 5
!
interface serial 1
 physical-layer async
 no ip address
 encapsulation bstun
 bstun group 20
 bstun route all apip 10.122.2.1 alternate 10.122.2.2 dialstring 4085555309
 asp role primary
 asp dcd always
!
line 1
 databits 7
 parity even
 stopbits 1
```

certificate reload

To configure Secure Socket Layer (SSL) Encryption Support enabled to read the profile security certificate from the file specified in the **servercert** command, use the **certificate reload** command in customer profile configuration mode.

certificate reload

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Profile configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

The TN3270 server must be configured for security.

Examples

The following example configures the TN3270 server with SSL Encryption Support to read the profile security certificate from the file specified in the **servercert** command:

```
certificate reload
```

Related Commands

Command	Description
servercert	Specifies the location of the TN3270 server's security certificate in the Flash memory.

channel-protocol

To define a data rate of either 3 MBps or 4.5 MBps for Parallel Channel Interfaces, use the **channel-protocol** command in interface configuration mode. To return to the default rate of 3 MBps, use the **no** form of this command.

channel-protocol [s | **s4**]

no channel-protocol

Syntax Description

s	(Optional) Specifies a data rate of 3 MBps.
s4	(Optional) Specifies a data rate of 4.5 MBps.

Defaults

If no value is specified, the default data rate for the Parallel Channel Adapter (PCA) and the Parallel Channel Port Adapter (PCPA) is 3 MBps.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1M.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid on Parallel Channel Interfaces.

Examples

The following example specifies a data rate of 4.5 MBps for the interface:

```
channel-protocol s4
```

claw (backup)

To configure a Common Link Access for Workstations (CLAW) device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and configure individual members of a CLAW backup group for the IP Host Backup feature, use the **claw** command in IP host backup configuration mode. To remove the CLAW device, use the **no** form of this command.

claw *path device-address ip-address host-name device-name host-app device-app* [**broadcast**]

no claw *device-address*

Syntax Description

path	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
device-address	Hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even-numbered value.
ip-address	IP address specified in the HOME statement of the host TCP/IP application configuration file.
host-name	Host name specified in the device statement in the host TCP/IP application configuration file.
device-name	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.
host-app	Host application name as specified in the host application file. When connected to the IBM TCP host offerings, this value will be **tcpip**, which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application.
device-app	CLAW workstation application specified in the host TCPIP application. When connected to the IBM TCP host offerings, this value will be **tcpip**, which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application.
broadcast	(Optional) Enables broadcast processing for this subchannel.

Defaults

No default behavior or values.

Command Modes

IP host backup configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines information that is specific to the hardware interface and the IBM channels supported on the interface.

CLAW devices are used to switch IP packets between a mainframe and a channel-attached router.

At most, 128 statements can be configured per interface because each interface is limited to 256 subchannels. Each CLAW device uses a read channel and a write channel. There is also a restriction of 64 unique paths.

A limit of 32 CLAW device configuration commands is recommended.

Duplicate IP addresses are invalid for nonbackup configurations.

Duplicate IP addresses are permitted if they appear within a backup group of only **claw** or **offload** interface configuration commands. All configuration commands in one backup group must specify the **backup** keyword.

You can use the **path** interface configuration command to specify a number of paths that belong to a backup group. In that case, a **claw** IP host backup configuration command is used that needs no *path* variable or **backup** keyword.

Examples

The following examples show two methods for entering the same IP host backup group information. The first group of commands is the long form, using the **claw** interface configuration command. The second group is the shortcut, using the **path** interface configuration command and a **claw** IP host backup configuration command.

Long form:

```
claw c000 00 10.92.10.5 sysa router1 tcpip tcpip
claw c100 00 10.92.10.5 sysa router1 tcpip tcpip
claw c200 00 10.92.10.5 sysa router1 tcpip tcpip
```

Shortcut form:

```
path c000 c100 c200
  claw 00 10.92.10.5 sysa router1 tcpip tcpip
```

Related Commands

Command	Description
claw (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
show extended channel packing names	Displays CLAW packing names and their connection state.
show extended channel packing stats	Displays CLAW packing statistics.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.

claw (primary)

To configure a Common Link Access for Workstations (CLAW) device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configure individual members of a CLAW backup group for the IP Host Backup feature, use the **claw** command in interface configuration mode. To remove the CLAW device, use the **no** form of this command.

claw *path device-address ip-address host-name device-name host-app device-app* [**broadcast**] [**backup**]

no claw *path device-address*

Syntax Description

path	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
device-address	Hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even-numbered value.
ip-address	IP address specified in the HOME statement of the host TCP/IP application configuration file.
host-name	Host name specified in the device statement in the host TCP/IP application configuration file.
device-name	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.
host-app	Host application name as specified in the host application file. When connected to the IBM TCP host offerings, or if the CLAW packing feature is not enabled on the mainframe TCPIP stack, this value will be **tcpip**, which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application. The value **packed** can be used for the *host-app* argument to enable the CLAW packing feature.
device-app	CLAW workstation application specified in the host TCPIP application. If connected to the IBM TCP host offerings, or if the CLAW packing feature is not enabled on the mainframe TCPIP stack, this value will be **tcpip**, which is the constant specified in the host TCP/IP application file. When attached to other applications, this value must match the value hard coded in the host application. The value **packed** can be used for the *device-app* argument to enable the CLAW packing feature.
broadcast	(Optional) Enables broadcast processing for this subchannel.
backup	(Optional) Enables this CLAW connection to be used as part of a backup group of CLAW connections for the specified IP address.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.
12.0	The following options were added: • **backup** • **packed**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command defines information that is specific to the hardware interface and the IBM channels supported on the interface. When used with the **path** command, the **claw** command provides a quick way to configure a CLAW backup group.

CLAW devices are used to switch IP packets between a mainframe and a channel-attached router.

At most, 128 statements can be configured per interface because each interface is limited to 256 subchannels. Each CLAW device uses a read channel and a write channel. There is also a restriction of 64 unique paths.

A limit of 32 CLAW device configuration commands is recommended.

Duplicate IP addresses are invalid for nonbackup configurations.

Duplicate IP addresses are permitted if they appear within a backup group of only **claw** or **offload** interface configuration commands. All configuration commands in one backup group must specify the **backup** keyword.

You can use the **path** interface configuration command to specify a number of paths that belong to a backup group. In that case, a **claw** IP host backup configuration command is used that needs no *path* variable or **backup** keyword. You can use the **packed** value as an optional keyword for the *host-app* and *device-app* arguments.

Examples

The following example shows how to enable IBM channel attach routing on channel interface 3/0, which is supporting an ESCON direct connection to the mainframe:

```
interface channel 3/0
ip address 172.18.4.49 255.255.255.248
claw c020 F4 172.18.4.52 HOSTB RTRA TCPIP TCPIP
```

The following example shows how to enable CLAW packing:

```
interface Channel 3/0
ip address 172.18.4.49 255.255.255.248
claw c010 F2 172.18.4.50 HOSTA RTRA PACKED PACKED
```

The following example shows how an IP host backup group is specified using the **backup** keyword:

```
interface Channel3/0
 no ip address
 no keepalive
 no shutdown
 claw 0100 C0 10.30.1.2 CISCOVM EVAL TCPIP TCPIP backup
 claw 0110 C0 10.30.1.2 CISCOVM EVAL TCPIP TCPIP backup
 claw 0120 C0 10.30.1.2 CISCOVM EVAL TCPIP TCPIP backup
 claw 0110 C2 10.30.1.3 CISCOVM EVAL TCPIP TCPIP
```

Related Commands

Command	Description
claw (backup)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
show extended channel packing names	Displays CLAW packing names and their connection state.
show extended channel packing stats	Displays CLAW packing statistics.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices.The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection.The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.

clear alps circuits

To remove configured Airline Product Set (ALPS) circuits, use the **clear alps circuits** command in user EXEC or privileged EXEC mode.

clear alps circuits [**ipaddr** *address* | **name** *string*]

Syntax Description

ipaddr *address*	(Optional) Clear ALPS circuits for peer with specified IP address.
name *string*	(Optional) Clear ALPS circuits for peer with specified name.

Defaults

If no IP address or name is specified, the command clears all ALPS circuits.

Command Modes

EXEC

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears the ALPS circuit named CKT1:

```
Router# clear alps circuits name CKT1
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

clear alps counters

To clear all counters relevant to the ALPS feature, use the **clear alps counters** command in user EXEC or privileged EXEC mode.

clear alps counters

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears all counters for the ALPS feature:

```
Router# clear alps counters
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.
show alps circuits	Displays the status of the ALPS circuits.
show alps peers	Displays the status of the ALPS partner peers.

clear bridge

To remove any learned entries from the forwarding database and to clear the transmit and receive counts for any statically or system-configured entries, use the **clear bridge** command in privileged EXEC mode.

clear bridge *bridge-group*

Syntax Description

bridge-group	Bridge group number specified in the **bridge protocol** command.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows the use of the **clear bridge** command:

```
Router# clear bridge 1
```

Related Commands

Command	Description
bridge address	Filters frames with a particular MAC-layer station source or destination address.
bridge protocol	Defines the type of Spanning Tree Protocol.

clear bridge multicast

To clear transparent bridging multicast state information, use the **clear bridge multicast** command in user EXEC or privileged EXEC mode.

clear bridge [*bridge-group*] **multicast** [**router-ports** | **groups** | **counts**]
[*group-address*] [*interface-unit*] [**counts**]

Syntax Description

bridge-group	(Optional) Bridge group number specified in the **bridge protocol** command.
router-ports	(Optional) Clear multicast router ports.
groups	(Optional) Clear multicast groups.
counts	(Optional) Clear RX and TX counts.
group-address	(Optional) Multicast IP address associated with a specific multicast group.
interface-unit	(Optional) Specific interface, such as Ethernet 0.

Defaults

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify arguments or keywords as part of the command, the command clears router ports, group ports, and counts for all configured bridge groups.

Use the **show bridge multicast** command to list transparent bridging multicast state information, then use specific pieces of state information in the **clear bridge multicast** command.

Examples

The following example clears router ports, group ports, and counts for bridge group 1:

```
Router# clear bridge 1 multicast
```

The following example clears the group and count information for the group identified as 235.145.145.223, interface Ethernet 0/3 for bridge group 1:

```
Router# clear bridge 1 multicast groups 235.145.145.223 Ethernet0/3 counts
```

Related Commands

Command	Description
bridge cmf	Enables CMF for all configured bridge groups.
show bridge multicast	Displays transparent bridging multicast state information.

clear dlsw circuit

To cause all data-link switching plus (DLSw+) circuits to be closed, use the **clear dlsw circuit** command in privileged EXEC configuration mode.

clear dlsw circuit [*circuit-id*]

Syntax Description

circuit-id	Circuit ID for a specific remote circuit. The valid range is from 0 to 4294967295.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A user can specify a circuit ID of a specific circuit to clear rather than clearing all circuits.

Caution This command also drops the associated Logical Link Control, type 2 (LLC2) session. The command usage should be used with caution and under the advice of a Cisco engineer.

Examples

The following example closes all DLSw+ circuits:

```
Router# clear dlsw circuit
```

clear dlsw history

To clear all currently inactive circuits from the DLSw+ circuit history, use the **clear dlsw history** privileged EXEC command.

clear dlsw history

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears all inactive circuits from the DLSW+ circuit history:

```
clear dlsw history
```

clear dlsw local-circuit

To cause all locally-switched DLSw+ circuits to be closed, use the **clear dlsw local-circuit** privileged EXEC command.

clear dlsw local-circuit [*circuit-id*]

Syntax Description

circuit-id	Circuit ID for a specific remote circuit. The valid range is 0 to 4294967295.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A user can specify a circuit ID of a specific circuit to clear rather than clearing all local-switched circuits.

Caution This command also drops the associated LLC2 session. The command usage should be used with caution and under the advice of a Cisco engineer.

Examples

The following example closes the locally-switched DLSw+ circuit with ID number 100:

```
clear dlsw local-circuit 100
```

clear dlsw reachability

To remove all entries from the data-link switching plus (DLSw+) reachability cache, use the **clear dlsw reachability** command in privileged EXEC configuration mode.

clear dlsw reachability

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command does not affect existing sessions.

Examples

The following example removes all entries from the DLSw+ reachability cache:

```
Router# clear dlsw reachability
```

clear dlsw statistics

To reset to zero the number of frames that have been processed in the local, remote, and group cache, use the **clear dlsw statistics** command in privileged EXEC configuration mode.

clear dlsw statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example resets to zero the number of frames in the local, remote, and group cache:

```
Router# clear dlsw statistics
```

clear dlsw transparent

To clear DLSw+ transparent local MAC entries, use the **clear dlsw transparent** privileged EXEC command.

clear dlsw transparent

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is designed to be used in networks that employ DLSw+ Ethernet redundancy without transparent mappings.

Examples

The following example clears DLSw+ transparent local MAC entries:

```
clear dlsw transparent
```

clear drip counters

To clear duplicate ring protocol (DRiP) counters from the Route Switch Module (RSM) interfaces, use the **clear drip counters** command in privileged EXEC mode.

clear drip counters

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **clear drip counters** command if you want to check whether the router is receiving any packets. The counters will start at 0. If the counters are incrementing, DRiP is active on the router.

Examples

The following example clears DRiP counters:

```
Router# clear drip counters
```

Related Commands

Command	Description
interface vlan	Configures a Token Ring or Ethernet interface on the RSM.
show drip	Displays the status of the DRiP database.

clear extended counters

To clear the extended interface counters associated with Cisco Mainframe Channel Connection (CMCC) features, use the **clear extended counters** command in user EXEC or privileged EXEC mode.

clear extended counters [**channel** *slot*/*port* [**csna** | **icmp-stack** | **ip-stack** | **llc2** | **statistics** | **tcp-connections** | **tcp-stack** | **tg** | **tn3270-server** | **udp-stack**]]

Syntax Description

channel	(Optional) Specifies a channel interface.
slot	(Optional) Slot number.
port	(Optional) Port number.
csna	(Optional) Clears Cisco Systems Network Architecture (CSNA) feature counters.
icmp-stack	(Optional) Clears Internet Control Message Protocol (ICMP) stack counters.
ip-stack	(Optional) Clears IP stack counters.
llc2	(Optional) Clears Logical Link Control, type 2 (LLC2) counters.
statistics	(Optional) Clears subchannel statistic counters.
tcp-connections	(Optional) Clears TCP connection counters.
tcp-stack	(Optional) Clears TCP stack counters.
tg	(Optional) Clears Transmission Group (TG) counters.
tn3270-server	(Optional) Clears TN3270 server counters.
udp-stack	(Optional) Clears User Datagram Protocol (UDP) stack counters.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid on both the physical and virtual channel interfaces. To clear counters for a selected CMCC feature, you must specify the channel interface on which the feature is configured or running.

Counters displayed using the **show extended channel** EXEC command are cleared using this command.

Entering any form of this command will prompt the user for a confirmation before clearing any counters. A "CLEAR-5-EXT_COUNT" message is displayed to indicate completion of the command.

These counters will be cleared in the **show** commands and remain uncleared when obtained through the Simple Network Management Protocol (SNMP) interface.

Examples

The following example shows how to clear the extended interface counters:

```
Router# clear extended counters
```

Related Commands

Command	Description
show extended channel csna	Displays information about the CSNA subchannels configured on the specified CMCC interface.
show extended channel icmp-stack	Displays information about the ICMP stack running on the CMCC channel interfaces.
show extended channel ip-stack	Displays information about the IP stack running on CMCC channel interfaces.
show extended channel lan	Displays the internal LANs and adapters configured on a CMCC adapter.
show extended channel llc2	Displays information about the LLC2 sessions running on the CMCC adapter interfaces.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel tcp-connections	Displays information about the TCP sockets on a channel interface.
show extended channel tcp-stack	Displays information about the TCP stack running on CMCC adapter interfaces.
show extended channel udp-listeners	Displays information about the UDP listener sockets running on the CMCC adapter interfaces.
show extended channel udp-stack	Displays information about the UDP stack running on the CMCC adapter interfaces.

clear ncia circuit

To drop a specified native client interface architecture (NCIA) circuit, use the **clear ncia circuit** command in privileged EXEC configuration mode.

clear ncia circuit [*id-number*]

Syntax Description

id-number	(Optional) Number assigned to identify the circuit. If no circuit ID number is specified, the command drops all circuits.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If no circuit ID number is specified, the command drops all circuits.

Examples

The following example clears the active NCIA circuit identified as 791F8C:

```
Router# clear ncia circuit 791F8C
```

Related Commands

Command	Description
show ncia circuits	Displays the state of all circuits involving this MAC address as a source and destination.

clear ncia client

To terminate a specified active client connection, use the **clear ncia client** command in privileged EXEC configuration mode.

clear ncia client [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the client. If no IP address is specified in the command, the command terminates all active client connections.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If no IP address is specified in the command, the command terminates all active client connections.

Examples

The following example terminates the active connection to the client identified by the IP address 10.2.20.126:

```
Router# clear ncia client 10.2.20.126
```

Related Commands

Command	Description
show ncia client	Displays the status of the NCIA client.

clear ncia client registered

To release the control block of a specified registered client after terminating the active connection to it, use the **clear ncia client registered** command in privileged EXEC configuration mode.

clear ncia client registered [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the registered client. If no IP address is specified in the command, the command releases the control blocks of all registered clients after terminating any active connections to them.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If no IP address is specified in the command, the command releases the control blocks of all registered clients after terminating any active connections to them.

Examples

The following example terminates the active connection to the registered client identified by the IP address 10.2.20.126 and releases its control block:

```
Router# clear ncia client registered 10.2.20.126
```

Related Commands

Command	Description
show ncia client	Displays the status of the NCIA client.

clear netbios-cache

To clear the entries of all dynamically learned NetBIOS names, use the **clear netbios-cache** command in privileged EXEC mode.

clear netbios-cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software automatically learns NetBIOS names. This command clears those entries. This command will not remove statically defined name cache entries.

Examples

The following example clears all dynamically learned NetBIOS names:

```
Router# clear netbios-cache
```

Related Commands

Command	Description
netbios enable-name-cache	Enables NetBIOS name caching.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.
show netbios-cache	Displays a list of NetBIOS cache entries.

clear rif-cache

To clear the entire Routing Information Field (RIF) cache, use the **clear rif-cache** command in privileged EXEC mode.

clear rif-cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Some entries in the RIF cache are dynamically added and others are static.

Examples

The following example clears the entire RIF cache:

```
Router# clear rif-cache
```

Related Commands

Command	Description
rif	Enters static source-route information into the RIF cache.
rif timeout	Determines the number of minutes an inactive RIF entry is kept. RIF information is maintained in a cache whose entries are aged.
show rif	Displays the current contents of the RIF cache.

clear source-bridge

To clear the source-bridge statistical counters, use the **clear source-bridge** command in privileged EXEC mode.

clear source-bridge

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears the source-bridge statistical counters:

```
Router# clear source-bridge
```

Related Commands

Command	Description
clear bridge	Removes any learned entries from the forwarding database and clears the transmit and receive counts for any statically or system-configured entries.

clear sse

To reinitialize the Silicon Switch Processor (SSP) on the Cisco 7000 series routers with RSP7000, use the **clear sse** command in privileged EXEC mode.

clear sse

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The silicon switching engine (SSE) is on the SSP board in the Cisco 7000 series routers with RSP7000.

Examples

The following example re initializes the SSP:

```
Router# clear sse
```

clear vlan statistics

To remove virtual LAN statistics from any statically or system-configured entries, use the **clear vlan statistics** command in privileged EXEC mode.

clear vlan statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example clears VLAN statistics:

```
Router# clear vlan statistics
```

Related Commands

Command	Description
show vlan counters	Displays the software-cached counter values.

client ip

To add an IP subnet to a client subnet response-time group, use the **client ip** command in response-time configuration mode. To remove an IP subnet from a client subnet response-time group, use the **no** form of this command.

client ip *ip-address* [*ip-mask*]

no client ip *ip-address* [*ip-mask*]

Syntax Description

ip-address	IP subnet being added to the response-time group.
ip-mask	(Optional) Mask applied to a client IP address to determine the client's membership in a client subnet group. When the mask is applied to a connecting client's IP address and the resulting address is equal to the defined IP address, the client becomes a member of the client group. The default mask is 255.255.255.255.

Defaults

The default mask is 255.255.255.255.

Command Modes

Response-time configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example adds an IP subnet to a client subnet response-time group:

```
tn3270-server
response-time group acctg
 client ip 10.1.2.3 255.0.0.0
```

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.

Command	Description
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

client ip lu

To define a specific logical unit (LU) or range of LUs to a client at the IP address or subnet, use the **client ip lu** command in TN3270 PU configuration mode. To cancel this definition, use the **no** form of this command.

client [**printer**] **ip** *ip-address* [*ip-mask*] **lu** *first-locaddr* [*last-locaddr*]

no client [**printer**] **ip** *ip-address* [*ip-mask*] **lu** *first-locaddr* [*last-locaddr*]

Syntax Description

printer	(Optional) Specifies that a client connection from the nailed IP addresses will be nailed to one of the specified LUs only if the client session negotiates a model type of 328*x*, where *x* is any alphanumeric character. Moreover, it ensures that a printer matching the IP address condition can used only an LU nailed as a printer LU. If the **printer** keyword is not specified for any **client** statement that has this IP address set, all model types can use this range of LUs.
ip-address	Specifies the remote client IP address.
ip-mask	(Optional) The mask applied to the remote device address. Multiple client IP addresses in the same subnet can be nailed to the same range of local address.
first-locaddr	Defines a single local address to nail.
last-locaddr	(Optional) Defines the end range of inclusive local address to be nailed from *first-locaddr* to *last-locaddr*.

Defaults

No LUs are nailed. They are all available to any client.

Command Modes

TN3270 PU configuration mode

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. Multiple statements can be configured for one IP address or nail type either on one PU or multiple PUs. But each LU can appear in only one **client** statement.

A client with a nailed IP address can request one of the nailed LUs via the TN3270 device name. If the requested LU is not available then the connection is rejected.

A client with a nailed IP address cannot request an LU outside the range of nailed LUs for its type (screen or printer).

A client with a nonnailed IP address cannot request an LU that is configured as nailed.

The command will be rejected if some of the local address are already nailed. If the local address are in use by other remote clients, the nailing statement will take effect only when the local address is made available.

To cancel the definition, the **no client** form of the command must be entered exactly as the **client** command was originally configured. If a range of local address was specified, to cancel this definition the whole range of local address must be specified. There is no way to cancel only one local address if a whole range of local address was configured.

Examples

In the following example, local address from 1 to 50 are reserved for remote devices in the 10.69.176.0 subnet:

```
interface channel 2/2
 tn3270-server
 pu BAGE4
  client ip 10.69.176.28 255.255.255.0 lu 1 50
```

In the following example, local address 1 to 40 are reserved for screen devices in the 10.69.176.0 subnet, and 41 to 50 are reserved for printers in that subnet:

```
interface channel 2/2
 tn3270-server
 pu BAGE4
  client ip 10.69.176.28 255.255.255.0 lu 1 40
  client printer ip 10.69.176.28 255.255.255.0 lu 41 50
```

In the following example, an attempt to cancel a definition is rejected because it does not specify the full range of local address and the second attempt fails to specify the correct nail type:

```
interface channel 2/2
 tn3270-server
  pu BAGE4
  client printer ip 10.69.176.50 255.255.255.0 lu 1 100
  no client printer ip 10.69.176.50 255.255.255.0 lu 1
  %Invalid LU range specified
  no client ip 10.69.176.50 255.255.255.0 lu 1 100
  %client ip 10.69.176.50 nail type not matched with configured nail type printer
```

Related Commands

Command	Description
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters DLUR PU configuration mode.

client ip pool

To nail clients to pools, use the **client ip pool** command in listen-point configuration mode. To remove clients from pools, use the **no** form of this command.

client ip *ip-address* [*ip-mask*] **pool** *poolname*

no client ip *ip-address* [*ip-mask*] **pool** *poolname*

Syntax Description

ip-address	Remote client IP address.
ip-mask	(Optional) Mask applied to the remote device address. The mask is part of the matching function that determines whether a client is governed by the nailing statement. The default is 255.255.255.255. Multiple client IP addresses in the same subnet can be nailed to the same range of local address.
poolname	Specifies a unique pool name. The pool name cannot exceed eight characters in length.

Defaults

No clients are nailed to pools.

Command Modes

Listen-point configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the pool is configured while logical unit (LU)s are in use, existing clients are allowed to complete their sessions. A pool name can be identical to an LU name. When assigning an LU, the TN3270 server searches the LU name space first for specific requests, such as connections that specify a device name on CONNECT or LU name in the terminal type negotiation. The request is assumed to be directed to the specific LU rather than to the pool. Make sure the name spaces do not clash.

Examples

The following is an example of the **client ip pool** command that nails the client at IP address 10.1.2.3 with an IP mask of 255.255.255.0 to the pool named POOL-1:

```
tn3270-server
 pool POOL-1 cluster layout 10s1p
 listen-point 172.18.4.18
  client ip 10.1.2.3 255.255.255.0 pool POOL-1
```

Related Commands

Command	Description
listen-point	Defines an IP address for the TN3270 server.
pool	Defines pool names for the TN3270 server and specifies the number of screens and printers in each logical cluster.
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

client lu maximum

To limit the number of logical unit (LU) sessions that can be established for each client IP address or IP subnet address, use the **client lu maximum** TN3270 server configuration command. To remove a single LU limit associated with a particular IP address, use the **no** form of this command.

client [*ip-address* [*ip-mask*]] **lu maximum** *number*

no client [*ip-address* [*ip-mask*]]

Syntax Description

ip-address	(Optional) IP address of the client. The value for the *ip* argument is optional when setting the maximum number of LU sessions. If no IP address is specified, then the limit is applied to all clients.
ip-mask	(Optional) IP network mask for the client. The default is 255.255.255.255.
number	(Optional) Maximum number of LU sessions. The allowed value is from 0 to 65535.

Defaults

The default is that there is no limit on the number of concurrent sessions from one client IP address.
The default value for the *ip-mask* argument is 255.255.255.255.
In the **no** form of this command, the default value for the *number* argument is 65535.

Command Modes

TN3270 server configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. An instance of the **client** (lu limit) command on a given tn3270-server is uniquely identified by the *ip-mask* and the logical AND of the *ip-addres*s with that mask. For example, if the command is entered as the following:

```
client 10.1.1.62 255.255.255.192 lu maximum 2
```

Then it will be stored (and subsequently displayed by **write term**) as:

```
client 10.1.1.0 255.255.255.192 lu maximum 2
```

The maximum specified on the command can be changed by reissuing the command with the new value. It is not necessary to remove the command first.

When you use the **no client** command, only the corresponding **client lu maximum** statement is removed, as identified by the IP address and IP address mask combination. You cannot use the **no client** command to specify an unlimited number of LU sessions. The **lu maximum** keyword is optional in the **no** form of the command.

For example, if a service bureau has 8000 clients and each client IP address is limited to four LU sessions, you will never need more than 32000 concurrent LU definitions even when the service is running at 100 percent capacity.

Examples

The following example limits all clients to a maximum of two LU sessions:

```
client lu maximum 2
```

The following example limits a client at IP address 10.1.1.28 to a maximum of three LU sessions:

```
client 10.1.1.28 lu maximum 3
```

The LU limit can be applied to different subnets as shown in the following example. The most exact match to the client IP address is chosen. Clients with IP addresses that reside in the subnet 10.1.1.64 (those with IP addresses in the range from 10.1.1.64 through 10.1.1.127) are limited to a maximum of five LU sessions while other clients with IP addresses in the subnet 10.1.1.0 are limited to a maximum of four LU sessions.

```
client 10.1.1.0  255.255.255.0 lu maximum 4
client 10.1.1.64 255.255.255.192 lu maximum 5
```

The following example prevents an LU session for the client at IP address 10.1.1.28:

```
client 10.1.1.28 lu maximum 0
```

Related Commands

Command	Description
maximum-lus	Limits the number of LU control blocks that will be allocated for TN3270 server use.

client pool

To nail clients to pools, use the **client pool** command in listen-point configuration mode. To remove clients from pools, use the **no** form of this command.

client {[**ip** *ip-address* [*ip-mask*]] | [**name** *DNS-name* [*DNS-domain-identifier*]] | [**domain-name** *DNS-domain*] | [**domain-id** *DNS-domain-identifier*]} **pool** *poolname*

no client {[**ip** *ip-address* [*ip-mask*]] | [**name** *DNS-name* [*DNS-domain-identifier*]] | [**domain-name** *DNS-domain*] | [**domain-id** *DNS-domain-identifier*]} **pool** *poolname*

Syntax Description

ip *ip-address*	Remote client IP address.
ip-mask	(Optional) Mask applied to the remote device address. The mask is part of the matching function that determines whether a client is governed by the nailing statement. The default is 255.255.255.255. Multiple client IP addresses in the same subnet can be nailed to the same pool.
name *DNS-name*	(Optional) Alphanumeric string that specifies a client machine name. The string can contain up to 24 characters. If a valid *DNS-domain-identifier* is not present, this name must be fully qualified. If this name is not fully qualified, any dot that forms the boundary between the Domain Name System (DNS) name and the DNS domain must be included here if it is not already present in the DNS domain.
DNS-domain-identifier	(Optional) A numeric identifier that specifies a domain name. The valid value range is from 1 to 255. Each **domain-id** command statement can have only one *DNS-domain-identifier* value.
domain-name *DNS-domain*	(Optional) Alphanumeric string that specifies a domain name suffix, including all dots (.) but not delimited by dots. The string can contain up to 80 characters. All dots must be included when the string is appended to a configured DNS-name. If the DNS-domain starts with a dot, then the dot must be included if it is not already at the end of the DNS-name.
domain-id *DNS-domain-identifier*	(Optional) Numeric identifier that specifies that a domain name suffix will be appended to the name configured in the **domain-id** command. The valid value range is from 1 to 255. Each **domain-id** command statement can have only one *DNS-domain-identifier* value. The domain id is originally specified in the **domain-id** command.
poolname	Specifies a unique pool name. The pool name cannot exceed eight characters in length.

Defaults

No default behavior or values.

Command Modes

Listen-point configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated in Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to include the **name**, **domain-name**, and **domain-id** keywords. The name of the command was changed from **client ip pool** to **client pool**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the pool is configured while logical units (LU)s are in use, existing clients are allowed to complete their sessions. A pool name can be identical to an LU name. When assigning an LU, the TN3270 server searches the LU name space first for specific requests, such as connections that specify a device name on CONNECT or LU name in the terminal type negotiation. The request is assumed to be directed to the specific LU rather than to the pool. Make sure the LU names do not conflict.

Examples

Nailing Clients to Pools by IP Address

The following is an example of the **client pool** command with the **ip** keyword configured. The command nails the client at IP address 10.1.2.3 with an IP mask of 255.255.255.0 to the pool named POOL-1:

```
tn3270-server
 pool POOL-1 cluster layout 10s1p
 listen-point 172.18.4.18
 client ip 10.1.2.3 255.255.255.0 pool POOL-1
```

Nailing Clients to Pools by Device Name

The following is an example of the **client pool** command with the **name** keyword configured. The command nails the client at device name user1.cisco.com to the pool named POOL-2:

```
tn3270-server
  pool POOL-2  cluster layout 4s1p
  listen-point 172.18.5.168
   pu T240CA   91922363 token-adapter 31 12 rmac 4000.4000.0001
    allocate lu 1 pool POOL-2  clusters 1
  client name user1.cisco.com pool POOL-2
```

Nailing Clients to Pools by Device Name Using a Domain ID

The following is an example of the **client pool** command with the **name** keyword and the optional *DNS-domain-identifier* argument configured. The command nails the client at device name lucy-isdn49.cisco.com to the pool named POOL-2:

```
tn3270-server
 domain-id 23 .cisco.com
  pool POOL-2  cluster layout 4s1p
  listen-point 172.18.5.168
   pu T240CA   91922363 token-adapter 31 12 rmac 4000.4000.0001
    allocate lu 1 pool POOL-2  clusters 1
 client name lucy-isdn49 23 pool POOL-2
```

Nailing Clients to Pools by Domain Name

The following is an example of the **client pool** command with the **domain-name** keyword configured. The command nails any client at domain name cisco.com to the pool named POOL-2:

```
tn3270-server
  pool POOL-2  cluster layout 4s1p
  listen-point 172.18.5.168
   pu T240CA   91922363 token-adapter 31 12 rmac 4000.4000.0001
    allocate lu 1 pool POOL-2  clusters 1
 client domain-name .cisco.com pool POOL-2
```

Nailing Clients to Pools by Domain Name Using a Domain ID

The following is an example of the **client pool** command with the **domain-id** keyword configured. The command nails any client at domain name cisco.com to the pool named POOL-2:

```
tn3270-server
 domain-id 23 .cisco.com
  pool POOL-2  cluster layout 4s1p
  listen-point 172.18.5.168
   pu T240CA   91922363 token-adapter 31 12 rmac 4000.4000.0001
    allocate lu 1 pool POOL-2  clusters 1
 client domain-id 23 pool POOL-2
```

Related Commands

Command	Description
listen-point	Defines an IP address for the TN3270 server.
pool	Defines pool names for the TN3270 server and specifies the number of screens and printers in each logical cluster.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.
domain-id	Specifies a domain name suffix that the TN3270 server appends to a configured machine name to form a fully-qualified name when configuring inverse DNS nailing.

cmpc

To configure a Cisco Multipath Channel (CMPC or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel, use the **cmpc** command in interface configuration mode. To remove a subchannel definition and to deactivate the transmission group, use the **no** form of this command.

cmpc *path device tg-name* {**read** | **write**}

no cmpc *path device*

Syntax Description

path	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
device	Hexadecimal value in the range from 00 to FF. This is the unit address associated with the control unit number and path as specified in the host IOCP file.
tg-name	Name of the CMPC or CMPC+ Transmission Group (TG). The maximum length of the name is eight characters.
read	Same read value as specified in the Transport Resource List (TRL) major node.
write	Same write value as specified in the TRL major node.

Defaults

No default is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.3(4)T	CMPC is no longer available in Cisco IOS release 12.3(4).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Each **cmpc** configuration command in a given CMPC or CMPC+ TG specifies the same TG name. The corresponding **tg** command specifies the same TG name. Together, the **cmpc** and **tg** commands make up the TG specification.

The **cmpc** command defines the read/write subchannel addresses that CMPC or CMPC+ uses to connect to the host. The command corresponds to the definitions in the TRL major node on the host. Configure the **cmpc** command on a Cisco Mainframe Channel Connection (CMCC) adapter physical interface.

Configure one read subchannel and one write subchannel. If CMPC or CMPC+ is configured on a CMCC adapter with two physical interfaces, the read and write CMPC or CMPC+ subchannels may be configured on separate physical interfaces.

The **no cmpc** command deactivates the CMPC or CMPC+ subchannel. If the TG is used for a non-High-Performance Routing (HPR) connection, all sessions using the TG will be terminated immediately. If the TG is an HPR connection, all sessions using the TG will be terminated if no other HPR connection is available to the host.

Examples

The following example configures a read and a write subchannel on path C020 for the CMPC or CMPC+ TG named CONFIGE:

```
cmpc C020 F8 CONFIGE READ
cmpc C020 F9 CONFIGE WRITE
```

Related Commands

Command	Description
tg (CMPC+)	Defines IP connection parameters for the CMPC+ transmission group.
show extended channel cmpc	Displays information about each CMPC or CMPC+ subchannel configured on the specified channel interface.
show extended channel tg	Displays configuration, operational information, and statistics information for CMPC or CMPC+ transmission groups configured on the virtual interface of the specified CMCC adapter.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.

csna

To configure Systems Network Architecture (SNA) support on a Cisco Mainframe Channel Connection (CMCC) physical channel interface, use the **csna** command in interface configuration mode. This command is used to specify the path and device or subchannel on a physical channel of the router to communicate with an attached mainframe. To delete the Cisco Systems Network Architecture (CSNA) device path, use the **no** form of this command.

csna *path device* [**maxpiu** *value*] [**time-delay** *value*] [**length-delay** *value*]

no csna *path device*

Syntax Description

path	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
device	Hexadecimal value in the range from 00 to FF. This is the unit address associated with the control unit number and path as specified in the host IOCP file.
maxpiu *value*	(Optional) Maximum channel I/O block size in bytes that is sent across the physical channel from the CMCC adapter to the attached mainframe. The range is from 4096 to 65535 bytes. The default is 20470 bytes.
time-delay *value*	(Optional) Number of milliseconds (ms) a host-bound SNA frame may be delayed in order to maximize the channel I/O block size. The range is from 0 to 100 ms. The default is 10 ms.
length-delay *value*	(Optional) Amount of SNA frame data in bytes the Cisco Systems Network Architecture (CSNA) subchannel accumulates before sending the accumulated channel I/O block to the attached mainframe. The range is from 0 to 65535 bytes. The default is 20470 bytes.

Defaults

maxpiu *value*: 20470 bytes

time-delay *value*: 10 ms

length-delay *value*: 20470 bytes

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **maxpiu**, **time-delay** and **length-delay** keywords control the characteristics of host-bound traffic for the CSNA subchannel. The channel protocol used by CSNA allows multiple SNA frames to be blocked into one channel I/O block, reducing the channel bandwidth utilization and mainframe and CMCC adapter process utilization.

The **maxpiu** keyword allows you to set the maximum size of a host-bound channel I/O block.

The **time-delay** keyword instructs the CSNA subchannel to delay sending the channel I/O block for the specified time in milliseconds, from the time the first SNA packet is blocked. This can increase the network latency for an SNA packet by up to the specified time delay.

The **length-delay** keyword instructs the CSNA subchannel to delay sending the channel I/O block until it contains the number of bytes specified by the **length-delay** keyword. An accumulated block is sent to the mainframe if one of the following conditions is true:

- **Time delay** expires
- Channel I/O block reaches the **length-delay** size
- Channel I/O block reaches the **maxpiu** size.

A time delay value of 0 instructs the CSNA subchannel to send SNA packets to the mainframe as soon as they are received from the network. A length delay value of 0 instructs the CSNA subchannel to ignore this parameter.

The **no csna** command deactivates and removes the CSNA subchannel configuration. It also deactivates all Logical Link Control, type 2 (LLC2) sessions established over the subchannel.

Examples

The following example shows CSNA, offload, and Common Link Access for Workstations (CLAW) configured on a channel interface. CSNA has no dependencies to CLAW, offload, or CMPC.

```
interface channel 1/0
 no ip address
 no keepalive
 offload c700 c0 172.18.1.127 TCPIP OS2TCP TCPIP TCPIP TCPIP API
 claw C700 c2 172.18.1.219 EVAL CISCOVM AAA BBB
 csna c700 c4
 csna c700 c5 maxpiu 65535 time-delay 100 length-delay 65535
 csna c700 c6 maxpiu 65535 time-delay 100
```

Related Commands

Command	Description
adapter	Configures internal adapters.
lan	Configures an internal LAN on a CMCC adapter interface and enters the internal LAN configuration mode.
show extended channel connection-map llc2	Displays the number of active LLC2 connections for each SAP and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.

Command	Description
show extended channel csna	Displays information about the CSNA subchannels configured on the specified CMCC interface.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.

default-profile

To specify the name of the profile to be applied as a default to all the listen points, use the **default-profile** command in security configuration mode. To disable the default profile specification, use the **no** form of this command.

default-profile *profilename*

no default-profile *profilename*

Syntax Description

profilename	A profile name that has already been configured.

Defaults

No default profile.

Command Modes

Security configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is configured, this profile name and all of its attributes will be associated with all listen points that do not specify an individual profile with the **sec-profile** command.

Profile names cannot be duplicated.

Entering the **no** form of this command removes the default specification and any listen points that do not have the **sec-profile** command specified will revert to a nonsecure mode.

This command has no retroactive effect. If a listen point is specified using the **listen-point** command, and the **sec-profile** command was already configured for that listen point, then all client connections to that listen point will be secure.

If a listen point is specified using the listen-point command, and the **default-profile** command is not configured, then all client connections to that listen point will not be secure. However, if the **default-profile** command is later configured, then all now connections to that listen point will be secure using the specified **default-profile** command. This will not affect the nonsecure connections.

Examples

The following example specifies DOMESTIC as the default profile name for all clients connecting to listen point 10.10.10.1 until the **default-profile LAM** command is configured. Once the **default-profile LAM** command is configured, all new client connections will use LAM as the default profile.

```
tn3270
 security
 profile NOSECURITY none
 default-profile DOMESTIC
pu DIRECT 012ABCDE tok 0 04
 default-profile LAM
listen-point 10.10.10.1
```

Related Commands

Command	Description
profile	Specifies a name and a security protocol for a security profile and enters profile configuration mode.
sec-profile	Specifies the security profile to be associated with a listen point.

disable (TN3270)

To turn off security in the TN3270 server, use the **disable** (TN3270) command in security configuration mode.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Security configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring the **disable** command does not terminate any active secure or nonsecure connections. This command specifies that all new connections established with the TN3270 server will be nonsecure. If a client initiates a change cipher specification for an existing secure connection, then the TN3270 server will process the request.

There is not a **no** form for this command. The **enable** command is equivalent to the **no** form of this command.

Examples

The following example turns off security in the TN3270 server so that all new connections established with the TN3270 server will be nonsecure:

```
disable
```

Related Commands

Command	Description
enable (TN3270)	Turns on security in the TN3270 server.

dlsw allroute-netbios

To change the single-route explorer to an all-route broadcast for NetBIOS, use the **dlsw allroute-netbios** command in global configuration mode. To return to the default single-route explorer, use the **no** form of this command.

dlsw allroute-netbios

no dlsw allroute-netbios

Syntax Description

This command has no arguments or keywords.

Defaults

Single-route explorer.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies all-route broadcasts for NetBIOS:

```
dlsw allroute-netbios
```

dlsw allroute-sna

To change the single-route explorer to an all-route broadcast for Systems Network Architecture (SNA), use the **dlsw allroute-sna** command in global configuration mode. To return to the default single-route explorer, use the **no** form of this command.

dlsw allroute-sna

no dlsw allroute-sna

Syntax Description

This command has no arguments or keywords.

Defaults

Single-route explorer.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies all-route broadcasts for SNA:

```
dlsw allroute-sna
```

dlsw bgroup-list

To map traffic on the local Ethernet bridge group interface to remote peers, use the **dlsw bgroup-list** command in global configuration mode. To cancel the map, use the **no** form of this command.

dlsw bgroup-list *list-number* **bgroups** *number*

no dlsw bgroup-list

Syntax Description

list-number	The ring list number. This number is subsequently used in the **dlsw remote-peer** command to define the segment to which the bridge group should be applied. The valid range is from 1 to 255.
bgroups *number*	The transparent bridge group list number. The valid range is from 1 to 63.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Traffic received from a remote peer is forwarded only to the bridge group specified in the bridge group list. Traffic received from a local interface is forwarded to peers if the input bridge group number appears in the bridge group list applied to the remote peer definition. The definition of a bridge group list is optional. Each remote peer has a single list number associated with it; therefore, if you want traffic to go to a bridge group and to either a ring list or port list, you should specify the same list number in each definition.

Examples

The following example configures bridge group list 1:

```
dlsw bgroup-list 1 bgroups 33
```

Related Commands

Command	Description
dlsw bridge-group	Links data-link switching plus (DLSw+) to the bridge group of the Ethernet LANs.
dlsw ring-list	Configures a ring list, mapping traffic on a local interface to remote peers.

dlsw bridge-group

To link data-link switching plus (DLSw+) to the bridge group of the Ethernet LANs, use the **dlsw bridge-group** command in global configuration mode. To disable the link, use the **no** form of this command.

dlsw bridge-group *group-number* [**llc2** [**N2** *number*] [**ack-delay-time** *milliseconds*] [**ack-max** *number*] [**idle-time** *milliseconds*] [**local-window** *number*] [**t1-time** *milliseconds*] [**tbusy-time** *milliseconds*] [**tpf-time** *milliseconds*] [**trej-time** *milliseconds*] [**txq-max** *number*] [**xid-neg-val-time** *milliseconds*] [**xid-retry-time** *milliseconds*]] [**locaddr-priority** *lu address priority list number*] [**sap-priority** *priority list number*]

no dlsw bridge-group *group-number* [**llc2** [**N2** *number*] [**ack-delay-time** *milliseconds*] [**ack-max** *number*] [**idle-time** *milliseconds*] [**local-window** *number*] [**t1-time** *milliseconds*] [**tbusy-time** *milliseconds*] [**tpf-time** *milliseconds*] [**trej-time** *milliseconds*] [**txq-max** *number*] [**xid-neg-val-time** *milliseconds*] [**xid-retry-time** *milliseconds*]] [**locaddr-priority** *lu address priority list number*] [**sap-priority** *priority list number*]

Syntax Description

group-number	Transparent bridge group to which DLSw+ will be attached. The valid range is from 1 to 63.
llc2	(Optional) Logical Link Control, type 2 (LLC2) interface subcommands.
N2 *number*	(Optional) Number of times router should retry various operations. The valid range is from 1 to 255.
ack-delay-time *milliseconds*	(Optional) Maximum time the router allows incoming I-frames to stay unacknowledged. The valid range is from 1 to 60000.
ack-max *number*	(Optional) Maximum number of I-frames received before an acknowledgment must be sent. The valid range is from 1 to 255.
idle-time *milliseconds*	(Optional) Frequency of polls during periods of idle traffic. The valid range is from 1 to 60000.
local-window *number*	(Optional) Maximum number of I-frames to send before waiting for an acknowledgment. The valid range is from 1 to 127.
t1-time *milliseconds*	(Optional) Amount of time the router waits for an acknowledgment to sent I-frames. The valid range is from 1 to 60000.
tbusy-time *milliseconds*	(Optional) Amount of time the router waits while the other LLC2 station is in a busy state before attempting to poll the remote station. The valid range is from 1 to 60000.
tpf-time *milliseconds*	(Optional) Amount of time the router waits for a final response to a poll frame before resending the original poll frame. The valid range is from 1 to 60000.
trej-time *milliseconds*	(Optional) Amount of time the router waits for a resend of a rejected frame before sending the reject command. The valid range is from 1 to 60000.
txq-max *number*	(Optional) Queue for holding LLC2 information frames. The valid range is from 20 to 200.
xid-neg-val-time *milliseconds*]	(Optional) Frequency of exchange of identification (XID). The valid range is from 1 to 60000.

xid-retry-time *milliseconds*	(Optional) Amount of time the router waits for reply to XID. The valid range is from 1 to 60000.
locaddr-priority *lu address priority list number*	(Optional) Assigns an input Systems Network Architecture (SNA) logical unit (LU) address priority list to this bridge group. The valid range is from 1 to 10.
sap-priority *priority list number*	(Optional) Assigns an input service access point (SAP) priority list to this bridge group. The valid range is from 1 to 10.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guideliness

More than one bridge group can be attached to DLSw+ by using this command multiple times. Multiple bridge group support is available in Cisco IOS Release 11.3.

Examples

The following example links DLSw+ to bridge groups 1, 2, and 3:

```
dlsw local-peer peer-id 1.1.1.1
dlsw remote-peer 0 tcp 2.2.2.2
dlsw bridge-group 1
dlsw bridge-group 2
dlsw bridge-group 3

interface Ethernet0
 bridge-group 1

interface Ethernet1
 bridge-group 2

interface Ethernet2
 bridge-group 3

bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
```

Related Commands

Command	Description
dlsw bgroup-list	Maps traffic on the local Ethernet bridge group interface to remote peers.

dlsw cache-ignore-netbios-datagram

To prevent data-link switching (DLSw) from caching NetBIOS names when a datagram (0x08) NetBIOS command is received, use the **dlsw cache-ignore-netbios-datagram** command in global configuration mode. To remove the filter, use the **no** form of this command.

dlsw cache-ignore-netbios-datagram

no dlsw cache-ignore-netbios-datagram

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example helps maintain a smaller name cache:

```
dlsw cache-ignore-netbios-datagram
```

dlsw disable

To disable data-link switching plus (DLSw+) without altering the configuration, use the **dlsw disable** command in global configuration mode. To reenable DLSw+, use the **no** form of this command.

dlsw disable

no dlsw disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example reenables DLSw+:

```
no dlsw disable
```

dlsw duplicate-path-bias

To specify how data-link switching plus (DLSw+) handles duplicate paths to the same MAC address or NetBIOS name, use the **dlsw duplicate-path-bias** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw duplicate-path-bias [**load-balance**]

no dlsw duplicate-path-bias [**load-balance**]

Syntax Description

load-balance	(Optional) Specifies that sessions are load-balanced across duplicate paths.

Defaults

Fault tolerance is the default logic used to handle duplicate paths.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A path is either a remote peer or a local port.

In full-tolerance mode, the preferred path is always used unless it is unavailable. The preferred path is either the path over which the first response to an explorer was received, or, in the case of remote peers, the peer with the least cost.

Examples

The following example specifies load balancing to resolve duplicate paths:

```
dlsw duplicate-path-bias load-balance
```

dlsw explorerq-depth

To establish queue depth for multiple queues that handle various types of explorer traffic, including Systems Network Architecture (SNA) and NetBIOS frames, use the **dlsw explorerq-depth** command in global configuration mode. To remove the queues, use the **no** form of this command.

dlsw explorerq-depth {**sna** *value* | **netbios** *value* | **other** *value*}

no dlsw explorerq-depth {**sna** *value* | **netbios** ***value*** | **other** *value*}

Syntax Description

sna *value*	Establishes queue depth for SNA frames. The valid range is from 10 to 1000. The default is unlimited.
netbios *value*	Establishes queue depth for NetBIOS frames. The valid range is from 10 to 1000. The default is unlimited.
other *value*	Establishes queue depth for unnumbered information (UI) frames. The valid range is from 10 to 1000. The default is 100.

Defaults

The default value for the **sna** queue and **netbios** queue is unlimited (that is, if no value is specified, there is no threshold for these queues). The default for the **other** queue is 100.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3 (1)	This command was removed from Cisco IOS software.
12.1 (3)T	This command was reintroduced to Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **dlsw explorererq-depth** command allows data-link switching plus (DLSw+) to establish queue depth for multiple queues that handle different types of traffic, including SNA and NetBIOS frames. UI frames are handled by the **other** queue. Using multiple queues, the SNA and NetBIOS frames will take priority over the UI frames. The UI frames will be dropped when the **other** queue reaches its threshold.

The **dlsw explorererq-depth** command is used in an Ethernet and transparent-bridging environment.

Examples

The following example specifies the maximum number of explorers allowed in the SNA queue:

```
dlsw explorerq-depth sna 100
```

Related Commands

Command	Description
source-bridge explorerq-depth	Sets the maximum explorer queue depth.

dlsw group-cache disable

To disable the border peer caching feature, use the **dlsw group-cache disable** command in global configuration mode. To return to the default peer caching feature, use the **no** form of this command.

dlsw group-cache disable

no dlsw group-cache disable

Syntax Description

This command has no arguments or keywords.

Defaults

Border peer caching is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a border peer becomes a nonborder peer, then the group cache is automatically deleted.

This command prevents a border peer from learning reachability information from relay responses. This command also prevents a border peer from using local or remote caches to make forwarding decisions.

Examples

The following example disables the group cache:

```
dlsw group-cache disable
```

Related Commands

Command	Description
dlsw group-cache max-entries	Limits the number of entries in the group cache.

dlsw group-cache max-entries

To limit the number of entries in the group cache, use the **dlsw group-cache max entries** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw group-cache max-entries *number*

no dlsw group-cache max entries

Syntax Description

number	Maximum number of entries allowed in the group cache. The valid range is from 0 through 12000. If the value is set to 0, then there is no limit to the number of entries. The default is 2000.

Defaults

The default setting is 2000.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Once the number of entries has reached the maximum number specified, if a new entry needs to be added an entry will be removed to make room.

The value set for the *number* argument applies to both the NetBIOS and Systems Network Architecture (SNA) group cache.

Examples

The following configuration defines the maximum number of entries allowed in the NetBIOS or SNA group cache as 1800:

```
dlsw group-cache max-entries 1800
```

Related Commands

Command	Description
dlsw group-cache disable	Disables the border peer caching feature.

dlsw history-log

To enable the data-link switching (DLSw) history log, use the **dlsw history-log** command in global configuration mode. To disable the DLSw history log, use the **no** form of this command.

dlsw history-log *size* [**connected-only**] [**ignore-info-frames**]

no dlsw history-log

Syntax Description

size	Specifies the number of circuits for which to retain history. The history size per circuit is fixed at the last 16 events. The *size* argument can range from 16 to 65536. The default value is 32.
connected-only	(Optional) Specifies that history will be recorded only for circuits that reach the CONNECTED state, and only finite state machines (FSM) events following the move to the CONNECTED state will be retained.
ignore-info-frames	(Optional) Specifies that the following FSM events will not be recorded in the history: • WAN infoframe • WAN dgmframe • Data-link control (DLC) udata.ind • DLC data.ind

Defaults

The DLSw history log is enabled with a value of 32 for the *size* argument.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The command was enabled by default with a value of 32 for the *size* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the DLSw history log size to 2000 circuits and specifies that history be recorded only for circuits that reach the CONNECTED state:

```
router(config)# dlsw history-log 2000 connected-only
```

dlsw icannotreach saps

To configure a list of service access points (SAPs) not locally reachable by the router, use the **dlsw icannotreach saps** command in global configuration mode. To remove the list, use the **no** form of this command.

dlsw icannotreach saps *sap*

no dlsw icannotreach saps *sap*

Syntax Description

sap	One or more SAPs, separated by spaces.

Defaults

No lists are configured.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **dlsw icannotreach saps** command causes the local router to send a control vector to its peers during the capabilities exchange, which tells the peers not to send canureach messages to the local router for sessions using those destination service access point (DSAP)s. (They are DSAPs from the peer's perspective, and source service access point (SSAP)s from the perspective of the devices attached to the local router.) The effect is that devices attached to the peer will not be able to initiate sessions to devices attached to the local router using the listed DSAPs. Devices attached to the local router, however, will still be able to start sessions with devices on its peers using the listed SAP as SSAPs. The reason is that the local router can still send canureach requests to its peers,because no filtering is actually done on the local router. The filtering done by the peers does not prohibit the peers from responding to canureach requests from the local router sending the control vector, only sending canureach requests to the local router.

Examples

The following example specifies that NetBIOS traffic will be denied:

```
dlsw icannotreach saps F0
```

dlsw icanreach

To configure a resource that is locally reachable by this router, use the **dlsw icanreach** command in global configuration mode. To remove the resource, use the **no** form of this command.

dlsw icanreach {**mac-exclusive** [**remote**] | **netbios-exclusive** [**remote**] | **mac-address** *mac-addr* [**mask** *mask*] | **netbios-name** *name* | **saps** *sap-value*}

no dlsw icanreach {**mac-exclusive** [**remote**] | **netbios-exclusive** [**remote**] | **mac-address** *mac-add* [**mask** *mask*] | **netbios-name** *name* | **saps** *sap-value*}

Syntax Description

mac-exclusive	Router can reach only the MAC addresses that are user configured.
remote	(Optional) Gives the MACs (that are local to the router and that are not already defined in the **dlsw icanreach mac-address** *mac-addr* command) access to remote MAC addresses.
netbios-exclusive	Router can reach only the NetBIOS names that are user configured.
remote	(Optional) Gives the NetBIOS workstations (that are local to the router and that are not already defined in the **dlsw icanreach netbios-name** *name* command) access to remote servers.
mac-address *mac-addr*	Configures a MAC address that this router can locally reach.
mask *mask*	(Optional) MAC address mask in hexadecimal *h.h.h*. The “f” value represents the “care” bit and the “0” value represents the “don’t care” bit. The mask indicates which bits in the MAC address are relevant.
netbios-name *name*	Configures a NetBIOS name that this router can locally reach. Wildcards (*) are allowed at the end of the name. Trailing white spaces are ignored when comparing against an actual name in a NetBIOS frame.
saps	Configures a list of SAPs that are locally reachable by this router.
sap-value	Even SAP value, in hex.

Defaults

No resources are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be entered at any time. It causes a capabilities exchange to relay the information to all active peers. By specifying resource names or MAC addresses in this command, you can avoid broadcasts from remote peers that are looking for this resource. By specifying “exclusive” you can avoid broadcasts to this router or any resources. For example, you could configure the front-end processor (FEP) MAC address or corporate site LAN servers in central site routers to avoid any broadcasts over the WAN for these resources.

Configuring the **remote** keyword gives the NetBIOS workstations and MACs that are local to the router and that are not already defined in the **dlsw icanreach netbios-name** *name* and **dlsw icanreach mac-address** *mac-addr* commands access to remote NetBIOS servers and remote MAC addresses. The connection must be from the local Netbios workstation or MAC address to the remote Netbios Server or MAC address.

In the default case (where the **remote** keyword is not specified), a local NetBIOS station that is not configured in the **icanreach netbios-name** list will not be able to make a connection in this router over data-link switching plus (DLSw+), whether incoming or outgoing.

Note Because the configuration of the **mac-address** and **netbios-name** keywords prevents the DLSw+ peer from exploring, an incorrect configuration could prevent DLSw+ from being able to find a resource actually available elsewhere in the network.

Examples

The following example indicates that this peer has information only has information about a single NetBIOS server, and that no peers should send this peer explorers searching for other NetBIOS names. Because the **remote** option is also configured, NetBIOS workstations that are connected to the NetBIOS server named lanserv will be able to establish a DLSw+ connection:

```
dlsw icanreach netbios-exclusive
dlsw icanreach netbios-name lanserv
```

Related Commands

Command	Description
show dlsw capabilities	Displays the configuration of a specific peer or all peers.

dlsw llc2 nornr

To prevent the receiver not ready (RNR) message from being sent while establishing a Logical Link Control, type 2 (LLC2) connection, use the **dlsw llc2 nornr** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw llc2 nornr

no dlsw llc2 nornr

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used when any device does not handle the LLC2 RNR frames.

Examples

The following example keeps the receiver not ready (RNR) message from being sent when establishing an LLC2 connection:

```
dlsw llc2 nornr
```

The following is output from a Sniffer trace showing when use of the **dlsw llc2 nornr** command would be appropriate because the RNR message is being rejected from the front-end processor (FEP) when the router is trying to establish an LLC2 connection:

```
SUMMARY  Delta T    From 400020401003                 From 400023491026
8      0.173                                    LLC C D=00 S=04 TEST P
9      0.003   LLC R D=04 S=00 TEST F
10     0.002                                    SNA XID Fmt 2 T4
11     0.059   SNA XID Fmt 2 T4
12     0.004                                    SNA XID Fmt 2 T4
13     0.065   SNA XID Fmt 2 T4
14     0.005                                    SNA XID Fmt 2 T4
16     0.054   LLC C D=04 S=04 SABME P
17     0.003                                    LLC R D=04 S=04 UA
```

The router sends an RNR message:

```
18    0.001   LLC C D=04 S=04 RNR NR=0
```

From frames 19 to 35, the FEP does not respond:

```
19    0.002   LLC C D=04 S=04 RR NR=0
20    0.048   SNA  C NC  NC-ER-OP
21    0.997   LLC C D=04 S=04 RR NR=0 P
22    1.000   LLC C D=04 S=04 RR NR=0 P
24    1.000   LLC C D=04 S=04 RR NR=0 P
25    1.000   LLC C D=04 S=04 RR NR=0 P
31    1.000   LLC C D=04 S=04 RR NR=0 P
32    1.000   LLC C D=04 S=04 RR NR=0 P
34    1.000   LLC C D=04 S=04 RR NR=0 P
35    1.000   LLC C D=04 S=04 RR NR=0 P
```

The router disconnects the circuit:

```
37    1.000   LLC C D=04 S=04 DISC P
38    0.002                                  LLC R D=04 S=04 UA F
```

The sequence repeats:

```
39    0.179                                  LLC C D=00 S=04 TEST P
41    0.767   SNA XID Fmt 2 T4
42    0.634   SNA XID Fmt 2 T4
43    0.173                                  LLC C D=00 S=04 TEST
44    0.003   LLC R D=04 S=00 TEST F
45    0.002                                  SNA XID Fmt 2 T4
46    0.060   SNA XID Fmt 2 T4
47    0.004                                  SNA XID Fmt 2 T4
48    0.063   SNA XID Fmt 2 T4
49    0.005                                  SNA XID Fmt 2 T4
```

dlsw load-balance

To enable load balancing and to select either round robin or circuit-count-based load balancing, use the **dlsw load-balance** command in global configuration mode. To disable the previous assignments, use the **no** form of this command.

dlsw load-balance [**round-robin** | **circuit-count** *circuit-weight*]

no dlsw load-balance [**round-robin** | **circuit-count** *circuit-weight*]

Syntax Description

round-robin	(Optional) Enables round-robin type of load balancing.
circuit-count *circuit-weight*	(Optional) Enables the data-link switching plus (DLSw+) Enhanced Load Balancing feature. The value represents the default circuit weight to be used for the peers that are not explicitly configured with a circuit-weight value in the **dlsw remote-peer tcp** command. The valid range is from 1 to 100.

Defaults

Fault-tolerant mode is the default setting. The default value for the *circuit weight* argument is 10.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A circuit is never be taken down and reestablished by the code in an attempt to rebalance the load. The DLSw+ Enhanced Load Balancing feature changes the decision-making process only at the time a new circuit is desired.

The **dlsw load-balance** command replaces the **dlsw duplicate-path-bias load balance** command. The latter command continues to be accepted, however, it will be converted to the new command if the configuration is displayed or saved.

Examples

The following example enables the DLSw+ Enhanced Load Balancing feature:

```
dlsw load-balance circuit-count 10
```

dlsw local-peer

To define the parameters of the data-link switching plus (DLSw+) local peer, use the **dlsw local-peer** command in global configuration mode. To cancel the definitions, use the **no** form of this command.

dlsw local-peer [**cluster** *cluster-id*] [**peer-id** *ip-address*] [**group** *group*] [**border**] [**cost** *cost*] [**lf** *size*] [**keepalive** *seconds*] [**passive**] [**promiscuous**] [**biu-segment**] [**init-pacing-window** *size*] [**max-pacing-window** *size*]

no dlsw local-peer [**cluster** *cluster-id*] [**peer-id** *ip-address*] [**group** *group*] [**border**] [**cost** *cost*] [**lf** *size*] [**keepalive** *seconds*] [**passive**] [**promiscuous**] [**biu-segment**] [**init-pacing-window** *size*] [**max-pacing-window** *size*]

Syntax Description

cluster *cluster-id*	(Optional) Implements the DLSw+ Peer Clusters feature and defines the router as part of a particular cluster. The valid range is from 1 to 255.
peer-id *ip-address*	(Optional) Local peer IP address. This address is required when Fast-Sequenced Transport (FST) or TCP is used.
group *group*	(Optional) Peer group number for this router. The valid range is from 1 to 255.
border	(Optional) Enables the router as a border peer. The **group** option must be specified to use the border peer option.
cost *cost*	(Optional) Peer cost advertised to remote peers in the capabilities exchange. The valid range is from 1 to 5.
lf *size*	(Optional) Largest frame size for this local peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
keepalive *seconds*	(Optional) Default remote peer keepalive interval in seconds. The valid range is from 0 to 1200 seconds. The default is 30 seconds. The value 0 means no keepalives.
passive	(Optional) Specifies that this router does not initiate remote peer connections to configured peers.
promiscuous	(Optional) Accept connections from nonconfigured remote peers.
biu-segment	(Optional) DLSw+ spoofs the maximum receivable I-frame size in exchange identification (XID) so that each end station sends its largest frame.
init-pacing-window *size*	(Optional) Size of the initial pacing window as defined in RFC 1795. The valid range is from 1 to 2000.
max-pacing-window *size*	(Optional) Maximum size of the pacing window as defined in RFC 1795. The valid range is from 1 to 2000.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The **cluster** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When there are multiple peers to a given destination, use the **cost** keyword to determine which router is preferred and which is capable. The **cost** keyword applies only in fault tolerance mode.

The **biu-segment** option is a performance and utilization improvement. If a frame that arrives from a remote peer is too large for the destination station to handle, DLSw+ segments the frame. If you choose to implement this option, you must add the option to both DLSw peer partners.

Examples

The following command defines the local peer IP address and specifies the peer group number for this router:

```
dlsw local-peer peer-id 10.2.17.1 group 2
```

Related Commands

Command	Description
dlsw duplicate-path-bias	Specifies how DLSw+ handles duplicate paths to the same MAC address or NetBIOS name.
show dlsw capabilities	Displays the configuration of a specific peer or all peers.

dlsw mac-addr

To configure a static MAC address, use the **dlsw mac-addr** command in global configuration mode. To cancel the configuration, use the **no** form of this command.

dlsw mac-addr *mac-addr* {**ring** *ring-number* | **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*}| **rif** *rif-string* | **group** *group*}

no dlsw mac-addr *mac-addr* {**ring** *ring -number*| **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*}| **rif** *rif-string* | **group** *group*}

Syntax Description

mac-addr	Specifies the MAC address.
ring *ring-number*	Maps the MAC address to a ring number or ring group number. The valid range is from 1 to 4095.
remote-peer	Maps the MAC address to a specific remote peer.
interface serial *number*	Specifies the remote peer by direct serial interface.
ip-address *ip-address*	Specifies the remote peer by IP address.
rif *rif-string*	Maps the MAC address to a local interface using a Routing Information Field (RIF) string. The RIF string describes a source-routed path from the router to the MAC address. It starts at the router's ring group and ends on the ring where the MAC address is located. The direction is from the router toward the MAC address. See the IEEE 802.5 standard for details.
group *group*	Maps the MAC address to a specified peer group. Valid numbers are in the range from 1 to 255.

Defaults

No static MAC address is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can statically define resources to prevent the Cisco IOS software from sending explorer frames for the specified resource. For example, you can include the MAC address of a front-end processor (FEP) in the configuration for each remote router to eliminate any broadcasts that are searching for a FEP.

Alternately, you can specify a single **dlsw icanreach** statement in the router attached to the FEP indicating the MAC address of the FEP. This information is sent to all remote routers as part of the capabilities exchange.

Note Because the configuration of this command prevents the data-link switching plus (DLSw+) peer from exploring, an incorrect configuration could prevent DLSw+ from being able to find a resource actually available elsewhere in the network.

Examples

The following example maps the static MAC address 1000.5A12.3456 to the remote peer at IP address 10.17.3.2:

```
dlsw mac-addr 1000.5A12.3456 remote-peer ip-address 10.17.3.2
```

Related Commands

Command	Description
show dlsw reachability	Displays DLSw+ reachability information.

dlsw max-multiple-rifs

To enable caching of multiple Routing Information Field (RIF)s per interface, use the **dlsw max-multiple-rifs** command in global configuration mode. To turn off the feature, use the **no** form of this command.

dlsw max-multiple-rifs *multiple-rifs-per-port*

no dlsw max-multiple-rifs *multiple-rifs-per-port*

Syntax Description

multiple-rifs-per-port	Number of multiple RIF entries per interface. The valid range is from 1 to 4. The default value is 1.

Defaults

The default value is 1.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A MAC address or NetBIOS name can have several RIF entries. Prior to this command, data-link switching plus (DLSw+) could cache only one of these RIF entries per local Token Ring port. With the **dlsw max-multiple-rifs** command configured, however, DLSw+ can cache multiple RIF entries (up to four) for a specific MAC address or NetBIOS name on one Token Ring port.

If the value 1 is specified, multiple RIF caching is not enabled.

Examples

The following example enables the router to cache up to two RIFs per interface:

```
dlsw max-multiple-rifs 2
```

dlsw multicast

To enable a DLSw router to participate in a multicast group, use the **dlsw multicast** command in global configuration mode. To remove the router from the multicast group, use the **no** form of this command.

dlsw multicast [*multicast-ip-address*]

no dlsw multicast [*multicast-ip-address*]

Syntax Description

multicast-ip-address	(Optional) The IP address used by the multicast group. The default is 224.0.10.0.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In order for routers to be able to receive multicast traffic through DLSw, they must be properly configured to receive multicasts. The appropriate multicast configuration will depend on the specific topologies used.

The **dlsw multicast** command is implemented together with the DLSw version 2 support (RFC2166). It allows anybody-to-anybody communication without configuring a full mesh of the DLSw peers.

Examples

The following example configures a router to be part of the multicast group using 224.0.11.0 as the multicast address:

```
dlsw local-peer peer-id 172.18.62.11 promiscuous
dlsw multicast 224.0.11.0
```

dlsw netbios-cache-length

To customize the number of characters of a NetBIOS name that are retained in the cache, use the **dlsw netbios-cache-length** command in global configuration mode. To restore the default cache length, use the **no** form of this command.

dlsw netbios-cache-length [**15** | **16**]

no dlsw netbios-cache-length

Syntax Description

15	The first 15 characters of NetBIOS names are cached.
16	The full 16 characters of NetBIOS names are cached.

Defaults

The first 15 characters of NetBIOS names are cached.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)	This command was introduced.
12.3(4)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configure the cache length to 16 characters only if the router will be dealing with NetBIOS names that differ only in the 16th byte.

Examples

The following example configures the cache to retain the full 16 characters of the NetBIOS name:

```
router(config)# dlsw netbios-cache-length 16
```

The following command restores the default behavior of caching only the first 15 characters of the NetBIOS name:

```
router(config)# no dlsw netbios-cache-length
```

dlsw netbios-keepalive-filter

To enable the NetBIOS dial-on-demand routing (DDR) feature, use the **dlsw netbios-keepalive-filter** command in global configuration mode. To turn off the feature, use the **no** form of this command.

dlsw netbios-keepalive-filter

no dlsw netbios-keepalive-filter

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Refer to the "Cisco IOS Bridging and IBM Networking Overview" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide* for more details on the NetBIOS DDR feature.

Examples

The following example enables NetBIOS DDR:

```
dlsw netbios-keepalive-filter
```

dlsw netbios-name

To configure a static NetBIOS name, use the **dlsw netbios-name** command in global configuration mode. To cancel the configuration, use the **no** form of this command.

dlsw netbios-name *netbios-name* {**ring** *ring-number* | **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*}| **rif** *rif-string* | **group** *group*}

no dlsw netbios-name *netbios-name* {**ring** *ring-number* | **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*}| **rif** *rif-string* | **group** *group*}

Syntax Description

netbios-name	Specifies the NetBIOS name. Wildcards are allowed.
ring *ring number*	Maps the NetBIOS name to a ring number or ring group number. Test frames for this name will be sent only to LAN ports in this ring group.
remote-peer	Maps the NetBIOS name to a specific remote peer.
interface serial *number*	Specifies the remote peer by direct interface.
ip-address *ip-address*	Specifies the remote peer by IP address.
rif *rif- string*	Maps the MAC address to a local interface using a Routing Information Field (RIF) string. The RIF string describes a source-routed path from the router to the MAC address, starting at the router's ring-group and ending on the ring where the MAC address is located. The direction is from the router toward the MAC address. See the IEEE 802.5 standard for details.
group *group*	Maps the NetBIOS name to a specified peer group. Valid numbers are in the range from 1 to 255.

Defaults

No static NetBIOS name is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Because the configuration of this command prevents the data-link switching plus (DLSw+) peer from exploring, an incorrect configuration could prevent DLSw+ from being able to find a resource actually available elsewhere in the network.

Examples

```
dlsw netbios-name netbios-1 remote-peer ip-address 10.132.248.5
```

Related Commands

Command	Description
show dlsw reachability	Displays DLSw+ reachability information.

dlsw peer-log-changes

To enable the logging of Syslog messages related to DLSw peer state changes, use the **dlsw peer-log-changes** global configuration command. To disable the logging of Syslog messages related to DLSw peer state changes, use the **no** form of this command.

dlsw peer-log-changes [**extend**]

no dlsw peer-log-changes

Syntax Description

extend	(Optional) Enables more verbose logging of messages, beyond the basic connection and disconnection messages.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **dlsw peer-log-changes** command is enabled, Syslog messages are generated for the following events:

- Connection attempt to a DLSw peer.
- Successful connection to a DLSw peer.
- Disconnection from a DLSw peer

When the **extended** keyword is enabled, Syslog messages are also generated for the following events:

- DLSw peer keepalive failure.
- DLSw TCP peer receives a TCP FINI.
- The configuration contains a promiscuous mismatch.
- Error when opening a priority peer.
- Explanation of why a backup peer was closed (such as linger timer expired or last circuit gone).

Examples

The following example enables verbose logging of Syslog messages related to DLSw peer state changes:

```
Router(config)# dlsw peer-log-changes extended
```

dlsw peer-on-demand-defaults

To configure defaults for peer-on-demand transport, use the **dlsw peer-on-demand-defaults** command in global configuration mode. To disable the previous assignment, use the **no** form of this command.

dlsw peer-on-demand-defaults [**fst**] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *destination-mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**inactivity** *minutes*] [**keepalive** *seconds*] [**lf** size] [**lsap-output-list** *list*] [**port-list** *port-list-number*] [**priority**] [**rsvp** {**global** | *average-bit-rate maximum burst*}] [**tcp-queue-max**]

no dlsw peer-on-demand-defaults [**fst**] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *destination-mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**inactivity** *minutes*] [**keepalive** *seconds*] [**lf** size] [**lsap-output-list** *list*] [**port-list** *port-list-number*] [**priority**] [**rsvp** {**global** | *average-bit-rate maximum burst*}] [**tcp-queue-max**]

Syntax Description

fst	(Optional) Use Fast Sequenced Transport (FST) encapsulation for all peers-on-demand established by this router.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for peer-on-demand peers. The *bytes-list-name* value is the name of the previously defined NetBIOS bytes access list filter.
cost *cost*	(Optional) Specifies the cost to reach peer-on-demand peer. The valid range is from 1 to 5. The default cost is 3.
dest-mac *destination-mac-address*	(Optional) Specifies the exclusive destination MAC address for peer-on-demand peers.
dmac-output-list *access-list-number*	(Optional) Specifies the filter output destination MAC addresses.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for peer-on-demand peers. The *host-list-name* value is the name of the previously defined NetBIOS host access list filter.
inactivity *minutes*	(Optional) Configures the length of time after the peer's circuit count is 0 that the peer-on-demand is disconnected. The valid range is from 0 to 1440 seconds. The default is 600 seconds.
keepalive *seconds*	(Optional) Configures the peer-on-demand keepalive interval. The valid range is from 0 to 1200 seconds. The default is 30 seconds.
lf *size*	(Optional) Largest frame size for this remote peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
lsap-output-list *list*	(Optional) Configures local service access point (LSAP) output filtering for peer-on-demand peers. Valid numbers are in the range from 200 to 299.
port-list *port-list-number*	(Optional) Configures a port list for peer-on-demand peers. Valid numbers are in the range from 0 to 4095.

priority	(Optional) Configures prioritization for peer-on-demand peers. The default state is off.
rsvp global	(Optional) Sets the Resource Reservation Protocol (RSVP) parameters to the global values specified in the **dlsw rsvp** command.
rsvp *average-bit-rate*	(Optional) Average bit rate (kilobits per second) to reserve up to 75 percent of total bits on the interface. The valid range is from 0 to 4294967.
maximum-burst	(Optional) Maximum burst size (kilobytes of data in queue). The valid range is from 0 to 4294967.
tcp-queue-max	(Optional) Configures the maximum output TCP queue size for peer-on-demand peers.

Defaults

The default peer-on-demand transport is TCP. The default **cost** is 3.
The default **inactivity** is 600 seconds.
The default **keepalive** is 30 seconds.
The default **priority** state is off.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(3)T	The **rsvp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A peer-on-demand peer is a nonconfigured remote peer that was connected because of a Logical Link Control, type 2 (LLC2) session established through a border peer data-link switching plus (DLSw+) network.

Setting the *average-bit-rate* and *maximum burst* values to 0 disables the RSVP bandwidth reservation for the peer connections.

Examples

The following example configures FST for peer-on-demand transport:

```
dlsw peer-on-demand-defaults fst
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw port-list

To map traffic on a local interface (Token Ring or serial) to remote peers, use the **dlsw port-list** command in global configuration mode. To disable the previous map assignment, use the **no** form of this command.

dlsw port-list *list-number type number*

no dlsw port-list *list-number type number*

Syntax Description

list-number	Port list number. The valid range is from 1 to 255.
type	Interface type.
number	Interface number.

Defaults

No port list is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Traffic received from a remote peer is forwarded only to the ports specified in the port list. Traffic received from a local interface is forwarded to peers if the input port number appears in the port list applied to the remote peer definition. The definition of a port list is optional.

Examples

The following example configures a data-link switching (DLSw) peer port list for Token Ring interface 1:

```
dlsw port-list 3 token ring 1
```

Related Commands

Command	Description
dlsw bgroup-list	Maps traffic on the local Ethernet bridge group interface to remote peers.
dlsw ring-list	Configures a ring list, mapping traffic on a local interface to remote peers.

dlsw prom-peer-defaults

To configure defaults for promiscuous transport, use the **dlsw prom-peer-defaults** command in global configuration mode. To disable the previous assignment, use the **no** form of this command.

dlsw prom-peer-defaults [**fst**] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *destination-mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**lsap-output-list** *list*] [**rsvp** {**global** | **learn** | [*average-bit-rate maximum burst*]}] [**tcp-queue-max** *size*]

no dlsw prom-peer-defaults [**fst**] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *destination-mac-address*] [**dmac-output-list** ***access-list-number***] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**lsap-output-list** *list*] [**rsvp** {**global** | **learn** | [*average-bit-rate maximum burst*]}] [**tcp-queue-max** *size*]

Syntax Description

fst	(Optional) Use Fast Sequenced Transport (FST) encapsulation for all promiscuous peers established by this router.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for promiscuous peers. The *bytes-list-name* value is the name of the previously defined NetBIOS bytes access list filter.
cost *cost*	(Optional) Specifies the cost to reach promiscuous peers. The valid range is from 1 to 5. The default cost is 3.
dest-mac *destination-mac-address*	(Optional) Specifies the exclusive destination MAC address for promiscuous peers.
dmac-output-list *access-list-number*	(Optional) Specifies the filter output destination MAC addresses.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for promiscuous peers. The *host-list-name* value is the name of the previously defined NetBIOS host access list filter.
keepalive *seconds*	(Optional) Configures the promiscuous keepalive interval. The valid range is from 0 to 1200 seconds. The default is 30 seconds.
lf *size*	(Optional) Largest frame size for this promiscuous peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
lsap-output-list *list*	(Optional) Configures Link Service Access Point (LSAP) output filtering for promiscuous peers. Valid numbers are 200 to 299.
rsvp global	(Optional) Sets the Resource Reservation Protocol (RSVP) parameters to the global values.
rsvp learn	(Optional) Configures RSVP parameters (*average-bit-rate* and *maximum burst* rate) to be those of the remote peer to which the promiscuous peer is connecting.

average-bit-rate	(Optional) Configures RSVP parameters for this peer connection, which are different from the global values. Average bit rate (kilobits per second) to reserve up to 75 percent of the total bits on the interface. The valid range is from 0 to 4294967.
maximum-burst	(Optional) Maximum burst size (kilobytes of data in queue). The valid range is from 0 to 4294967.
tcp-queue-max *size*	(Optional) Configures the maximum output TCP queue size for promiscuous peers.

Defaults

The default promiscuous-peer transport is TCP.
The default cost is 3.
The default keepalive value is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(3)T	The **rsvp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines-

A prom peer is a peer not configured as a remote peer on this data-link switching plus (DLSw+) device, but that initiated a peer connection that was accepted because promiscuous peering was enabled.

Setting the *average-bit-rate* and *maximum burst* values to 0 disables the RSVP bandwidth reservation for non configured remote peers.

Examples

The following example configures cost for promiscuous peers:

```
dlsw prom-peer-defaults cost 4
```

Related Commands

Command	Description
show dlsw capabilities	Displays the configuration of a specific peer or all peers.

dlsw redundant-rings

To eliminate caching problems and explorer looping when multiple data-link switching plus (DLSw+) peers are connected to a single Token Ring LAN where the virtual ring numbers configured in those DLSw+ routers are different, use the **dlsw redundant-rings** command in global configuration mode. To disable the previous settings, use the **no** form of this command.

dlsw redundant-rings [*ring*]

no dlsw redundant-rings [*ring*]

Syntax Description

ring	(Optional) Virtual ring number. You can configure up to 10 redundant rings, separated by spaces.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures router remote-router-1 so that the redundant virtual ring 300 should drop any explorer that is sourced from ring number 300. Similarly, router remote-router-2 knows that 300 is a redundant ring and any explorer sourced from ring 300 should be dropped.

```
remote-router-1# dlsw redundant-rings 300
remote-router-2# dlsw redundant-rings 300
```

dlsw remote-peer frame-relay

To specify the remote peer with which the router will connect, use the **dlsw remote-peer frame-relay** command in global configuration mode. To disable the previous assignments, use the **no** form of this command.

dlsw remote-peer *list-number* **frame-relay interface serial** *number dlci-number* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | **circuit-inactivity** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**] **pass-thru**

no dlsw remote-peer *list-number* **frame-relay interface serial** *number dlci-number* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | ***circuit-inactivity*** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**] **pass-thru**

Syntax Description

list-number	Ring list number. The valid range is from 1 to 255. The default is 0, which means data-link switching plus (DLSw+) forwards explorers over all ports or bridge groups on which DLSw+ is enabled.
interface serial *number*	Serial interface number of the remote peer with which the router is to communicate.
dlci-number	data-link connection identifier (DLCI) number of the remote peer.
backup-peer *ip-address*	(Optional) IP address of the existing TCP or Fast Sequenced Transport (FST) peer for which this peer is the backup peer.
backup-peer frame-relay interface serial *number dlci-number*	(Optional) Serial interface and DLCI number of the existing DirectLogical Link Control, type 2 (LLC2) Frame Relay peer for which this peer is the backup peer.
backup-peer interface *name*	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
backup-peer circuit-inactivity *minutes*	(Optional) Configures the length of time a circuit is inactive before terminating the circuit. May be used with the linger option. The valid range is from 1 to 1440 minutes.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The *bytes-list-name* argument is the name of the previously defined NetBIOS bytes access list filter.
circuit-weight *weight*	(Optional) Configures circuit weight for this remote peer.
cost *cost*	(Optional) Cost to reach this remote peer. The valid range is from 1 to 5. This cost takes precedence over the cost learned as part of the capabilities exchange with the remote peer. The **cost** keyword is relevant only in fault-tolerance mode.

dest-mac *mac-address*	(Optional) Permits the connection to be established only when an explorer frame is destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
dmac-output-list *access-list-number*	(Optional) Permits the connection to be established only when the explorer frame passes the specified access list. The *access-list-number* is the list number specified in the **access-list** command.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is from 0 to 1200 seconds.
lf *size*	(Optional) Largest frame size, in bytes, this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger *minutes*	(Optional) Configures the length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is from 1 to 300 minutes. The default is 5 minutes.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range from 200 to 299.
passive	(Optional) Designates this remote peer as passive.
pass-thru	(Optional) Selects pass-through mode. The default is local acknowledgment mode.

Defaults

No remote peers are specified.
The **linger** default is 5 minutes.
The **pass-thru** default is local acknowledgment mode.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.2	The following keywords and arguments were added: • **cost** *cost* • **dest-mac** *mac-address* • **dmac-output-list** *access-list-number* • **linger** *minutes* • **pass-thru**
12.0(3)T	The **circuit-weight** keyword was added.
12.2	The **backup peer circuit-inactivity** keyword and *minutes* argument were added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you need to permit access to only a single MAC address, the **dest-mac** option is a shortcut over the **dmac-output-list** option.

When the **pass-thru** keyword is not specified, traffic will be locally acknowledged and reliably transported in Logical Link Control, type 2 (LLC2) across the WAN.

The following keywords and arguments first appeared in Cisco IOS Release 12.2:

The backup-peer circuit-inactivity is only configurable in tandem with the backup-peer command for TCP or LLC2 peers.

Examples

The following example specifies a DLSw+ Lite peer as a backup to a primary direct peer:

```
dlsw remote-peer 0 frame-relay interface serial 1 40 pass-thru
dlsw remote-peer 0 frame-relay interface serial 0 30 backup-peer frame-relay interface 
serial 1 40
```

The following example specifies Frame Relay encapsulation connection for remote peer transport:

```
dlsw remote-peer 0 frame-relay interface serial 0 30
```

The following example specifies Remote Peer Backup Peer circuit-inactivity linger before termination:

```
dlsw local-peer peer-id 10.1.1.3
dlsw remote-peer 0 frame-relay 10.1.1.1
dlsw remote-peer 0 frame-relay 10.1.1.2 backup-peer 10.1.1.1 linger 20 
circuit-inactivity 3
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw remote-peer fst

To specify a Fast Sequenced Transport (FST) encapsulation connection for remote peer transport, use the **dlsw remote-peer fst** command in global configuration mode. To disable the previous FST assignments, use the **no** form of this command.

dlsw remote-peer *list-number* **fst** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**]

no dlsw remote-peer *list-number* **fst** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**]

Syntax Description

list-number	Ring list number. The valid range is from 1 to 255. The default is 0, which means DLSw+ forwards explorers over all ports or bridge groups on which data-link switching plus (DLSw+) is enabled.
ip-address	IP address of the remote peer with which the router is to communicate.
backup-peer *ip-address*	(Optional) IP address of the existing TCP or FST peer for which this peer is the backup peer.
backup-peer frame-relay-interface serial *number dlci-number*	(Optional) Serial interface and data-link connection identifier (DLCI) number of the existing direct or LLC2 Frame Relay peer for which this peer is the backup peer.
backup-peer interface *name*	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The *bytes-list-name* argument is the name of the previously defined NetBIOS bytes access list filter.
circuit-weight *weight*	(Optional) Configures circuit weight for this remote peer.
cost *cost*	(Optional) Cost to reach this remote peer. The valid range is from 1 to 5. This cost takes precedence over the cost learned as part of the capabilities exchange with the remote peer. The **cost** keyword is relevant only in fault-tolerance mode.
dest-mac *mac-address*	(Optional) Permits the connection to be established only when an explorer frame is destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
dmac-output-list *access-list-number*	(Optional) Permits the connection to be established only when the explorer frame passes the specified access list. The *access-list-number* is the list number specified in the **access-list** command.

host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is from 0 to 1200 seconds.
lf *size*	(Optional) Largest frame size this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger *minutes*	(Optional) Configures the length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is from 1 to 300 minutes. The default is 5 minutes.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range from 200 to 299.
passive	(Optional) Designates this remote peer as passive.

Defaults

No FST encapsulation connection is specified.

The **linger** default is 5 minutes.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2	The following keywords and arguments were added: • **dest-mac** *mac-address* • **dmac-output-list** *access-list-number* • **linger** *minutes*
12.0(3)T	The **circuit-weight** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you need to permit access to a single MAC address, the **dest-mac** option is a shortcut over the **dmac-output-list** option.

Examples

The following example specifies an FST peer as backup to a primary TCP peer:

```
dlsw remote-peer 0 tcp 10.2.18.1
dlsw remote-peer 1 fst 10.2.17.8 backup-peer 10.2.18.1
```

The following example specifies an FST encapsulation connection for remote peer transport:

```
dlsw remote-peer 1 fst 10.2.17.8
```

The following example specifies Remote Peer Backup Peer circuit inactivity and lingering before termination:

```
dlsw local-peer peer-id 10.1.1.3
dlsw remote-peer 0 tcp 10.1.1.1
dlsw remote-peer 0 tcp 10.1.1.2 backup-peer 10.1.1.1 linger 20
circuit-inactivity 3
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw remote-peer interface

To specify a point-to-point direct encapsulation connection, use the **dlsw remote-peer interface** command in global configuration mode. To disable previous interface assignments, use the **no** form of this command.

dlsw remote-peer *list-number* **interface serial** *number* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | **circuit-inactivity** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**] [**pass-thru**]

no dlsw remote-peer *list-number* **interface serial** *number* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | ***circuit-inactivity*** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**] [**pass-thru**]

Syntax Description

list-number	Ring list number. The valid range is from 1 to 255. The default is 0, which means all.
serial *number*	Specifies the remote peer by direct serial interface.
backup-peer *ip-address*	(Optional) IP address of the existing TCP or FST peer for which this peer is the backup peer.
backup-peer frame-relay interface serial *number dlci-number*	(Optional) Serial interface and data-link connection identifier (DLCI) number of the existing direct or Logical Link Control, type 2 (LLC2) Frame Relay peer for which this peer is the backup peer.
backup-peer interface *name*	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
backup-peer circuit-inactivity *minutes*	(Optional) Configures the length of time a circuit is inactive before being terminated. May be used with the linger option. The valid range is from 1 to 1440 minutes.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The *bytes-list-name* argument is the name of the previously defined NetBIOS bytes access list filter.
circuit-weight *weight*	(Optional) Configures circuit weight for this remote peer.
cost *cost*	(Optional) Cost to reach this remote peer. The valid range is from 1 to 5.
dest-mac *mac-address*	(Optional) Permits the connection to be established only when an explorer frame is destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
dmac-output-list *access-list-number*	(Optional) Permits the connection to be established only when the explorer frame passes the specified access list. The *access-list-number* is the list number specified in the **access-list** command.

host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is from 0 to 1200 seconds.
lf *size*	(Optional) Largest frame size, in bytes, this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger *minutes*	(Optional) Configures the length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is from 1 to 300 minutes. The default is 5 minutes.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range from 200 to 299.
passive	(Optional) Designates this remote peer as passive.
pass-thru	(Optional) Selects pass-through mode. The default is local acknowledgment mode.

Defaults

No point-to-point direct encapsulation connection is specified.
The **linger** default is 5 minutes.
The **pass-thru** default is local acknowledgment mode.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2	The following keywords and arguments were added: • **dest-mac** *mac-address* • **dmac-output-list** *access-list-number* • **linger** *minutes*
12.0(3)T	The **circuit-weight** keyword was added.
12.2	The **backup peer circuit-inactivity** keyword *minutes* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **cost** keyword specified in a remote peer statement takes precedence over the cost learned as part of the capabilities exchange with the remote peer. The **cost** keyword is relevant only in fault-tolerance mode.

When you need to permit access to a single MAC address only, the **dest-mac** option is a shortcut over the **dmac-output-list** option.

Examples

The following example specifies a point-to-point direct peer backup to a primary direct peer:

```
dlsw remote-peer 0 interface serial 1 pass-thru
dlsw remote-peer 1 interface serial 2 backup-peer interface serial 1 pass-thru
```

The following example specifies a point-to-point direct encapsulation connection for remote peer transport:

```
dlsw remote-peer 1 interface serial 2 pass-thru
```

The following example specifies Remote Peer Backup Peer circuit inactivity and lingering before termination:

```
dlsw local-peer peer-id 10.1.1.3
dlsw remote-peer 0 tcp 10.1.1.1
dlsw remote-peer 0 tcp 10.1.1.2 backup-peer 10.1.1.1 linger 20
circuit-inactivity 3
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw remote-peer tcp

To identify the IP address of a peer with which to exchange traffic using TCP, use the **dlsw remote-peer tcp** command in global configuration mode. To remove a remote peer, use the **no** form of this command.

dlsw remote-peer *list-number* **tcp** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | **circuit-inactivity** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**cluster** *cluster-id*] [**circuit-weight** *value*] [**cost** *cost*] [**dest-mac** *mac-address*] **dmac-output-list** *access-list-number*] [**dynamic**] [**host-netbios-out** *host-list-name*] [**inactivity** *minutes*] [**dynamic**] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**no-llc** *minutes*] [**passive**] [**priority**] [**rif-passthru** *virtual-ring-number*] [**rsvp** {**global** | *average-bit-rate maximum burst*}] [**tcp-queue-max** *size*] [**timeout** *seconds*]

no dlsw remote-peer *list-number* **tcp** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | **circuit-inactivity** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**cluster** *cluster-id*] [**circuit-weight** *value*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**dynamic**] [**host-netbios-out** *host-list-name*] [**inactivity** *minutes*] [**dynamic**] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] **lsap-output-list** *list*] [**no-llc** *minutes*] [**passive**] [**priority**] [**rif-passthru** *virtual-ring-number*] [**rsvp** {**global** | *average-bit-rate maximum burst*}] [**tcp-queue-max** *size*] [**timeout** *seconds*]

Syntax Description

list-number	Remote peer ring group list number. This ring group list number default is 0. Otherwise, this value must match the number you specify with the **dlsw ring-list**, **dlsw port-list**, or **dlsw bgroup-list** command.
ip-address	IP address of the remote peer with which the router is to communicate.
backup-peer *ip-address*	(Optional) IP address of the existing TCP or FST peer for which this peer is the backup peer.
backup-peer frame-relay interface serial *number dlci-number*	(Optional) Serial interface and data-link connection identifier (DLCI) number of the existing direct or Logical Link Control, type 2 (LLC2) Frame Relay peer for which this peer is the backup peer.
backup-peer interface *name*	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
backup-peer circuit-inactivity *minutes*	(Optional) Configures the length of time a circuit is inactive before terminating the circuit. The valid range is from 1 to 1440.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The *bytes-list-name* argument is the name of the previously defined NetBIOS bytes access list filter.
cluster *cluster-id*	(Optional) Used to indicate to a border peer that a particular remote peer should be treated as part of a specific peer cluster. The valid range is from 1 to 255.
circuit-weight *value*	(Optional) Configures the target state that data-link switching plus (DLSw+) tries to maintain. The valid range is from 1 to 100.
cost *cost*	(Optional) Cost to reach this remote peer. The valid range is from 1 to 5.

dest-mac *mac-address*	(Optional) Specifies the exclusive 48-bit destination MAC address, written as a dotted triple of four-digit hexadecimal numbers, for peer-on-demand peers. If the **dynamic** keyword is also specified, the TCP connection is established only when there is an explorer frame destined for the specified MAC address.
dmac-output-list *access-list-number*	(Optional) Specifies the filter output destination MAC addresses. The *access-list-number* is the list number specified in an **access-list** command. If the **dynamic** keyword is also specified, the TCP connection is established only when the explorer frame passes the specified access list.
dynamic	(Optional) Establishes the TCP connection only when there is DLSw+ data to send.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
inactivity *minutes*	(Optional) Configures the length of time a connection is inactive before closing the dynamic remote peer connection. The valid range is from 1 to 300 minutes. The default is 5 minutes.
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is from 0 to 1200 seconds.
lf *size*	(Optional) Largest frame size, in bytes, this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger *minutes*	(Optional) Configures the length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is from 0 to 1440 minutes.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range from 200 to 299.
no-llc *minutes*	(Optional) Configures the length of time a remote peer remains connected after all Logical Link Control, type 2 (LLC2) connections are gone. The valid range is from 1 to 300 minutes. The default is 5 minutes.
passive	(Optional) Designates this remote peer as passive.
priority	(Optional) Enables prioritization features for this remote peer. Valid TCP port numbers are the following: • High—2065 • Medium—1981 • Normal—1982 • Low—1983

rif-passthru *virtual-ring-number*	(Optional) Configures the remote peer as RIF-Passthru. The *virtual-ring-number* value is the same number as the *ring number* value assigned in the **source-bridge ring-group** commands of the DLSw+ Passthru peers.
rsvp global	(Optional) Configures the RSVP parameters for this specific peer back to the global values.
rsvp *average-bit-rate*	(Optional) Configures Resource Reservation Protocol (RSVP) parameters for this peer, which are different from the global values. Average bit rate (kilobits per second) reserves up to 75 percent of the total bits on the interface. range is from 0 to 4294967.
maximum burst	(Optional) Maximum burst size (kilobytes of data in queue). range is from 0 to 4294967.
tcp-queue-max *size*	(Optional) Maximum output TCP queue size for this remote peer. The valid maximum TCP queue size is a number in the range from 10 to 2000.
timeout *seconds*	(Optional) Resend time limit for TCP. The valid range is from 5 to 1200 seconds. The default is 90 seconds.

Defaults

No peer IP address is identified.

The **dynamic** option is not on by default. If the dynamic option is added without either the **inactivity** or **no-llc** argument specified, the default is to terminate the TCP connection to the remote peer after 5 minutes of no active LLC2 connection.

The **inactivity** default is 5 minutes.

The **no-llc** default is 5 minutes.

The **timeout** default is 90 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.1	The following keywords and arguments were added: • **dynamic** • **inactivity** *minutes* • **linger** *minutes* • **no-llc** *minutes* • **timeout** *seconds*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
11.2	The following keywords and arguments were added: • **dest-mac** *mac-address* • **dmac-output-list** *access-list-number* • **linger** *minutes*
12.0(3)T	The following keywords and arguments were added: • **circuit-weight** *value* • **rsvp** *maximum burst*
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Systems Network Architecture (SNA) dial-on-demand routing (DDR) technology allows switched links to be closed during idle periods. To enable this feature, set the **keepalive** keyword *seconds* argument to 0 and configure the **timeout** keyword *seconds* argument. When the **dynamic** keyword is configured, the **keepalive** keyword *seconds* argument is automatically set to 0.

To enhance DDR cost savings, you can configure the TCP connection to a remote peer to be dynamically established (that is, established only when there is DLSw data to send). You can further configure the TCP connection to terminate after a specified period of idle time on the peer or after a specified period of no active LLC sessions on the peer.

You cannot use both **no-llc** and **inactivity** in a command specifying a dynamic peer.

When you need to permit access to a single MAC address, the **dest-mac** keyword *mac-address* argument is a shortcut over the **dmac-output-list** keyword *access-list-number* argument.

Use the **linger** keyword *minutes* argument to specify that a backup peer will remain connected for a specified period of time after the primary connection is reestablished. Setting the **linger** keyword *minutes* argument to 0 causes sessions connected to the backup peer to drop immediately when the primary peer recovers. If the **linger** keyword is omitted, all sessions connected to the backup peer remain active until they terminate on their own.

When the **priority** keyword on the **dlsw remote-peer** command is configured, DLSw+ automatically activates four TCP ports to that remote peer (ports 2065, 1981, 1982 and 1983) and assigns traffic to specific ports. Furthermore, if Advanced Peer-to-Peer Networking (APPN) is running with DLSw+ and you specify the **priority** keyword option on the **dlsw remote-peer** command, then the SNA type of service (ToS) will map APPN class of service (COS) to TCP ToS and will preserve the APPN COS characteristics throughout the network.

The **rif passthru** keyword works only on Token Ring LANs via source-route bridging (SRB). Other LAN types, such as Synchronous Data Link Control (SDLC) and Qualified Logical Link Control (QLLC), are not supported. The RIF Passthru feature is supported with TCP encapsulation and it disables local acknowledgment.

The following features are not supported with the DLSw+ RIF Passthru feature:

- Border peers
- Peer-on-demand peers
- Dynamic peers
- Backup peers

The **cluster** keyword is available only on border peers. This option enables the DLSw+ Peer Clusters feature without forcing every DLSw+ router in the network to upgrade its software.

Setting the *average-bit-rate* or *maximum burst* value to 0 turns off RSVP for this peer.

Examples

The following example specifies a TCP encapsulation connection for remote peer transport:

```
dlsw remote-peer 0 tcp 10.2.17.8
```

The following example specifies a TCP peer as backup to a primary Fast Sequenced Transport (FST) peer:

```
dlsw remote-peer 0 fst 10.2.18.9
dlsw remote-peer 0 tcp 10.2.17.8 backup-peer 10.2.18.9
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw ring-list

To configure a ring list, mapping traffic on a local interface to remote peers, use the **dlsw ring-list** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dlsw ring-list *list-number* **rings** *ring-number*

no dlsw ring-list *list-number* **rings** *ring-number*

Syntax Description

list-number	Ring list number. The valid range is from 1 to 255.
rings	Specify one or more physical or virtual rings.
ring-number	Physical or virtual ring numbers. Multiple values are allowed. The valid range is from 1 to 4095.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Traffic received from a remote peer is forwarded only to the rings specified in the ring list. Traffic received from a local interface is forwarded to peers if the input ring number appears in the ring list applied to the remote peer definition. The definition of a ring list is optional.

Examples

The following example configures a data-link switching (DLSw) ring list, assigning rings 1, 2, and 3 to ring list 3:

```
dlsw ring-list 3 rings 1 2 3
```

Related Commands

Command	Description
dlsw port-list	Maps traffic on a local interface (Token Ring or serial) to remote peers.
dlsw remote-peer frame-relay	Specifies the remote peer with which the router will connect.
show dlsw capabilities	Displays the configuration of a specific peer or all peers.

dlsw rsvp

To enable the data-link switching plus (DLSw+) RSVP Bandwidth Reservation feature on the local peer, use the **dlsw rsvp** command in global configuration mode. To disable the DLSw+ RSVP Bandwidth Reservation feature for all peers in the router, use the **no** form of this command.

dlsw rsvp {**default** | *average-bit-rate maximum-burst*]}

no dlsw rsvp {**default** | *average-bit-rate maximum-burst*}

Syntax Description

default	Sets the average bit rate to 10 kbps and the maximum burst rate to 28 kbps.
average-bit-rate	Average bit rate (kilo*bits* per second) to reserve up to 75 percent of the total bits on the interface. The valid range is from 1 to 4294967 kbps.
maximum-burst	Maximum burst size (kilo*bytes* of data in queue). The valid range is from 1 to 4294967 kbps.

Defaults

The default values for the *average-bit-rate* and *maximum-burst* are 10 kbps and 28 kbps, respectively.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The DLSw+ RSVP Bandwidth Reservation feature does not require that all peers in a network have Resource Reservation Protocol (RSVP) configured. However, the feature does require that the end peer devices are configured with RSVP and that all devices in the middle are IP RSVP-capable.

The **default** keyword assumes that the DLSw+ peer is connected via a 56-kbps link. If this is not the case, then the default values will likely not produce optimal results. Even if the line speed is 56 kbps, the default values (10 kbps *average-bit-rate* and 28 kBps *maximum-burst*) may not be optimal in a particular network environment and should be changed accordingly.

Setting the *average-bit-rate* or *maximum-burst* value to 0 turns off RSVP for this peer.

Examples

The following example configures the DLSw+ RSVP Bandwidth Reservation feature with an *average bit rate* of 10 kbps and a *maximum-burst* value of 28 kbps:

```
dlsw rsvp default
```

Related Commands

Command	Description
dlsw peer-on-demand-defaults	Configures defaults for peer-on-demand transport.
dlsw prom-peer-defaults	Configures defaults for promiscuous transport
dlsw remote-peer tcp	Identifies the IP address of a peer with which to exchange traffic using TCP.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.
show ip rsvp request	Displays RSVP-related request information being requested upstream.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.

dlsw timer

To tune an existing configuration parameter, use the **dlsw timer** command in global configuration mode. To restore the default parameters, use the **no** form of this command.

dlsw timer {**icannotreach-block-time** | **netbios-cache-timeout** | **netbios-explorer-timeout** | **netbios-group-cache** | **netbios-retry-interval** | **netbios-verify-interval** | **sna-cache-timeout** | **explorer-delay-time** | **sna-explorer-timeout** | **explorer-wait-time** | **sna-group-cache** | **sna-retry-interval** | **sna-verify-interval**} *time*

no dlsw timer {**icannotreach-block-time** | **netbios-cache-timeout** | **netbios-explorer-timeout** | **netbios-group-cache** | **netbios-retry-interval** | **netbios-verify-interval** | **sna-cache-timeout** | **explorer-delay-time** | **sna-explorer-timeout** | **explorer-wait-time** | **sna-group-cache** | **sna-retry-interval** | **sna-verify-interval**} *time*

Syntax Description

icannotreach-block-time	Cache life of unreachable resource; during this time searches for the resource are blocked. The valid range is from 1 to 86400 seconds. The default is 0 (disabled).
netbios-cache-timeout	Cache life of NetBIOS name location for the local and remote reachability caches. The valid range is from 1 to 86400 seconds. The default is 960 seconds (16 minutes).
netbios-explorer-timeout	Length of time that the Cisco IOS software waits for an explorer response before marking a resource unreachable (on both a LAN and a WAN). The valid range is from 1 to 86400 seconds. The default is 6 seconds.
netbios-group-cache	Cache life of NetBIOS entries in the group cache. The valid range is from 1 to 86000 seconds. The default is 240 seconds (4 minutes).
netbios-retry-interval	NetBIOS explorer retry interval (on a LAN only). The valid range is from 1 to 86400 seconds. The default is 1 second.
netbios-verify-interval	Number of seconds between a cache entry's creation and its marking as stale. If a search request comes in for a stale cache entry, a directed verify query is sent to ensure that the cache still exists. The valid range is from 1 to 86400 seconds. The default is 240 seconds (4 minutes).
sna-cache-timeout	Length of time that anSystems Network Architecture (SNA) MAC or service access point (SAP) location cache entry exists before it is discarded (for local and remote caches). The valid range is from 1 to 86400 seconds. The default is 960 seconds (16 minutes).
explorer-delay-time	Time to wait before sending or accepting explorers. The valid range is from 1 to 5 minutes. The default is 0.
sna-explorer-timeout	Length of time that the Cisco IOS software waits for an explorer response before marking a resource unreachable (on a LAN and WAN). The valid range is from 1 to 86400 seconds. The default is 180 seconds (3 minutes).
explorer-wait-time	Time to wait for all stations to respond to explorers. The valid range is from 1 to 86400 seconds. The default is 0.
sna-group-cache	Cache life of SNA entries in the group cache. The valid range is from 1 to 86000 seconds. The default is 240 seconds (4 minutes).

sna-retry-interval	Interval between SNA explorer retries (on a LAN). The valid range is from 1 to 86400 seconds. The default is 30 seconds.
sna-verify-interval	Number of seconds between a cache entry's creation and its marking as stale. If a search request comes in for a stale cache entry, a directed verify query is sent to ensure that the cache still exists. The valid range is from 1 to 86400 seconds. The default is 240 seconds (4 minutes).
time	Length of time for selected timer, in seconds.

Defaults

The **icannotreach-block-time** default is 0 (disabled).

The **netbios-cache-timeout** default is 960 seconds (16 minutes).

The **netbios-explorer-timeout** default is 6 seconds.

The **netbios-group-cache** default is 240 seconds (4 minutes).

The **netbios-retry-interval** default is 1 second.

The **netbios-verify-interval** default is 240 seconds (4 minutes).

The **sna-cache-timeout** default is 960 seconds (16 minutes).

The **explorer-delay-time** default is 0.

The **sna-explorer-timeout** default is 180 seconds (3 minutes).

The **explorer-wait-time** default is 0.

The **sna-group-cache** default is 240 seconds (4 minutes).

The **sna-retry-interval** default is 30 seconds.

The **sna-verify-interval** default is 240 seconds (4 minutes).

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **netbios-group-cache** and **sna-group-cache** options were added to this command for the border peer caching feature.

Examples

The following configuration defines the length of time that an entry will stay in the group cache as 120 seconds (2 minutes):

```
dlsw timers sna-group-cache 120
```

The following example configures the length of time that an SNA MAC location cache entry exists before it is discarded:

```
dlsw timer sna-cache-timeout 3
```

dlsw timer connect-timeout

To modify the maximum allowed interval between first exchange identification (XID) and set asynchronous balanced mode extended unnumbered acknowledgment (SABME/UA) frames for circuits, use the **dlsw timer connect-timeout** command in global configuration mode. To disable the modification of XID and SABME/UA frames for circuits, use the **no** form of this command.

dlsw timer connect-timeout *time*

no dlsw timer connect-timeout *time*

Syntax Description

time	The time interval between XID and SABME/UA frames for circuits, in seconds. The complete XID negotiation has to be finished within this time interval. The range is 1 to 86400. The default is 60 seconds.

Command Default

Modification of XID and SABME/UA frames for circuits is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3T	This command was introduced.

Usage Guidelines

Use the **dlsw timer connect-timeout** command to override the value of the timer value default.

Examples

The following example sets the interval to 30 seconds for the modification of XID and SABME/UA frames for circuits:

```
Router(config)# dlsw timer connect-timeout 30
```

Related Commands

Command	Description
dlsw timer	Tunes an existing configuration parameter.
dlsw timer local-connect-timeout	Modifies the maximum allowed interval between local-switched circuits.

dlsw timer local-connect-timeout

To modify the maximum allowed interval between local-switched circuits, use the **dlsw timer local-connect-timeout** command in global configuration mode. To disable the modification of time intervals between local-switched circuits, use the **no** form of this command.

dlsw timer local-connect-timeout *time*

no dlsw timer local-connect-timeout *time*

Syntax Description

time	The time interval between local-switched circuits, in seconds. The range is 1 to 86400. The default is 30 seconds.

Command Default

Modification of the maximum allowed interval between local-switched circuits is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3T	This command was introduced.

Usage Guidelines

Use the **dlsw timer local-connect-timeout** command for the following reasons:

- This command overrides the value of the timer value default.
- This command enables you to link between local-switched circuits, such as Synchronous Data Link Control (SDLC) protocol to Logical Link Control, type 2 (LLC2) protocol and Qualified Logical Link Control (QLLC) protocol LLC2 protocol.

Examples

The following example sets the interval between local-switched circuits to 60 seconds:

```
Router(config)# dlsw timer local-connect-timeout 60
```

Related Commands

Command	Description
dlsw timer	Tunes an existing configuration parameter.
dlsw timer connect-timeout	Modifies the maximum allowed interval between XID and SABME/UA frames for circuits.

dlsw tos disable

To disable any type of service (ToS) bits in data-link switching plus (DLSw+)-generated packets, use the **dlsw tos disable** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw tos disable

no dlsw tos disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example disables the ToS bits in DLSw+-generated packets:

```
dlsw tos disable
```

dlsw tos map

To associate a type of service (ToS) value for priority peers, use the **dlsw tos map** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw tos map [**high** *value* [**medium** *value* | **normal** *value* | **low** *value*]]

no dlsw tos map [**high** *value* [**medium** *value* | **normal** *value* | **low** *value*]]

Syntax Description

high *value*	(Optional) Overrides the default values set for the port labeled "high." The value is the ToS bit value. Valid range is from 0 to 7.
medium *value*	(Optional) Overrides the default values set for the port labeled "medium." The value is the ToS bit value. Valid range is from 0 to 7.
normal *value*	(Optional) Overrides the default values set for the port labeled "normal." The value is the ToS bit value. Valid range is from 0 to 7.
low *value*	(Optional) Overrides the default values set for the port labeled "low." The value is the ToS bit value. Valid range is from 0 to 7.

Defaults

The default settings, with priority peers configured, are defined in Table 11.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, data-link switching plus (DLSw+) peer traffic is set to Critical-ECP. When the **priority** keyword is specified in the **dlsw remote peer tcp** command, DLSw+ automatically activates four TCP ports to that remote peer (ports 2065, 1981, 1982 and 1983) and associates a priority level. This command enables the user to customize the prioritization of DLSw+ traffic within the network. If priority peers are not configured, high is the only option. See Table 11 for corresponding priority levels and options.

Table 11 Priority Levels and Options

ToS Bit Value	DLSw+ Translation Value	ToS Bit Value Meaning	TCP Port Numbers
0[1]	Routine	—	—
1[1]	Priority	—	—
2	Immediate	Low	1983
3	Flash	Normal	1982
4	Flash Override	Medium	1981
5	Critical ECP	High	2065
6[2]	Internetwork Control	—	—
7[2]	Network Control	—	—

[1] Using ToS bit values 0 and 1 does not cause negative impact to the network, but these values do not prioritize the traffic.

[2] ToS bit values 6 and 7 are not recommended because of potential interference with critical network infrastructure flows.

Examples

The following example changes the default setting on IP packets generated by DLSw+ from high to low:

```
dlsw tos map low 2
```

The following is an example policy routing configuration that shows how to modify the default setting of TCP port 2065. The configuration changes the default setting on IP packets from network control priority to routine priority.

```
ip local policy route-map test
access-list 101 permit tcp any eq 2065 any
access-list 101 permit tcp any any eq 2065
route-map test permit 20
 match ip address 101
set ip precedence routine
```

dlsw transparent map

To enable MAC address mapping in a switch-based environment, use the **dlsw transparent map** command in interface configuration mode. To disable MAC address mapping, use the **no** form of this command.

dlsw transparent map local mac *mac-address* **remote mac** *mac-address* [**neighbor** *mac-address*]

no dlsw transparent map local mac *mac-address* **remote mac** *mac-address* [**neighbor** *mac-address*]

Syntax Description

local mac *mac-address*	MAC address that is created and given to the remote device. This MAC address is mapped to the actual MAC address that is specified in the **remote mac** *mac-address* option.
remote mac *mac-address*	MAC address of the remote device.
neighbor *mac-address*	(Optional) MAC address of the data-link switching plus (DLSw+) device that takes over mapping if the primary DLSw+ device becomes unavailable.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only the routers that are connected to the switch are configured for address mapping.

Examples

The following example maps MAC address 4000.1000.1234 to the actual device with the MAC address of 4000.3754.1000 and designates the DLSw+ device with MAC address 0000.0c12.0001 as backup:

```
dlsw transparent map local-mac 4000.1000.1234 remote mac 4000.3754.1000 neighbor
0000.0c12.0001
```

Related Commands

Command	Description
dlsw transparent switch-support	Enables the special support that is required for the interfaces connected to an Ethernet switch with the **dlsw transparent redundancy-enable** command configured.

dlsw transparent redundancy-enable

To configure transparent redundancy, use the **dlsw transparent redundancy-enable** command in interface configuration mode. To disable transparent redundancy, use the **no** form of this command.

dlsw transparent redundancy-enable *multicast-mac-address* [**master-priority** *value*]

no dlsw transparent redundancy-enable *multicast-mac-address* [**master-priority** *value*]

Syntax Description

multicast-mac-address	MAC address to which all data-link switching plus (DLSw+) devices on a transparent bridged domain advertise their presence by sending the master present frame.
master-priority *value*	(Optional) Configures the router as a master device. The valid range is from 0 to 254. The lower the value, higher the priority. The default value is 100.

Defaults

No default behavior or value

The **master-priority** default is 100.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The same *multicast-mac-address* value must be configured on all DLSw+ devices within the same transparent bridged domain. All the DLSw+ devices advertise their presence via frames to this *multicast-mac-address* value.

All routers in the transparent bridged domain compete and elect one master router. The master router is elected based on its **master-priority** value. In the case of equal master priority setting, the router with the lowest MAC address is the elected master router.

Examples

The following example configures Ethernet redundancy with a **master-priority** value of 100:

```
dlsw transparent redundancy-enable 9999.9999.9999 master-priority 100
```

Related Commands

Command	Description
show dlsw transparent cache	Displays the master circuit cache for each transparent bridged domain.
show dlsw transparent neighbor	Displays DLSw neighbors in a transparent bridged domain.

dlsw transparent switch-support

To enable the special support that is required for the interfaces connected to an Ethernet switch with the **dlsw transparent redundancy-enable** command configured, use the **dlsw transparent switch-support** command in global configuration mode. To disable data-link switching (DLSw) transparent switch support, use the **no** form of this command.

dlsw transparent switch-support

no dlsw transparent switch-support

Syntax Description

This command has no arguments or keywords.

Defaults

Switch support is off.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **dlsw transparent switch-support** command must be configured before the **dlsw transparent map** command.

Examples

The following example configures Ethernet switch support:

```
dlsw transparent switch-support
```

Related Commands

Command	Description
dlsw transparent map	Enables MAC address mapping in a switch-based environment.

dlsw transparent timers

To configure the timeout value the master router waits for all requests for a circuit before giving the permission for a router for a circuit, use the **dlsw transparent timers** command in interface configuration mode. To disable the timeout value, use the **no** form of this command.

dlsw transparent timers [**netbios** *value* | **sna** *value*]

no dlsw transparent timers [**netbios** *value* | **sna** *value*]

Syntax Description

netbios *value*	(Optional) Timeout value for the NetBIOS session. The valid range is from 100 to 900 milliseconds (ms). The default value is 400 ms.
sna *value*	(Optional) Timeout value for the Systems Network Architecture (SNA) session. The valid range is from 100 to 5000 ms. The default value is 1000 ms (1 second).

Defaults

The default NetBIOS value is 400 ms.
The default SNA value is 1000 ms (1 second).

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **dlsw transparent redundancy-enable** command must be configured before the **dlsw transparent timers** command.

Examples

The following example configures the master router to wait 500 ms for a NetBIOS session before giving or denying permission to a router to create a circuit:

```
dlsw transparent timers netbios 500
```

Related Commands

Command	Description
dlsw transparent redundancy-enable	Configures transparent redundancy.

dlsw udp-disable

To disable the User Datagram Protocol (UDP) unicast feature, use the **dlsw udp-disable** command in global configuration mode. To return to the default UDP unicast feature, use the **no** form of this command.

dlsw udp-disable

no dlsw udp-disable

Syntax Description

This command has no arguments or keywords.

Defaults

The UDP unicast feature is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **dlsw udp-disable** command is configured, then a data-link switching plus data-link switching plus (DLSw+) node will not send packets via UDP unicast and will not advertise UDP Unicast support in its capabilities exchange message.

Refer to the “Bridging and IBM Networking Overview” chapter of the *Bridging and IBM Networking Configuration Guide* for more information on the UDP Unicast feature.

Examples

The following example disables the UDP unicast feature:

```
dlsw udp-disable
```

dlur

To enable the Systems Network Architecture (SNA) session switch function on the Cisco Mainframe Channel Connection (CMCC) adapter and enter dependent logical unit requester (DLUR) configuration mode, use the **dlur** command in TN3270 server configuration mode. To disable the SNA session switch function and discard all parameter values associated with the SNA session switch, use the **no** form of this command.

dlur [*fq-cpname fq-dlusname*]

no dlur

Syntax Description

fq-cpname	(Optional) Fully qualified control point (CP) name used by the SNA session switch and the logical unit (LU) name for the DLUR function. This name must be unique among Advanced Peer-to-Peer Networking (APPN) nodes in the network including other values for the *fq-cpname* argument specified on all other TN3270 servers running under the Cisco IOS software.
fq-dlusname	(Optional) Fully qualified name of the primary choice for the dependent LU server (DLUS). This is the name of an LU, usually a CP, in an APPN host. The value for the *fq-dlusname* argument can be repeated and shared across servers.

Defaults

No DLUR function is enabled.

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. If the SNA session switch function is already enabled, the **dlur** command with no arguments puts you in DLUR configuration mode. The session switch function implements an End Node DLUR.

Several parameters in the DLUR configuration mode consist of fully qualified names, as defined by the APPN architecture. Fully qualified names consist of two case-insensitive alphanumeric strings, separated by a period. However, for compatibility with existing APPN products, including virtual telecommunications access method (VTAM), the characters “#” (pound), “@” (at), and “$” (dollar) are allowed in the fully qualified name strings. Each string is from one to 8 characters long; for example, RA12.NODM1PP. The portion of the name before the period is the network entity title (NET) ID and is shared between entities in the same logical network.

The **no dlur** command hierarchically deletes all resources defined beneath it.

Examples

The following example performs two functions: It enters DLUR configuration mode and it enables the DLUR function and defines the LU name for the DLUR as SYD.TN3020 and the primary choice for DLUS as SYD.VMG. Note that the NET ID portion of both names is the same:

```
dlur SYD.TN3020 SYD.VMG
```

Related Commands

Command	Description
lsap	Creates a SAP in the SNA session switch and enters DLUR SAP configuration mode.
preferred-nnserver	Specifies a preferred NN as server.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters DLUR PU configuration mode.

dlus-backup

To specify a backup Dependent Logical Unit Server (DLUS) for the Dependent Logical Unit Requestor (DLUR) function, use the **dlus-backup** command in DLUR configuration mode. To remove a backup DLUS name, use the **no** form of this command.

dlus-backup *dlusname*

no dlus-backup

Syntax Description

dlusname	Fully qualified name of the backup DLUS for the DLUR.

Defaults

No backup DLUS is specified.

Command Modes

DLUR configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. Only one backup DLUS can be specified per Cisco Mainframe Channel Connection (CMCC) adapter. If the backup DLUS specified in the **dlus-backup** command is in use when a **no dlus-backup** command is issued, the connection is not torn down.

Several parameters in DLUR configuration mode consist of fully qualified names, as defined by the Advanced Peer-to-Peer Networking (APPN) architecture. Fully qualified names consist of two case-insensitive alphanumeric strings, separated by a period. However, for compatibility with existing APPN products, including virtual telecommunications access method (VTAM), the characters “#” (pound), “@” (at), and “$” (dollar) are allowed in the fully qualified name strings. Each string is from one to eight characters long; for example, RA12.NODM1PP. The portion of the name before the period is the network entity title (NET) ID and is shared between entities in the same logical network.

Examples

The following example specifies SYD.VMX as the backup DLUS:

```
dlus-backup SYD.VMX
```

Related Commands

Command	Description
client pool	Nails clients to pools.

domain-id

To specify a domain name suffix that the TN3270 server appends to a configured machine name to form a fully qualified name when configuring inverse Domain Name System (DNS) nailing, use the **domain-id** command in TN3270 server configuration mode. To disable this specification, use the **no** form of this command.

domain-id *DNS-domain-identifier DNS-domain*

no domain-id *DNS-domain-identifier DNS-domain*

Syntax Description

DNS-domain-identifier	A numeric identifier that specifies the domain name. The valid value range is from 1 to 255. Each domain ID statement can have only one *DNS-domain-identifier* value. This identifier is also used in the **client pool** command.
DNS-domain	An alphanumeric string that specifies a domain name suffix, including all dots (.) but not delimited by dots. The string can contain no more than 80 characters. All dots must be included when the string is appended to a configured DNS name. If the DNS domain starts with a dot, then the dot must be included if it is not already at the end of the DNS name.

Defaults

No default behavior or values

Command Modes

TN3270 server configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The user can configure up to 255 domain names, one per statement. This command must be configured before you configure the **client pool** command with either the **domain-id** keyword or the **name** keyword and the optional *DNS-domain-identifier* argument.

Examples

In the following example, the **domain-id** command specifies 23 as the *DNS domain identifier* for the .cisco.com domain name. All clients nailed to the pool GENERAL will use .cisco.com as the domain name suffix. For example, the client name ally-isdn1 will become ally-isdn1.cisco.com.

```
tn3270-server
 domain-id 23 .cisco.com
  pool GENERAL  cluster layout 4s1p
  listen-point 172.18.5.168
   pu T240CA   91922363 token-adapter 31 12 rmac 4000.4000.0001
    allocate lu 1 pool GENERAL  clusters 1
 client name ally-isdn1 23 pool GENERAL
```

dspu activation-window

To define the number of activation request units (RUs) and response messages (such as activate logical unit (ACTLU)s or Dynamic Definition of Dependent LU (DDDLU) Network Management Vector Transport (NMVT)s that can be sent without waiting for responses from the remote physical unit (PU), use the **dspu activation-window** command in global configuration mode. To restore the default window size, use the **no** form of this command.

dspu activation-window *window-size*

no dspu activation-window

Syntax Description

window-size	Number of outstanding unacknowledged activation RUs. The default is five.

Defaults

The default window size is five outstanding unacknowledged activation RUs.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You do not typically need to define the number of activation RUs, but doing so can enhance activation performance in some situations. Increasing the downstream physical unit (DSPU) activation window allows more logical unit (LU)s to become active in a shorter amount of time (assuming the required buffers for activation RUs are available). Conversely, decreasing the DSPU activation window limits the amount of buffers the DSPU can use during PU or LU activation. This command provides pacing to avoid depleting the buffer pool during PU activation.

Examples

In the following example, the DSPU activation window is configured to 10. The DSPU can send up to 10 activation RUs without a response from the remote PU. However, the DSPU cannot send any additional activation RUs until a response is received. The DSPU can only have 10 activation RUs awaiting response at any given time.

```
dspu activation-window 10
```

dspu default-pu

To enable the default PU feature to be used when a downstream physical unit (PU) attempts to connect, but does not match any of the explicit PU definitions, use the **dspu default-pu** command in global configuration mode. To disable the default PU feature, use the **no** form of this command.

dspu default-pu [**window** *window-size*] [**maxiframe** *max-iframe*]

no dspu default-pu [**window** *window-size*] [**maxiframe** *max-iframe*]

Syntax Description

window *window-size*	(Optional) Send and receive window sizes used across the link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum size (in bytes) of an I-frame that can be sent or received across the link. The range is from 64 bytes to 18432 bytes. The default is 1472.

Defaults

The default window size is 7.

The default maximum I-frame size is 1472.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the downstream physical unit (DSPU) default PU is not defined, a connection attempt by a downstream PU that does not match any explicit PU definition is rejected.

The **dspu default-pu** command must be followed by at least one **dspu lu** command to define which pool the default LUs will be assigned from. Default LUs cannot be defined as dedicated LUs from a host.

The maximum I-frame size includes the Systems Network Architecture (SNA) transmission header (TH), request header (RH), and request unit (RU), but does not include the Data-link control (DLC) header. The DSPU feature segments frames being sent to fit within this frame size. If an exchange identification (XID) is received from a remote PU, which indicates that it supports a different maximum I-frame size, then the lower of the two values is used.

Examples

In the following example, the default PU feature is enabled with a window size of five and a maximum I-frame size of 128. Each default PU can have up to three LUs assigned from the hostpool pool of LUs.

```
dspu pool hostpool host ibm3745 lu 2 254
dspu default-pu window 5 maxiframe 128
dspu lu 2 4 pool hostpool
```

Related Commands

Command	Description
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.
dspu pool	Defines a range of host LUs in an LU pool.

dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay)

To enable a local service access point (SAP) on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts, use the **dspu enable-host** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

dspu enable-host [**lsap** *local-sap*]

no dspu enable-host [**lsap** *local-sap*]

Syntax Description

lsap	(Optional) Specifies that the local SAP will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts.
local-sap	(Optional) Local SAP address. The default is 12.

Defaults

The default local SAP address is 12.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the local SAP address 10 on Token Ring interface 0 is enabled for use by upstream host connections:

```
interface tokenring 0
 dspu enable-host lsap 10
```

Related Commands

Command	Description
dspu host (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.

dspu enable-host (QLLC)

To enable an X.121 subaddress for use by upstream host connections via Qualified Logical Link Control (QLLC), use the **dspu enable-host** command in interface configuration mode. To disable the X.121 subaddress, use the **no** form of this command.

dspu enable-host qllc *x121-subaddress*

no dspu enable-host qllc *x121-subaddress*

Syntax Description

qllc	Specifies that the interface will use QLLC.
x121-subaddress	X.121 subaddress.

Defaults

No default X.121 subaddress is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, X.121 subaddress 320108 is enabled for use by upstream host connections:

```
interface serial 0
 encapsulation x35
 x25 address 3202
 x25 map qllc 320112
 dspu enable-host qllc 320108
```

Related Commands

Command	Description
dspu host (QLLC)	Defines a DSPU host over an X.25/QLLC connection.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.

dspu enable-host (SDLC)

To enable an Synchronous Data Link Control (SDLC) address for use by upstream host connections, use the **dspu enable-host** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

dspu enable-host sdlc *sdlc-address*

no dspu enable-host sdlc *sdlc-address*

Syntax Description

sdlc	Specifies that the interface will use SDLC.
sdlc-address	SDLC address.

Defaults

No default SDLC address is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, SDLC address C1 is enabled for use by upstream host connections:

```
interface serial 0
 encapsulation sdlc
 sdlc role secondary
 sdlc address c1
 dspu enable-host sdlc c1
```

Related Commands

Command	Description
dspu host (SDLC)	Defines a DSPU host over an SDLC connection.
sdlc address	Assigns a set of secondary stations attached to the serial link.
sdlc role	Establishes the router to be either a primary or secondary SDLC station.

dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)

To enable an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstreamphysical unit (PU) connections, use the **dspu enable-pu** command in interface configuration mode. To disable the connection, use the **no** form of this command.

dspu enable-pu [**lsap** *local-sap*]

no dspu enable-pu [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Local service access point (SAP) address used by the downstream physical unit (DSPU) to establish connection with the remote host. The default local SAP address is 8.

Defaults

The default local SAP address is 8.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example demonstrates the configuration of a downstream PU via Token Ring and Ethernet:

```
interface tokenring 0
 ring-speed 16
 dspu enable-pu lsap 8

interface ethernet 0
 dspu enable-pu lsap 8
```

Related Commands

Command	Description
dspu pu (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), virtual data-link control (VDLC), or NCIA connections.

dspu enable-pu (QLLC)

To enable an X.121 subaddress for use by downstream physical unit (PU) connections via Qualified Logical Link Control (QLLC), use the **dspu enable-pu** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

dspu enable-pu qllc *x121-subaddress*

no dspu enable-pu qllc *x121-subaddress*

Syntax Description

qllc	Required keyword for Qualified Logical Link Control (QLLC) data-link control.
x121-subaddress	Variable-length X.121 address. It is assigned by the X.25 network service provider.

Defaults

No default address is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables an X.121 subaddress for use by downstream PU connections:

```
interface serial 0
 encapsulation x25
 x25 address 3201
 x25 map qllc 320208
 dspu enable-pu qllc 08
```

Related Commands

Command	Description
dspu pu (QLLC)	Defines a downstream PU over an X.25 connection explicitly.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.

dspu enable-pu (SDLC)

To enable an Synchronous Data Link Control (SDLC) address for use by downstream physical unit (PU) connections, use the **dspu enable-pu** command in interface configuration mode. To disable the connection, use the **no** form of this command.

dspu enable-pu sdlc *sdlc-address*

no dspu enable-pu sdlc *sdlc-address*

Syntax Description

sdlc	Required keyword for SDLC data-link control.
sdlc-address	SDLC address.

Defaults

No default address is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables a downstream physical unit (DSPU) downstream connection:

```
interface serial 0
 encapsulation x25
 sdlc role primary
 sdlc address c1
 dspu enable-pu sdlc c1
```

Related Commands

Command	Description
dspu pu (SDLC)	Defines a DSPU host over an SDLC connection.
sdlc address	Assigns a set of secondary stations attached to the serial link.
sdlc role	Establishes the router to be either a primary or secondary SDLC station.

dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)

To define a downstream physical unit (DSPU) host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections, use the **dspu host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu host *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no dspu host *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	The specified DSPU host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both Block and ID numbers. For example, if the XID value is 05D00001, the Block number is 05D and the ID number is 00001.
rmac *remote-mac*	MAC address of the remote host physical unit (PU).
rsap *remote-sap*	(Optional) SAP address of the remote host PU. The default is 4.
lsap *local-sap*	(Optional) Local SAP address used by the DSPU to establish connection with the remote host. The default is 12.
interface *slot/port]*	(Optional) Slot and port number of the interface. The slash mark is required.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Specifies that the host link will be used for the focal point support.

Defaults

The default remote SAP address is 4.
The default local SAP address is 12.
The default window size is 7.
The default maximum I-frame is 1472.
The default number of retries is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The local SAP address must be enabled by one of the following commands: **dspu enable-host**, **dspu rsrb enable-host**, or **dspu vdlc enable-host**.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the lower of the two values is used.

Alerts from downstream PUs will be forwarded to the focal point host. The **focalpoint** keyword must be included in no more than one **dspu host** command.

Examples

The following example shows the definition for a DSPU host with 252 logical unit (LU)s and a connection to be established across an RSRB link:

```
dspu rsrb 88 1 99 4000.ffff.0001
dspu rsrb enable-host lsap 10
dspu host ibm3745 xid 06500001 rmac 4000.3745.0001 lsap 10
dspu pool hostpool lu 2 253 host ibm3745
```

Related Commands

Command	Description
dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay)	Enables a local SAP on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts.
dspu pool	Defines a range of host LUs in an LU pool.
dspu rsrb enable-host	Enables an RSRB SAP for use by DSPU host connections.
dspu rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name through the RSRB.
dspu start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name.
dspu vdlc enable-host	Enables a SAP for use by DSPU host connections.

dspu host (Frame Relay)

To define a downstream physical unit (DSPU) host over a Frame Relay connection, use the **dspu host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu host *host-name* **xid-snd** *xid* **dlci** *dlci-number* [**rsap** *rsap-addr*] [**lsap** *lsap-addr*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no dspu host *host-name* **xid-snd** *xid* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	The specified DSPU host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
dlci *dlci-number*	Frame Relay data-link connection identifier (DLCI) number; a decimal number.
rsap *rsap-addr*	(Optional) Remote service access point (SAP) address.
lsap *lsap-addr*	(Optional) Local SAP address.
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with remote host physical unit (PU). The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Specifies that the host link will be used for the focal point support.

Defaults

The default remote SAP is 4.
The default local SAP is 12.
The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The local SAP address must be enabled by a **dspu enable-host** command.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the lower of the two values is used.

Alerts from downstream PUs will be forwarded to the focal point host. The **focalpoint** keyword must be included in no more than one **dspu host** command.

Examples

The following example defines a DSPU host for Frame Relay support:

```
dspu host rosebud xid-snd 06500001 dlci 200 rsap 4 lsap 12
```

Related Commands

Command	Description
dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay)	Enables a local SAP on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts.
dspu pool	Defines a range of host LUs in an LU pool.

dspu host (QLLC)

To define a downstream physical unit (DSPU) host over an X.25 or Qualified Logical Link Control (QLLC) connection, use the **dspu host** command in global configuration mode. To delete the DSPU host definition, use the **no** form of this command.

dspu host *host-name* **xid-snd** *xid* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**interface** *slot* | *port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no dspu host *host-name* **xid-snd** *xid* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	The specified DSPU host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the Block number is 05D and the ID number is 00001.
x25 *remote-x121-addr*	Remote X.121 address.
qllc *local-x121-subaddr*	(Optional) Local X.121 subaddress.
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with remote host physical unit (PU). The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Specifies that the host link will be used for the focal point support.

Defaults

The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The X.121 subaddress must be enabled by a **dspu enable-host** command.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the lower of the two values is used.

Alerts from downstream PUs will be forwarded to the focal point host. The **focalpoint** keyword must be included in no more than one **dspu host** command.

Examples

The following example defines a DSPU host:

```
dspu host hosta xid-snd 065ffff0 x25 00000123005 qllc 12
```

Related Commands

Command	Description
dspu enable-host (QLLC)	Enables an X.121 subaddress for use by upstream host connections through QLLC.
dspu pool	Defines a range of host LUs in an LU pool.
dspu start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name.

dspu host (SDLC)

To define a downstream physical unit (DSPU) host over an Synchronous Data Link Control (SDLC) connection, use the **dspu host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu host *host-name* **xid-snd** *xid* **sdlc** *sdlc-addr* [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no dspu host *host-name* **xid-snd** *xid* **sdlc** *sdlc-addr* [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	The specified DSPU host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both Block and ID numbers. For example, if the XID value is 05D00001, the Block number is 05D and the ID number is 00001.
sdlc *sdlc-addr*	SDLC hexadecimal address.
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default window size is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with remote host physical unit (PU). The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Specifies that the host link will be used for the focal point support.

Defaults

The default window size is 7.
The default maximum I-frame is 1472.
The default number of retries is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The SDLC address must be enabled by a **dspu enable-host** command.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the lower of the two values is used.

Alerts from downstream PUs will be forwarded to the focal point host. The **focalpoint** keyword must be included in no more than one **dspu host** command.

Examples

The following example defines a DSPU host for SDLC:

```
dspu host hosta xid-snd 065ffff0 sdlc c1
```

Related Commands

Command	Description
dspu enable-host (SDLC)	Enables an SDLC address for use by upstream host connections.
dspu pool	Defines a range of host LUs in an LU pool.

dspu lu

To define a dedicated logical unit (LU) or a range of LUs for an upstream host and a downstream physical unit (PU), use the **dspu lu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu lu *lu-start* [*lu-end*] {**host** *host-name host-lu-start* | **pool** *pool-name*} [**pu** *pu-name*]

no dspu lu *lu-start* [*lu-end*] {**host** *host-name host-lu-start* | **pool** *pool-name*} [**pu** *pu-name*]

Syntax Description

lu-start	Starting LU address in the range of LUs to be assigned from a pool or dedicated to a host.
lu-end	(Optional) Ending LU address in the range of LUs to be assigned from a pool or dedicated to a host.
host *host-name host-lu-start*	Specifies that each LU in the range of LUs will be dedicated to a host LU *host-name* value. The range of host LUs starts with the *host-lu-start* address.
pool *pool-name*	Specifies that each LU in the range of LUs will be assigned from the specified pool.
pu *pu-name*	(Optional) Downstream PU for which this range of LUs is being defined.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **dspu lu** command immediately follows a **dspu default-pu** or **dspu pu** command, then the **dspu lu** command is applied to that PU**, and the pu** *pu-name* option is not necessary for the **dspu lu** command.

If the keyword and argument are included, the LU defined by the **dspu lu** command will be applied to the named PU.

The **pool** and **host** keywords are mutually exclusive. You can define a range of LUs to be either assigned from a pool or dedicated to a host.

Examples

The following example defines downstream LUs as dedicated LUs. The downstream PU, ciscopu, has three downstream LUs with addresses 2 and 4. When ciscopu establishes a connection with the downstream physical unit (DSPU), the three downstream LUs (2, 3, and 4) are dedicated to LUs 22, 23, and 24, respectively, from the IBM 3745 host.

```
dspu host ibm3745 xid-snd 065000001 rmac 4000.3745.0001
dspu pu ciscopu xid-rcv 05D00001 rmac 1000.5AED.1F53
dspu lu 2 4 host ibm3745 22
```

Related Commands

Command	Description
dspu default-pu	Enables the default PU feature to be used when a downstream PU attempts to connect, but does not match any of the explicit PU definitions.
dspu host (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu host (QLLC)	Defines a DSPU host over an X.25/QLLC connection.
dspu host (SDLC)	Defines a DSPU host over an SDLC connection.
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
dspu pool	Defines a range of host LUs in an LU pool.
dspu pu (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu pu (QLLC)	Defines a downstream PU over an X.25 connection explicitly.
dspu pu (SDLC)	Defines a DSPU host over an SDLC connection.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.

dspu ncia

To configure the native client interface architecture (NCIA) server as the underlying transport, use the **dspu ncia** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu ncia [*server-number*]

no dspu ncia [*server-number*]

Syntax Description

server-number	(Optional) Server number configured in the **ncia server** command. Currently, only one NCIA server is supported.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must use the **ncia server** command to configure an NCIA server on the router before using the **dspu ncia** command to configure the NCIA server as the underlying transport.

Examples

The following example configures the NCIA server as the underlying transport mechanism communicating directly with the downstream physical unit (DSPU):

```
dspu ncia 1
```

Related Commands

Command	Description
dspu ncia enable-pu	Enables a SAP on the NCIA server for use by downstream connections.
ncia server	Configures an NCIA server on a Cisco router.

dspu ncia enable-pu

To enable a destination service access point (DSAP) on the native client interface architecture (NCIA) server for use by downstream connections, use the **dspu ncia enable-pu** command in global configuration mode. To disable the SAP, use the **no** form of this command.

dspu ncia enable-pu [**lsap** *local-sap*]

no dspu ncia enable-pu [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for receiving incoming connection attempts. The default is 8.

Defaults

The default local SAP is 8.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the local SAP address 8 is enabled for use by the downstream PU CISCOPU-A:

```
dspu ncia 1
dspu ncia enable-pu lsap 8
!
dspu host HOST-9370 xid-snd 11100001 rmac 4000.1060.1000 rsap 4 lsap 4
!
dspu pu CISCOPU-A xid-rcv 01700001
dspu lu 2 6 host HOST-9370 2
!
interface TokenRing 0
 ring-speed 16
 llc2 xid-retry-time 0
 dspu enable-host lsap 4
 dspu start HOST-9370
```

Related Commands

Command	Description
dspu ncia	Configures the NCIA server as the underlying transport.
dspu pu (**Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA**)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.

dspu notification-level

To specify the downstream physical unit (DSPU) notifications to send to Simple Network Management Protocol (SNMP) and Systems Network Architecture (SNA) network management, use the **dspu notification-level** command in global configuration mode. To specify the default notification level **low**, use the **no** form of this command.

dspu notification-level {**off** | **low** | **medium** | **high**}

no dspu notification-level

Syntax Description

off	Sends neither SNMP traps nor unsolicited SNA messages for the DSPU.
low	Sends physical unit (PU) and logical unit (LU) activation failures only.
medium	Sends PU state changes and PU and LU activation failures.
high	Sends both PU and LU state changes and activation failures.

Defaults

The default notification level is low.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to both SNMP traps and unsolicited SNA messages to the operator. The upstream PU and LU notification events and the LU state change notification events are not sent as unsolicited SNA messages to the operator. These events are sent as SNMP traps only.

Examples

The following example sets the notification level to enable the DSPU to send notifications to network management for both PU and LU state changes and activation failures:

```
dspu notification-level high
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of SNMP notifications.

dspu pool

To define a range of host logical unit (LU)s in an LU pool, use the **dspu pool** command in global configuration mode. To remove the definition, use the **no** form of this command.

dspu pool *pool-name* **host** *host-name* **lu** *lu-start* [*lu-end*] [**inactivity-timeout** *minutes*]

no dspu pool *pool-name* **host** *host-name* **lu** *lu-start* [*lu-end*] [**inactivity-timeout** *minutes*]

Syntax Description

pool-name	Name identifier of the pool.
host *host-name*	Name of the host that owns the range of host LUs in the pool.
lu *lu-start*	Starting LU address in the range of host LUs in the pool.
lu-end	(Optional) Ending address (inclusive) of the range of host LUs in the pool. If no ending address is specified, only one LU (identified by the *lu-start* argument) will be defined in the pool.
inactivity-timeout *minutes*	(Optional) Interval of inactivity (in minutes) on either the system services control points (SSCP)-LU or LU-LU sessions, which will cause the downstream LU to be disconnected from the upstream LU. The default is disabled.

Defaults

The inactivity-timeout is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can include multiple **dspu pool** commands that specify the same pool name. In this way, an LU pool can include several LU ranges from the one host physical unit (PU), or it can include LUs from different host PUs. The LUs from the host *host-name* value starting at the *lu-start* value and ending with the *lu-end* value, inclusive, will be included in the pool *pool-name*. For the LUs in this pool, if there is no traffic on either the SSCP-LU or LU-LU sessions for the inactivity timeout number of minutes, the downstream LU will be disconnected from the upstream LU, and the upstream LU will be allocated to any downstream LU waiting for a session. A value of zero for inactivity minutes means no timeouts. (The inactivity timeout applies to all LUs in this pool, not just the LUs defined by this **dspu pool** command. The last value configured will be used.)

Examples

The following example defines a pool of host LUs. A pool of 253 host LUs is defined with all LUs supplied from the ibm3745 host PU:

```
dspu host ibm3745 xid-snd 065000001 rmac 4000.3745.0001
dspu pool hostpool host ibm3745 lu 2 254
```

The following example defines multiple pools and defines a disjoint pool of host LUs. One pool with a total of 205 host LUs and second pool with a total of 48 host LUs are defined with all LUs supplied from the same ibm3745 host PU. Host LUs with addresses 2 to 201 and 250 to 254 are defined in hostpool1. Host LUs with addresses 202 to 249 are defined in hostpool2.

```
dspu host ibm3745 xid-snd 065000001 rmac 4000.3745.0001
dspu pool hostpool1 host ibm3745 lu 2 201
dspu pool hostpool2 host ibm3745 lu 202 249
dspu pool hostpool1 host ibm3745 lu 250 254
```

The following example defines a pool of LUs from multiple hosts. A pool of 506 host LUs is defined with 253 LUs supplied by the ibm3475 host PU and 253 supplied by the ibm3172 host PU.

```
dspu host ibm3745 xid-snd 065000001 rmac 4000.3745.0001
dspu host ibm3172 xid 06500002 rmac 4000.3172.0001
dspu pool hostpool host ibm3745 lu 2 254
dspu pool hostpool host ibm3172 lu 2 254
```

Related Commands

Command	Description
dspu host (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu host (QLLC)	Defines a DSPU host over an X.25/QLLC connection.
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)

To define an explicit downstream physical unit (PU) over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), virtual data-link control, or NCIA connections, use the **dspu pu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu pu *pu-name* [**rmac** *remote-mac*] [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**interface** *slot* | *port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

no dspu pu *pu-name* [**rmac** *remote-mac*] [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Syntax Description

pu-name	Name of the downstream PU.
rmac *remote-mac*	(Optional) MAC address of the downstream PU.
rsap *remote-sap*	(Optional) service access point (SAP) address of the downstream PU. The default is 4.
lsap *local-sap*	(Optional) Local SAP address used by the downstream physical unit (DSPU) to establish connection with the downstream PU. The default is 8.
xid-rcv *xid*	(Optional) Specifies a match on exchange identification (XID).
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive sizes used for the downstream PU link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is from 1 to 600 seconds. The default is 30 seconds.

Defaults

The default remote SAP is 4.
The default local SAP is 8.
The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 4.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The local SAP address must be enabled by one of the following commands:

- **dspu enable-pu lsap fo5**
- **dspu ncia enable-pu lsap**
- **dspu rsrb enable-pu lsap**
- **dspu vdlc enable-pu lsap**

The send and receive maximum I-frame size includes the Systems Network Architecture (SNA) transmission header (TH) and request/response (RH), but does not include the data-link control header. The DSPU feature will segment frames being sent to fit within this frame size. If an XID is received from a remote PU, which indicates that it supports a different maximum I-frame size, then the lower of the two values is used.

If you want the DSPU to attempt a ConnectOut to the remote node using the **dspu start** command, you must configure the **rmac** keyword and argument. If you want this PU to match against a ConnectIn attempt, then several combinations of the **rmac**, **rsap**, and **xid-rcv** keywords are possible. The matching algorithms are as follows:

- **rmac**—Match on remote MAC/SAP address of downstream PU.
- **xid-rcv**—Match on XID value received from downstream PU.
- **rmac/rsap, xid-rcv**—Match on remote MAC or SAP address of downstream PU and XID value received from downstream PU.

If an XID is received from a remote PU, which indicates that it supports a different maximum I-frame size, then the lower of the two values is used.

For Cisco IOS Release 11.3 and later releases, the number of DSPU PUs that can be configured is 1024.

Examples

In the following example, a downstream PU is defined with only the MAC address and SAP address specified. A downstream PU that attempts an incoming connection to the DSPU will be accepted only if the remote MAC or SAP address matches the configured values for this downstream PU (and the proper local SAP address is enabled).

```
dspu pu ciscopu rmac 1000.5AED.1F53 rsap 20
dspu lu 2 5 pool hostpool
interface tokenring 0
dspu enable-pu lsap 8
```

In the following example, a downstream PU is defined with only an **xid-rcv** value. Any downstream PU that attempts an incoming connection specifying the **xid-rcv** value, 05D00001, will be accepted without regard to remote MAC or SAP address (although the proper local SAP address must be enabled).

```
dspu pu ciscopu xid-rcv 05d00001
dspu lu 2 5 pool hostpool
interface tokenring 0
 dspu enable-pu lsap 8
```

In the following example, a downstream PU is defined with **xid-rcv**, **rmac**, and **rsap** keywords. Any downstream PU that attempts to connect in to the DSPU must match all three configured values for the connection to be accepted (the proper local SAP address must also be enabled).

```
dspu pu ciscopu rmac 1000.5AED.1F53 rsap 20 xid-rcv 05d00001
dspu lu 2 5 pool hostpool
interface tokenring 0
 dspu enable-pu lsap 8
```

Related Commands

Command	Description
dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)	Enables an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstream PU connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.
dspu ncia enable-pu	Enables a SAP on the NCIA server for use by downstream connections.
dspu rsrb enable-pu	Enables an RSRB SAP for use by DSPU downstream connections.
dspu rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name through the RSRB.
dspu start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name.
dspu vdlc enable-pu	Enables a SAP for use by DSPU virtual data-link control (VDLC) downstream connections.

dspu pu (Frame Relay)

To define a downstream physical unit (DSPU) host over a Frame Relay connection, use the **dspu pu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu pu *pu-name* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**interface** *slot* | *port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

no dspu pu *pu-name* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Syntax Description

pu-name	Name of the downstream physical unit (PU).
dlci *dlci-number*	Frame Relay data-link connection identifier (DLCI) number. This number is a decimal.
rsap *remote-sap*	(Optional) service access point (SAP) address of the downstream PU. The default is 4.
lsap *local-sap*	(Optional) Local SAP address used by the DSPU to establish connection with the downstream PU. The default is 8.
xid-rcv *xid*	(Optional) Specifies a match on exchange identification (XID).
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive sizes used for the downstream PU link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is from 1 to 600 seconds. The default is 30 seconds.

Defaults

The default remote SAP is 4.
The default local SAP is 8.
The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 4.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example defines a downstream PU:

```
dspu pu pub dlci 8
```

Related Commands

Command	Description
dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)	Enables an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstream PU connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu pu (QLLC)

To explicitly define a downstream physical unit (PU) over an X.25 connection, use the **dspu pu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu pu *pu-name* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**xid-rcv** *xid*] [**interface** *slot* | *port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

no dspu pu *pu-name* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**xid-rcv** *xid*] [**interface** *slot* | *port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Syntax Description

pu-name	Name of the downstream PU.
x25 *remote-x121-addr*	Variable-length X.121 address. It is assigned by the X.25 network service provider.
qllc *local-x121-subaddr*	(Optional) Local X.121 subaddress.
xid-rcv *xid*	(Optional) Specifies a match on exchange identification (XID).
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive sizes used for the downstream PU link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is from 1 to 600 seconds. The default is 30 seconds.

Defaults

The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 4.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example defines a downstream PU:

```
dspu pu testpu x25 32012 qllc 12 xid-rcv 05d00001
```

Related Commands

Command	Description
dspu enable-pu (QLLC)	Enables an X.121 subaddress for use by downstream PU connections through QLLC.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu pu (SDLC)

To define a downstream physical unit (DSPU) host over an Synchronous Data Link Control (SDLC) connection, use the **dspu pu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu pu *pu-name* **sdlc** *sdlc-addr* [**xid-rcv** *xid*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

no dspu pu *pu-name* **sdlc** *sdlc-addr* [**xid-rcv** *xid*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Syntax Description

pu-name	Name of the downstream PU.
sdlc *sdlc-addr*	SDLC address.
xid-rcv *xid*	(Optional) Specifies a match on exchange identification (XID).
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive sizes used for the downstream PU link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is from 1 to 600 seconds. The default is 30 seconds.

Defaults

The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 4.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example defines a downstream PU:

```
dspu pu testpu sdlc c1 interface serial 1/1
```

Related Commands

Command	Description
dspu enable-pu (SDLC)	Enables an SDLC address for use by downstream PU connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu rsrb

To define the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the downstream physical unit (DSPU) feature will simulate at the remote source-route bridging (RSRB), use the **dspu rsrb** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu rsrb *local-virtual-ring bridge-number target-virtual-ring virtual-macaddr*

no dspu rsrb *local-virtual-ring bridge-number target-virtual-ring virtual-macaddr*

Syntax Description

local-virtual-ring	DSPU local virtual ring number.
bridge-number	Bridge number connecting the DSPU local virtual ring and the RSRB target virtual ring. The valid range is from 1 to 15.
target-virtual-ring	RSRB target virtual ring number. The RSRB target virtual ring corresponds to the **ring-number** value defined by a **source-bridge ring-group** command.
virtual-macaddr	DSPU virtual MAC address.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The *bridge-number* argument can be specified only once in a configuration.

Use the **dspu rsrb** command to enable DSPU host and downstream connections to be established across an RSRB link.

If the **local-ack** value is specified on the **source-bridge remote-peer** statement, DSPU will establish host connections across RSRB using local acknowledgment. DSPU cannot support local acknowledgment for downstream PU connections across RSRB.

Examples

The following example defines DSPU to start a connection to the host across an RSRB link (without local acknowledgment). The DSPU is identified by its local ring number 88 and its virtual MAC address 4000.FFFF.0001. When the DSPU attempts an outgoing connection to the ibm3745 host, the connection will be established across the RSRB virtual ring 99.

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

dspu rsrb 88 1 99 4000.FFFF.0001
dspu rsrb enable-host lsap 10

dspu host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10
dspu rsrb start ibm3745
interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

The following example defines the DSPU to start a connection to the host across an RSRB link (with local acknowledgment). The DSPU is identified by its local ring number 88 and its virtual MAC address 4000.FFFF.0001. When the DSPU attempts an outward connection to the ibm3745 host, the connection will be established across the RSRB virtual ring 99 using RSRB local acknowledgment.

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2 local-ack

dspu rsrb 88 1 99 4000.FFFF.0001
dspu rsrb enable-host lsap 10

dspu host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10
dspu rsrb start ibm3745

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

The following example define the s DSPU to allow a connection from the downstream PU across an RSRB link. The DSPU is identified by its local ring number 88 and its virtual MAC address 4000.FFFF.0001. The downstream PU will specify the DSPU virtual MAC address 4000.FFFF.0001 and SAP address 20 in its host definitions. The DSPU will accept incoming connections from the downstream PU across the RSRB virtual ring 99.

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

dspu rsrb 88 1 99 4000.FFFF.0001
dspu rsrb enable-pu lsap 20

dspu pu ciscopu xid-rcv 05D00001 lsap 20

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
dspu rsrb enable-host	Enables an RSRB SAP for use by DSPU host connections.
dspu rsrb enable-pu	Enables an RSRB SAP for use by DSPU downstream connections.
dspu rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name through the RSRB.
source-bridge ring-group	Defines or removes a ring group from the configuration.
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

dspu rsrb enable-host

To enable an remote source-route bridging (RSRB) service access point (SAP) for use by downstream physical unit (DSPU) host connections, use the **dspu rsrb enable-host** command in global configuration mode. To disable the RSRB SAP, use the **no** form of this command.

dspu rsrb enable-host [**lsap** *local-sap*]

no dspu rsrb enable-host [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connections attempts and for starting outgoing connection attempts. The default is 12.

Defaults

The default local SAP is 12.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the local SAP address 10 of the RSRB is enabled for use by the ibm3745 host physical unit (PU):

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

dspu rsrb 88 1 99 4000.FFFF.0001
dspu rsrb enable-host lsap 10

dspu host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections.
dspu rsrb	Defines the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the DSPU feature will simulate at the RSRB.

dspu rsrb enable-pu

To enable an remote source-route bridging (RSRB) service access point (SAP) for use by downstream physical unit (DSPU) downstream connections, use the **dspu rsrb enable-pu** command in global configuration mode. To disable the SAP, use the **no** form of this command.

dspu rsrb enable-pu [**lsap** *local-sap*]

no dspu rsrb enable-pu [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts. The default is 8.

Defaults

The default local SAP is 8.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the local SAP address 20 of the RSRB is enabled for use by the ciscopu DSPU downstream physical unit (PU):

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

dspu rsrb 88 1 99 4000.FFFF.0001
dspu rsrb enable-pu lsap 20

dspu pu ciscopu xid-rcv 05D00001 lsap 20
```

Related Commands

Command	Description
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.
dspu rsrb	Defines the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the DSPU feature will simulate at the RSRB.

dspu rsrb start

To specify that an attempt will be made to connect to the remote resource defined by host name or physical unit (PU) name through the remote source-route bridging (RSRB), use the **dspu rsrb start** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu rsrb start {*host-name* | *pu-name*}

no dspu rsrb start {*host-name* | *pu-name*}

Syntax Description

host-name	Name of a host defined in a **dspu host** (Token Ring, Ethernet, FDDI, RSRB, virtual data-link control (VDLC)) command.
pu-name	Name of a PU defined in a **dspu host** (Token Ring, Ethernet, FDDI, RSRB, VDLC) command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before issuing this command, you must enable the correct local service access point (SAP) with the appropriate enable command (**dspu rsrb enable-host** for a host resource, and **dspu rsrb enable-pu** for a PU resource).

This command is valid only if the target MAC address has been defined in the resource. For a host resource, this is not a problem because the MAC address is mandatory, but for a PU resource the MAC address is optional. The command will fail if the MAC address is missing.

Examples

In the following example, the downstream physical unit (DSPU) will initiate a connection with the ibm3745 host PU across the RSRB link:

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

dspu rsrb 88 1 99 4000.FFFF.0001
dspu rsrb enable-host lsap 10

dspu host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10
dspu rsrb start ibm3745

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.
dspu rsrb	Defines the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the DSPU feature will simulate at the RSRB.
dspu rsrb enable-host	Enables an RSRB SAP for use by DSPU host connections.
dspu rsrb enable-pu	Enables an RSRB SAP for use by DSPU downstream connections.

dspu start

To specify that an attempt will be made to connect to the remote resource defined by host name or physical unit (PU) name, use the **dspu start** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

dspu start {*host-name* | *pu-name*}

no dspu start {*host-name* | *pu-name*}

Syntax Description

host-name	Name of a host defined in a **dspu host** command.
pu-name	Name of a PU defined in a **dspu pu** command.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before issuing this command, you must enable the correct address using the appropriate **dspu enable-host** or **dspu enable-pu** command.

This command is valid only if the target address (remote MAC [RMAC], Synchronous Data Link Control [SDLC], data-link connection identifier [DLCI], or X.25 parameter) has been defined for the resource. For a host resource, this is not a problem because the address specification is mandatory, but for a PU resource, specifying the address is optional. The **dspu start** command will fail if the address is missing.

Examples

In the following example, the downstream physical unit (DSPU) will initiate a connection with the ciscopu downstream PU on Token Ring interface 0:

```
dspu pu ciscopu xid-rcv 05D00001 rmac 1000.5AED.1F53 lsap 20
interface tokenring 0
 dspu enable-pu lsap 20
 dspu start ciscopu
```

Related Commands

Command	Description
dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay)	Enables a local service access point (SAP) on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts.
dspu enable-host (QLLC)	Enables an X.121 subaddress for use by upstream host connections through QLLC.
dspu enable-host (SDLC)	Enables an SDLC address for use by upstream host connections.
dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)	Enables an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstream PU connections.
dspu enable-pu (SDLC)	Enables an SDLC address for use by downstream PU connections.
dspu enable-pu (QLLC)	Enables an X.121 subaddress for use by downstream PU connections through QLLC.
dspu host (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu host (QLLC)	Defines a DSPU host over an X.25/QLLC connection.
dspu host (SDLC)	Defines a DSPU host over an SDLC connection.
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
dspu pu (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu pu (QLLC)	Defines a downstream PU over an X.25 connection explicitly.
dspu pu (SDLC)	Defines a DSPU host over an SDLC connection.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.

dspu vdlc

To identify the local virtual ring and virtual MAC address that will be used to establish downstream physical unit (DSPU) host and downstream connections over data-link switching plus (DLSw+) using virtual data-link control, use the **dspu vdlc** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu vdlc *ring-group virtual-mac-address*

no dspu vdlc *ring-group virtual-mac-address*

Syntax Description

ring-group	Local virtual ring number identifying the SRB ring group.
virtual-mac-address	Virtual MAC address that represents the DSPU virtual data-link control.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The virtual data-link control local virtual ring must have been previously configured using the **source-bridge ring-group** command.

The virtual data-link control virtual MAC address must be unique within the DLSw+ network.

To avoid an address conflict on the virtual MAC address, use a locally administered address in the form 4000.*xxxx.xxxx*.

Examples

The following example defines the DSPU to start a connection to the host using virtual data-link control. The DSPU virtual data-link control is identified by its virtual MAC address 4000.4500.01f0, existing on the SRB virtual ring 99. When the DSPU attempts an outgoing connection to the host HOST-B, the connection will be established across the virtual ring 99.

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

dspu vdlc 99 4000.4500.01f0
dspu vdlc enable-host lsap 12
dspu host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint

dspu vdlc start HOST-B

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
dlsw local-peer	Defines the parameters of the DLSw+ local peer.
dlsw remote-peer tcp	Identifies the IP address of a peer with which to exchange traffic using TCP.
dspu vdlc enable-host	Enables a SAP for use by DSPU host connections.
dspu vdlc enable-pu	Enables a SAP for use by DSPU VDLC downstream connections.
dspu vdlc start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name through VDLC.
source-bridge ring-group	Defines or removes a ring group from the configuration.

dspu vdlc enable-host

To enable a service access point (SAP) for use by downstream physical unit (DSPU) host connections, use the **dspu vdlc enable-host** command in global configuration mode. To disable the SAP, use the **no** form of this command.

dspu vdlc enable-host [**lsap** *local-sap*]

no dspu vdlc enable-host [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connections attempts and for starting outgoing connection attempts. The default is 12.

Defaults

The default local SAP is 12.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the local SAP address 12 is enabled for use by the host PU HOST-B:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

dspu vdlc 99 4000.4500.01f0
dspu vdlc enable-pu lsap 8
dspu vdlc enable-host lsap 12

dspu host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint
dspu pool pool-b host HOST-B lu 2 254

dspu host HOST3K-A xid-snd 05d0000a rmac 4000.3000.0100 rsap 8 lsap 12
dspu pool pool3k-a host HOST3K-A lu 2 254

dspu pu PU3K-A xid-rcv 05d0000a rmac 4000.3000.0100 rsap 10 lsap 8
dspu lu 2 254 pool pool-b

dspu default-pu
dspu lu 2 5 pool pool3k-a

dspu vdlc start HOST-B
dspu vdlc start HOST3K-A
dspu vdlc start PU3K-A

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections.
dspu vdlc	Identifies the local virtual ring and virtual MAC address that will be used to establish DSPU host and downstream connections over DLSw+ using VDLC.

dspu vdlc enable-pu

To enable a service access point (SAP) for use by downstream physical unit (DSPU) virtual data-link control downstream connections, use the **dspu vdlc enable-pu** command in global configuration mode. To disable the SAP, use the **no** form of this command.

dspu vdlc enable-pu [**lsap** *local-sap*]

no dspu vdlc enable-pu [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts. The default is 8.

Defaults

The default local SAP is 8.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the local SAP address 8 is enabled for use by the downstream PU PU3K-A:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

dspu vdlc 99 4000.4500.01f0
dspu vdlc enable-pu lsap 8
dspu vdlc enable-host lsap 12

dspu host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint
dspu pool pool-b host HOST-B lu 2 254

dspu host HOST3K-A xid-snd 05d0000a rmac 4000.3000.0100 rsap 8 lsap 12
dspu pool pool3k-a host HOST3K-A lu 2 254

dspu pu PU3K-A xid-rcv 05d0000a rmac 4000.3000.0100 rsap 10 lsap 8
dspu lu 2 254 pool pool-b

dspu default-pu
dspu lu 2 5 pool pool3k-a

dspu vdlc start HOST-B
dspu vdlc start HOST3K-A
dspu vdlc start PU3K-A
interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
dspu pu (**Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA**)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.
dspu vdlc	Identifies the local virtual ring and virtual MAC address that will be used to establish DSPU host and downstream connections over DLSw+ using VDLC.

dspu vdlc start

To specify that an attempt will be made to connect to the remote resource defined by host name or physical unit (PU) name through virtual data-link control, use the **dspu vdlc start** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu vdlc start {*host-name* | *pu-name*}

no dspu vdlc start {*host-name* | *pu-name*}

Syntax Description

host-name	Name of a host defined in a **dspu host** command.
pu-name	Name of a PU defined in a **dspu host** command.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before issuing this command, you must enable the correct local service access point (SAP) with the appropriate enable command (**dspu vdlc enable-host** for a host resource, and **dspu vdlc enable-pu** for a PU resource).

This command is valid only if the target MAC address has been defined in the resource. For a host resource, this is not a problem because the MAC address is mandatory, but for a PU resource the MAC address is optional. The command will fail if the MAC address is missing.

Examples

In the following example, the downstream physical unit (DSPU) attempts to initiate connections with host PU HOST-B, host PU HOST3k-A, and downstream PU PU3k-A over data-link switching plus (DLSw+) using virtual data-link control:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

dspu vdlc 99 4000.4500.01f0
dspu vdlc enable-pu lsap 8
dspu vdlc enable-host lsap 12

dspu host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint
dspu pool pool-b host HOST-B lu 2 254

dspu host HOST3K-A xid-snd 05d0000a rmac 4000.3000.0100 rsap 8 lsap 12
dspu pool pool3k-a host HOST3K-A lu 2 254

dspu pu PU3K-A xid-rcv 05d0000a rmac 4000.3000.0100 rsap 10 lsap 8
dspu lu 2 254 pool pool-b

dspu default-pu
dspu lu 2 5 pool pool3k-a
dspu vdlc start HOST-B
dspu vdlc start HOST3K-A
dspu vdlc start PU3K-A

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.
dspu vdlc	Identifies the local virtual ring and virtual MAC address that will be used to establish DSPU host and downstream connections over DLSw+ using VDLC.
dspu vdlc enable-host	Enables a SAP for use by DSPU host connections.
dspu vdlc enable-pu	Enables a SAP for use by DSPU VDLC downstream connections.

enable (TN3270)

To turn on security in the TN3270 server, use the **enable** command in security configuration mode.

enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Security configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

If the **security** command has been disabled, then issuing this command does not affect existing connections.

This command is not displayed in the **show running-config** command output because the security functionality is enabled by default.

Examples

The following example turns on security in the TN3270 server:

```
enable
```

Related Commands

Command	Description
security (TN3270)	Enables security on the TN3270 server.
disable (TN3270)	Turns off security in the TN3270 server.

encapsulation alc

To specify that the P1024B Airline Control (ALC) protocol will be used on the serial interface, use the **encapsulation alc** command in interface configuration mode. To remove ALC protocol handling from the serial interface, and return the default encapsulation high-level data link control (HDLC) to the interface, use the **no** form of this command.

encapsulation alc

no encapsulation alc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation alc** command causes any agent-set control unit (ASCU) configuration to be removed from the interface. As each ASCU defined on the interface is removed it is also unlinked from the ASCU circuit it belongs to. All data frames queued for sending to the ASCU are destroyed.

This command must be entered prior to any ASCU configuration. Note that all timer and counter values are applicable to all ASCUs on the interface.

Examples

The following example specifies that the ALC protocol is used:

```
encapsulation alc
```

Related Commands

Command	Description
show interfaces	Displays statistics for the interfaces configured on a router or access server.

encapsulation bstun

To configure block serial tunnel (BSTUN) on a particular serial interface, use the **encapsulation bstun** command in interface configuration mode. To disable the BSTUN function on the interface, use the **no** form of this command.

encapsulation bstun

no encapsulation bstun

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation bstun** command must be configured on an interface before any further BSTUN or Bisync commands are configured for the interface.

You must use this command to enable BSTUN on an interface. Before using this command, perform the following two tasks:

- Enable BSTUN on a global basis by identifying BSTUN on IP addresses. The command is **bstun peer-name**.
- Define a protocol group number to be applied to the interface. Packets travel only between interfaces that are in the same protocol group. The command is **bstun protocol-group**.

After using the **encapsulation bstun** command, use the **bstun group** command to place the interface in the previously defined protocol group.

Examples

The following example configures the BSTUN function on serial interface 0:

```
interface serial 0
 no ip address
 encapsulation bstun
```

Related Commands

Command	Description
bstun group	Specifies the BSTUN group to which the interface belongs.
bstun peer-name	Enables the BSTUN function.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.

encapsulation sdlc

To configure an Synchronous Data Link Control (SDLC) interface, use the **encapsulation sdlc** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

encapsulation sdlc

no encapsulation sdlc

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation sdlc** command must be used to configure an SDLC interface if you plan to implement data-link switching plus (DLSw+) or Frame Relay access support.

SDLC defines two types of network nodes: primary and secondary. Primary nodes poll secondary nodes in a predetermined order. Secondaries then send if they have outgoing data. When configured as primary and secondary nodes, Cisco routers are established as SDLC stations. Use the **sdlc role** interface configuration command to establish the role as primary or secondary.

In the IBM environment, a front-end processor (FEP) is the primary station and establishment controllers (ECs) are secondary stations. In a typical scenario, an EC may be connected to dumb terminals and to a Token Ring network at a local site. At the remote site, an IBM host connects to an IBM FEP, which can also have links to another Token Ring LAN. Typically, the two sites are connected through an SDLC leased line.

If a router is connected to an EC, it takes over the function of the FEP, and must therefore be configured as a primary SDLC station. If the router is connected to a FEP, it takes the place of the EC, and must therefore be configured as a secondary SDLC station.

Examples

The following example configures an SDLC interface:

```
interface serial 2/6
 no ip address
 encapsulation sdlc
```

Related Commands

Command	Description
sdlc role	Establishes the router to be either a primary or secondary SDLC station.

encapsulation sdlc-primary

To configure the router as the primary Synchronous Data Link Control (SDLC) station if you plan to configure the SDLC Logical Link Control (SDLLC) media translation feature, use the **encapsulation sdlc-primary** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

encapsulation sdlc-primary

no encapsulation sdlc-primary

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation sdlc-primary** or **encapsulation sdlc-secondary** command must be used to configure an SDLC interface. To use the **encapsulation sdlc-primary** command, first select the interface on which you want to enable SDLC. Then establish the router as a primary station. Next, assign secondary station addresses to the primary station using the **sdlc address** command.

SDLC defines two types of network nodes: primary and secondary. Primary nodes poll secondary nodes in a predetermined order. Secondaries then send if they have outgoing data. When configured as primary and secondary nodes, Cisco routers are established as SDLC stations.

In the IBM environment, a front-end processor (FEP) is the primary station and establishment controllers (ECs) are secondary stations. In a typical scenario, an EC may be connected to dumb terminals and to a Token Ring network at a local site. At the remote site, an IBM host connects to an IBM FEP, which can also have links to another Token Ring LAN. Typically, the two sites are connected through an SDLC leased line.

If a router is connected to an EC, it takes over the function of the FEP, and must therefore be configured as a primary SDLC station. If the router is connected to an FEP, it takes the place of the EC, and must therefore be configured as a secondary SDLC station.

Examples

The following example shows how to configure serial interface 0 on your router to allow two SDLC secondary stations to attach through a modem-sharing device (MSD) with addresses C1 and C2:

```
! enter a global command if you have not already
interface serial 0
 encapsulation sdlc-primary
 sdlc address c1
 sdlc address c2
```

Related Commands

Command	Description
encapsulation sdlc-secondary	Configures the router as a secondary SDLC station if you plan to configure the SDLLC media translation feature.
sdlc address	Assigns a set of secondary stations attached to the serial link.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

encapsulation sdlc-secondary

To configure the router as a secondary Synchronous Data Link Control (SDLC) station if you plan to configure the SDLC Logical Link Control (SDLLC) media translation feature, use the **encapsulation sdlc-secondary** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

encapsulation sdlc-secondary

no encapsulation sdlc-secondary

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An **encapsulation sdlc-primary** or **encapsulation sdlc-secondary** command must be used to configure an SDLC interface. To use the **encapsulation sdlc-secondary** command, select the interface on which you want to enable SDLC. Then establish the router as a secondary station. Next, assign secondary station addresses to the primary station using the **sdlc address** command.

SDLC defines two types of network nodes: primary and secondary. Primary nodes poll secondary nodes in a predetermined order. Secondaries then send if they have outgoing data. When configured as primary and secondary nodes, Cisco devices are established as SDLC stations.

In the IBM environment, a front-end processor (FEP) is the primary station and establishment controllers (ECs) are secondary stations. In a typical scenario, an EC may be connected to dumb terminals and to a Token Ring network at a local site. At the remote site, an IBM host connects to an IBM FEP, which can also have links to another Token Ring LAN. Typically, the two sites are connected through an SDLC leased line.

If a router is connected to an EC, it takes over the function of the FEP, and must therefore be configured as a primary SDLC station. If the router is connected to a FEP, it takes the place of the EC, and must therefore be configured as a secondary SDLC station.

Examples

The following example establishes the router as a secondary SDLC station:

```
interface serial 0
 encapsulation sdlc-secondary
```

Related Commands

Command	Description
encapsulation sdlc-primary	Configures the router as the primary SDLC station if you plan to configure the SDLLC media translation feature.
sdlc address	Assigns a set of secondary stations attached to the serial link.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

encapsulation stun

To enable serial tunnel (STUN) encapsulation on a specified serial interface, use the **encapsulation stun** command in interface configuration mode.

encapsulation stun

Syntax Description

This command has no arguments or keywords.

Defaults

STUN encapsulation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enable STUN on an interface. Before using this command, perform the following two tasks:

- Enable STUN on a global basis by identifying STUN on IP addresses. The command is **stun peer-name**.
- Define a protocol group number to be applied to the interface. Packets travel only between interfaces that are in the same protocol group. The command is **stun protocol-group**.

After using the **encapsulation stun** command, use the **stun group** command to place the interface in the previously defined protocol group.

To disable stun encapsulation, configure the default interface encapsulation using the **encapsulation** command and specify HDLC as the encapsulation type

There is not a **no** form for this command.

Examples

This partial configuration example shows how to enable serial interface 5 for STUN traffic:

```
! sample stun peer name and stun protocol-group global commands
stun peer-name 10.108.254.6
stun protocol-group 2 sdlc
!
interface serial 5
! sample ip address command
no ip address
! enable the interface for STUN; must specify encapsulation stun
! command to further configure the interface
encapsulation stun
! place interface serial 5 in previously defined STUN group 2
stun group 2
! enter stun route command
stun route 7 tcp 10.108.254.7
```

Related Commands

Command	Description
stun group	Places each STUN-enabled interface on a router in a previously defined STUN group.
stun peer-name	Enables STUN for an IP address.
stun protocol-group	Creates a protocol group.

encapsulation uts

To specify that the P1024C Universal Terminal Support (UTS) protocol will be used on the serial interface, use the **encapsulation uts** command in interface configuration mode. To remove P1024C UTS protocol handling from the serial interface and return the default encapsulation high-level data link control (HDLC) to the interface, use the **no** form of this command.

encapsulation uts

no encapsulation uts

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation uts** command causes any agent-set control unit (agent-set control unit (ASCU)) configuration to be removed from the interface. As each ASCU defined on the interface is removed it is also unlinked from the ASCU circuit it belongs to. All data frames queued for sending to the ASCU are destroyed.

This command must be entered prior to any ASCU configuration. Note that all timer and counter values are applicable to all ASCUs on the interface.

Examples

The following example specifies that the P1024C UTS protocol is used:

```
encapsulation uts
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on a router or access server.

encryptorder

To specify the security encryption algorithm for the Secure Socket Layer (SSL) Encryption Support feature, use the **encryptorder** command in profile configuration mode.

encryptorder [**RC4**] [**RC2**] [**RC5**] [**DES**] [**3DES**]

Syntax Description

RC4	(Optional) Specifies the RC4 encryption algorithm.
RC2	(Optional) Specifies the RC2 encryption algorithm.
RC5	(Optional) Specifies the RC5 encryption algorithm.
DES	(Optional) Specifies the DES encryption algorithm.
3DES	(Optional) Specifies the 3DES encryption algorithm.

Defaults

The default encryption order is RC4, RC2, RC5, DES, 3DES for domestic software. The default encryption order is RC4, RC2, DES for exportable software.

Command Modes

Profile configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

These algorithms may be entered in any order, but can be specified only once per **encryptorder** command.

Exportable versions of software cannot accept the 3DES or RC5 encryption algorithms.

Examples

The following example specifies RC4, DES, and RC2 as the encryption algorithms:

```
tn3270
 security
 profile DOMESTIC SSL
  encryptorder RC4 DES RC2
```

ethernet-transit-oui

To choose the Organizational Unique Identifier (OUI) code to be used in the encapsulation of Ethernet Type II frames across Token Ring backbone networks, use the **ethernet-transit-oui** command in subinterface configuration mode. Various versions of this OUI code are used by Ethernet/Token Ring translational bridges. To return the default OUI code, use the **no** form of this command.

ethernet-transit-oui [**90-compatible** | **standard** | **cisco**]

no ethernet-transit-oui

Syntax Description

90-compatible	(Optional) Default OUI form.
standard	(Optional) Standard OUI form.
cisco	(Optional) Cisco's OUI form.

Defaults

The default OUI form is 90-compatible.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before using this command, you must have completely configured your router using multiport source bridging and transparent bridging.

The **standard** keyword is used when you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity.

Table 12 shows the actual OUI codes used, when they are used, and how they compare to Software Release 9.0-equivalent commands.

Table 12 Bridge OUI Codes

Keyword	OUI Used	When Used/Benefits	Software Release 9.0 Command Equivalent
90-compatible	0000F8	By default, when talking to other Cisco routers. Provides the most flexibility.	**no bridge old-oui**

Table 12 Bridge OUI Codes (continued)

Keyword	OUI Used	When Used/Benefits	Software Release 9.0 Command Equivalent
cisco	00000C	Provided for compatibility with future equipment.	None
standard	000000	When talking to IBM 8209 bridges and other vendor equipment. Does not provide for as much flexibility as the other two choices.	**bridge old-oui**

Specify the **90-compatible** keyword when talking to our routers. This keyword provides the most flexibility. When **90-compatible** is specified or the default is used, Token Ring frames with an OUI of 0x0000F8 are translated into Ethernet Type II frames and Token Ring frames with the OUI of 0x000000 are translated into Subnetwork Access Protocol (SNAP)-encapsulated frames. Specify the **standard** keyword when talking to IBM 8209 bridges and other vendor equipment. This OUI does not provide for as much flexibility as the other two choices. The **cisco** keyword oui is provided for compatibility with future equipment.

Do not use the **standard** keyword unless you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity. Only use the **standard** keyword only when you are transferring data between IBM 8209 Ethernet/Token Ring bridges and routers running the source-route translational bridging (SR/TLB) software (to create a Token Ring backbone to connect Ethernets).

Use of the **standard** keyword causes the OUI code in Token Ring frames to always be 0x000000. In the context of the **standard** keyword, an OUI of 0x000000 identifies the frame as an Ethernet Type II frame. (Compare with 90-compatible, where 0x000000 OUI means SNAP-encapsulated frames.)

If you use the **90-compatible** keyword, the router, acting as an SR/TLB, can distinguish immediately on Token Ring interfaces between frames that started on an Ethernet Type II frame and those that started on an Ethernet as a SNAP-encapsulated frame. The distinction is possible because the router uses the 0x0000F8 OUI when converting Ethernet Type II frames into Token Ring SNAP frames, and leaves the OUI as 0x000000 for Ethernet SNAP frames going to a Token Ring. This distinction in OUIs leads to efficiencies in the design and execution of the SR/TLB product; no tables need to be kept to know which Ethernet hosts use SNAP encapsulation and which hosts use Ethernet Type II.

The IBM 8209 bridges, however, by using the 0x000000 OUI for all the frames entering the Token Ring, must take extra measures to perform the translation. For every station on each Ethernet, the 8209 bridges attempt to remember the frame format used by each station, and assume that once a station sends out a frame using Ethernet Type II or 802.3, it will always continue to do so. It must do this because in using 0x000000 as an OUI, there is no way to distinguish between SNAP and Type II frame types. Because the SR/TLB router does not need to keep this database, when 8209 compatibility is enabled with the **standard** keyword, the SR/TLB chooses to translate all Token Ring SNAP frames into Ethernet Type II frames as described earlier in this discussion. Because every nonroutable protocol on Ethernet uses either non-SNAP 802.3 (which traverses fully across a mixed IBM 8209/ router Token Ring backbone) or Ethernet Type II, this results in correct inter connectivity for virtually all applications.

Do not use the **standard** keyword OUI if you want SR/TLB to output Ethernet SNAP frames. Using either the **90-compatible** or **cisco** keyword OUI does not present such a restriction, because SNAP frames and Ethernet Type II-encapsulated frames have different OUI codes on Token Ring networks.

Examples

The following example specifies standard OUI form:

```
interface tokenring 0
 ethernet-transit-oui standard
```

Related Commands

Command	Description
source-bridge transparent	Establishes bridging between transparent bridging and SRB.

exception slot

To provide a core dump of a Cisco Mainframe Channel Connection (CMCC) adapter, use the **exception slot** command in global configuration mode. To disable the core dump, use the **no** form of this command.

exception slot [*slot*] *protocol*://*host*/*filename*

no exception slot [*slot*] *protocol*://*host*/*filename*

Syntax Description

slot	(Optional) Slot number of the CMCC adapter. If no *slot* value is specified, all installed CMCC adapters will output a core dump when they halt unexpectedly.
protocol	Protocol for transferring the file. Currently, the only allowed value is FTP. The colon and two slash marks are required.
host	Name or IP address of the host that receives the core dump information. The slash mark is required.
filename	Filename on the host that receives the core dump information. The maximum name length is 31 characters. When written to the host, the *slot* argument is automatically appended, where *slot* is the slot number.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is supported only on the Cisco 7000 with RSP7000 and Cisco 7500 series routers.

You must configure FTP services on the router before you can create a CMCC adapter core dump.

Do not exceed your host limits on filename length. Two characters are added to the filename, *slot*, where *slot* is the slot number.

Examples

The following example shows how to configure a router to perform a CMCC adapter core dump. Assuming the Channel Interface Processor (CIP) is installed in slot 3, the filename cipdump.3 will be written to the host.

```
ip domain-name cisco.com
ip name-server 168.69.161.21
ip ftp username tech1
ip ftp password tech1
exception slot ftp://168.18.2.196/cipdump
```

Related Commands

Command	Description
ip domain-name	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
ip ftp username	Configures the username for FTP connections.
ip ftp password	Specifies the password to be used for FTP connections.

frame-relay map bridge broadcast

To bridge over a Frame Relay network, use the **frame-relay map bridge broadcast** command in interface configuration mode. To delete the mapping entry, use the **no** form of this command.

frame-relay map bridge *dlci* **broadcast**

no frame-relay map bridge *dlci* **broadcast**

Syntax Description

dlci	Data Link Connection Identifier (DLCI) number. The valid range is from 16 to 1007.

Defaults

No mapping entry is established.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Bridging over a Frame Relay network is supported on networks that do and do not support a multicast facility.

The following example allows bridging over a Frame Relay network:

```
frame-relay map bridge 144 broadcast
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.

frame-relay map bstun

To configure block serial tunnel (BSTUN) over Frame Relay for pass-through, use the **frame-relay map bstun** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

frame-relay map bstun *dlci*

no frame-relay map bstun *dlci*

Syntax Description

dlci	Frame Relay DLCI number on which to support pass-through.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Direct encapsulation over Frame Relay is supported only for an encapsulation type of cisco, configured using the **encapsulation frame-relay** command.

Examples

The following example maps BSTUN traffic to DLCI number 16:

```
frame-relay map bstun 16
```

Related Commands

Command	Description
bstun lisnsap	Configures a service access point (SAP) on which to listen for incoming calls.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
encapsulation frame-relay	Enables Frame Relay encapsulation.

frame-relay map llc2

To configure block serial tunnel (BSTUN) over Frame Relay when using Bisync local acknowledgment, use the **frame-relay map llc2** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

frame-relay map llc2 *dlci*

no frame-relay map llc2 *dlci*

Syntax Description

dlci	Frame Relay data-link connection identifier (DLCI) number on which to support local acknowledgment.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Direct encapsulation over Frame Relay is supported only for an encapsulation type of cisco, configured using the **encapsulation frame-relay** command.

Examples

The following example maps BSTUN traffic to data-link connection identifier (DLCI) number 16:

```
frame-relay map dlci 16
```

Related Commands

Command	Description
bstun lisnsap	Configures a service access point (SAP) on which to listen for incoming calls.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
encapsulation frame-relay	Enables Frame Relay encapsulation.

frame-relay map rsrb

To specify the data-link connection identifier (DLCI) number onto which the remote source-route bridging (RSRB) traffic is to be mapped, use the **frame-relay map rsrb** command in interface configuration mode. To cancel the RSRB map, use the **no** form of this command.

frame-relay map rsrb *dlci*

no frame-relay map rsrb

Syntax Description

dlci	Frame Relay DLCI.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Direct encapsulation over Frame Relay is supported only for an encapsulation type of cisco, configured using the **encapsulation frame-relay** command.

Examples

The following example shows RSRB traffic mapped to DLCI number 30:

```
frame-relay map rsrb 30
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.

fras backup dlsw

To configure an auxiliary route between the end stations and the host for use as a backup when the data-link connection identifier (DLCI) connection to the Frame Relay network is lost, use the **fras backup dlsw** command in interface configuration mode. To cancel the backup configuration, use the **no** form of this command.

fras backup dlsw *virtual-mac-address target-ring-number host-mac-address* [**retry** *retry-number*]

no fras backup dlsw *virtual-mac-address target-ring-number host-mac-address* [**retry** *retry-number*]

Syntax Description

virtual-mac-address	12-digit hexadecimal string used as a source MAC address for all packets going to the host.
target-ring-number	Number configured in the **source-bridge ring-group** command. This is a virtual ring. The valid range is from 1 to 4095.
host-mac-address	Destination MAC address of the host.
retry *retry-number*	(Optional) Number of attempts by the end station to reconnect to the primary Frame Relay interface before activating the backup link. The range is from 1 to 5 retries. If the **retry** option is not specified, the default number of retries is 5.

Defaults

Frame Relay access support (FRAS) dial backup over data-link switching plus (DLSw+) is disabled. The default number of retries is 5.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configure DLSw+ as normally required. Specify the optional keyword **dynamic** at the end of the **dlsw remote-peer** configuration command to enable the peer relationship to be established only when needed (for example, when the **fras backup dlsw** command becomes active).

Examples

The following example configures FRAS dial backup over DLSw+:

```
fras backup dlsw 4000.1000.2000 200 1000.5aed.1f53
```

Related Commands

Command	Description
dlsw local-peer	Defines the parameters of the DLSw+ local peer.
dlsw remote-peer tcp	Identifies the IP address of a peer with which to exchange traffic using TCP.
frame-relay lmi-type	Selects the LMI type.
frame-relay map llc2	Configures BSTUN over Frame Relay when using Bisync local acknowledgment.
fras map llc	Associates an LLC connection with a Frame Relay DLCI.
show fras	Displays notification that the FRAS dial backup over DLSw+ feature is active, information about the connection state in FRAS, and information about current BNN, boundary access node (BAN), and dial backup.
source-bridge ring-group	Defines or removes a ring group from the configuration.

fras ban

To associate bridging over a Frame Relay network using boundary access node (BAN), use the **fras ban** command in interface configuration mode. To cancel each association, use the **no** form of this command.

fras ban *local-ring bridge-number ring-group ban-dlci-mac* **dlci** *dlci1* [*dlci2 … dlci5*] [**bni** *mac-addr*]

no fras ban *local-ring bridge-number ring-group ban-dlci-mac* **dlci** *dlci1* [*dlci2 … dlci5*] [**bni** *mac-addr*]

Syntax Description

local-ring	Decimal number from 1 to 4095 describing the Token Ring interface.
bridge-number	Decimal number from 1 to 15 that uniquely identifies a bridge connecting two rings.
ring-group	Decimal number from 1 to 4095 representing a collection of Token Ring interfaces on one or more routers.
ban-dlci-mac	Frame Relay BAN permanent virtual circuit (PVC) MAC address.
dlci *dlci1* [*dlci2 … dlci5*]	Frame Relay data-link connection identifier (DLCI). The **dlci** keyword precedes the list of one or more DLCI numbers. If you need more than one DLCI number for load balancing, you can configure up to five DLCI numbers, separated by spaces. Each DLCI number must be unique and must be a decimal in the range from 16 through 1007.
bni *mac-addr*	(Optional) Boundary node identifier (BNI) MAC address of the NCP that receives frames from the router.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Multiple **fras ban** commands may be configured; however, each **fras ban** command must use a unique DLCI MAC address.

You must configure the **source-bridge ring-group** command in global configuration mode prior to configuring the **fras ban** command.

Examples

The following example shows Frame Relay access support (FRAS) BAN support for Token Ring and serial interfaces:

```
source-bridge ring-group 200
!
interface serial 0
 mtu 4000
 encapsulation frame-relay ietf
 frame-relay lmi-type ansi
 frame-relay map llc2  16
 frame-relay map llc2  17
 fras ban 120 1 200 4000.1000.2000 dlci 16 17
!
interface tokenring 0
 source-bridge 100 5 200
```

Related Commands

Command	Description
source-bridge ring-group	Defines or removes a ring group from the configuration.

fras ddr-backup

To configure an auxiliary interface for use as a backup when the primary Frame Relay link to the Frame Relay WAN fails, use the **fras ddr-backup** command in interface configuration mode. To cancel the backup configuration, use the **no** form of this command.

fras ddr-backup interface *interface dlci-number*

no fras ddr-backup

Syntax Description

interface *interface*	Interface over which the backup connection is made.
dlci-number	Data-link connection identifier (DLCI) number of the session.

Defaults

Frame Relay access support (FRAS) DLCI backup is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures FRAS DLCI backup on serial interface 1:

```
fras ddr-backup interface serial 1 188
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show fras	Displays notification that the FRAS dial backup over data-link switching plus (DLSw+) feature is active, information about the connection state in FRAS, and information about current boundary network node (BNN), boundary access node (BAN), and dial backup.

fras map llc

To associate an Logical Link Control (LLC) connection with a Frame Relay data-link connection identifier (DLCI), use the **fras map llc** command in interface configuration mode. To disable the association, use the **no** form of this command.

fras map llc *lan-lsap* **serial** *interface* **frame-relay dlci** *dlci fr-rsap*

no fras map llc *lan-lsap* **serial** *interface* **frame-relay dlci** *dlci fr-rsap*

Syntax Description

lan-lsap	Logical Link Control, type 2 (LLC2) LAN service access point (SAP) that is the local SAP address of the router.
serial *interface*	Serial interface on which Frame Relay is configured.
frame-relay dlci *dlci*	Frame Relay DLCI.
fr-rsap	LLC2 Frame Relay SAP that is the destination SAP of the router on the Frame Relay side.

Defaults

The default state is Frame Relay access support (FRAS) boundary network node (BNN) enhancement is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the destination SAP specified by the end station is equal to the *lan-lsap* value, the router associates the LLC (LAN) connection with the Frame Relay DLCI.

The MAC address and the SAP address of the end station are no longer required for the BNN enhanced configuration.

Examples

In the FRAS BNN enhancement, the revised **fras map llc** command achieves the same result as using multiple **fras map llc** commands in the original FRAS BNN implementation. The following example provides one map definition for both end stations:

```
fras map llc 4 Serial 0 frame-relay dlci 16 04
```

Related Commands

Command	Description
show fras	Displays notification that the FRAS dial backup over data-link switching plus (DLSw+) feature is active, information about the connection state in FRAS, and information about current BNN, BAN, and dial backup.
show llc2	Displays the LLC2 connections active in the router.

fras map sdlc

To associate an Synchronous Data Link Control (SDLC) link with a Frame Relay data-link connection identifier (DLCI), use the **fras map sdlc** command in interface configuration mode. To cancel the association, use the **no** form of this command.

fras map sdlc *sdlc-address* **serial** *port* **frame-relay** *dlci fr-lsap fr-rsap* [**pfid2** | **afid2** | **fid4**]

no fras map sdlc *sdlc-address* **serial** *port* **frame-relay** *dlci fr-lsap fr-rsap* [**pfid2** | **afid2** | **fid4**]

Syntax Description

sdlc-address	SDLC address of the downstream service access point (SAP) device in hexadecimal.
serial *port*	Serial interface on which Frame Relay is configured.
frame-relay *dlci*	Frame Relay DLCI.
fr-lsap	Local service access point (SAP) address of the logical link connection on the Cisco Frame Relay Access Device (CFRAD).
fr-rsap	Destination SAP address on the host.
pfid2	(Optional) format indicator 2 (FID2) Systems Network Architecture (SNA) transmission header for SNA peripheral traffic.
afid2	(Optional) FID2 transmission header for Advanced Peer-to-Peer Networking (APPN) traffic.
fid4	(Optional) Transmission header used on SNA subarea flows.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can map multiple SDLC links to a DLCI.

Examples

The following example associates an SDLC link with a Frame Relay DLCI:

```
fras map sdlc c1 serial 0 frame-relay 200 4 4
```

Related Commands

Command	Description
frame-relay map llc2	Configures block serial tunnel (BSTUN) over Frame Relay when using Bisync local acknowledgment.

fras-host ban

To enable the Frame Relay access support (FRAS) Host function for boundary access node (BAN), use the **fras-host ban** command in interface configuration mode. To disable the FRAS Host BAN functionality, use the **no** form of this command.

fras-host ban *interface* **hmac** *hmac* [**bni** *bni*]

no fras-host ban

Syntax Description

interface	Associated Frame Relay interface or subinterface.
hmac *hmac*	MAC address of the Channel Interface Processor (CIP) adapter or LAN-attached host.
bni *bni*	(Optional) Boundary node identifier MAC address. The default *bni* value is 4FFF.0000.0000.

Defaults

The FRAS Host function for BAN is disabled for the Frame Relay subinterface.

The default *bni* value is 4FFF.0000.0000.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables the FRAS Host function for BAN:

```
fras-host ban Serial0 hmac 4001.3745.0001
```

Related Commands

Command	Description
fras ban	Associates bridging over a Frame Relay network using BAN.
fras-host bnn	Enables the FRAS Host function for boundary network node (BNN).
fras-host dlsw-local-ack	Enables Logical Link Control, type 2 (LLC2) local termination for FRAS Host connections using the virtual Token Ring.
interface virtual-tokenring	Creates a virtual Token Ring interface.

fras-host bnn

To enable the Frame Relay access support (FRAS) Host function for boundary network node (BNN), use the **fras-host bnn** command in interface configuration mode. To disable the FRAS Host function, use the **no** form of this command.

fras-host bnn *interface* **fr-lsap** *sap* **vmac** *virt-mac* **hmac** *hmac* [**hsap** *hsap*]

no fras-host bnn

Syntax Description

interface	Associated Frame Relay interface or subinterface.
fr-lsap *sap*	Logical Link Control, type 2 (LLC2) service access point (SAP). The destination SAP on inbound BNN frames received from Frame Relay.
vmac *virt-mac*	Used in combination with the data-link connection identifier (DLCI) number to form a unique MAC address. The first 4 bytes of the MAC address are formed by the Virtual Media Access Control (VMAC) and the last 2 bytes are formed from the DLCI number. The last 2 bytes of the VMAC must be configured as zeros.
hmac *hmac*	MAC address of the Channel Interface Processor (CIP) adapter or LAN-attached host.
hsap *hsap*	(Optional) Host SAP. If this keyword value is not specified, the host SAP value used will match the **fr-lsap** value.

Defaults

FRAS Host for BNN is disabled for the Frame Relay subinterface.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables the FRAS Host function for BNN:

```
fras-host bnn Serial0 fr-lsap 04 vmac 4005.3003.0000 hmac 4001.3745.0001
```

Related Commands

Command	Description
fras-host ban	Enables the FRAS Host function for boundary access node (boundary access node (BAN)).
fras-host dlsw-local-ack	Enables LLC2 local termination for FRAS Host connections using the virtual Token Ring.
fras map sdlc	Associates an Synchronous Data Link Control (SDLC) link with a Frame Relay DLCI.
interface virtual-tokenring	Creates a virtual Token Ring interface.

fras-host dlsw-local-ack

To enable Logical Link Control, type 2 (LLC2) local termination for Frame Relay access support (FRAS) Host connections using the virtual Token Ring, use the **fras-host dlsw-local-ack** command in interface configuration mode. To disable LLC2 local termination, use the **no** form of this command.

fras-host dlsw-local-ack

no fras-host dlsw-local-ack

Syntax Description

This command has no arguments or keywords.

Defaults

The default state is FRAS Host LLC2 local termination disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables LLC2 local termination for FRAS Host connections using the virtual Token Ring:

```
fras-host dlsw-local-ack
```

Related Commands

Command	Description
dlsw local-peer	Defines the parameters of the data-link switching plus (DLSw+) local peer.
fras-host ban	Enables the FRAS Host function for boundary access node (BAN).
fras-host bnn	Enables the FRAS Host function for boundary network node (BNN).
interface virtual-tokenring	Creates a virtual Token Ring interface.

generic-pool

To specify whether leftover logical unit (LU)s will be made available to TN3270 sessions that do not request a specific LU or LU pool through TN3270E, use the **generic-pool** command in TN3270 server configuration mode. To selectively remove the permit or deny condition of generic pool use, use the **no** form of this command.

generic-pool {**permit** | **deny**}

no generic-pool

Syntax Description

permit	Leftover LUs should be made available to TN3270 users wanting generic sessions. This value is the default.
deny	Leftover LUs should not be given to a generic pool. The physical unit (PU) is not automatically fully populated with 255 LOCADDR definitions. The default is the value configured in TN3270 server configuration mode.

Defaults

In TN3270 server configuration mode, generic pool use is permitted.

In PU configuration mode, the default is the value configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface.

A leftover LU is defined as one for which all of the following conditions are true:

- The system services control point (SSCP) did not send an activate logical unit (ACTLU) during PU startup.
- The PU controlling the LU is capable of carrying product set ID (PSID) vectors on network management vector transport (NMVT) messages, thus allowing dynamic definition of dependent LU (DDDLU) operation for that LU.

All LUs in the generic pool are, by definition, DDDLU capable.

Values entered for the **generic-pool** in the TN3270 server configuration mode apply to all PUs for that TN3270 server but can be changed in PU configuration mode.

In PU configuration mode, a **no generic-pool** command will restore the **generic-pool** value entered in TN3270 command mode.

In TN3270 server configuration mode, the **no generic-pool** command reverts to the default, which permits generic pool use.

The command takes effect immediately. If the **generic-pool deny** command is specified on a PU, no further dynamic connections to it will be allowed. Existing sessions are unaffected, but as they terminate the LUs will not become available for dynamic connections.

Similarly, if the **generic-pool permit** command is specified, any inactive LUs are immediately available for dynamic connections. Moreover, any active LUs that were dynamic previously (before the **generic-pool deny** command was issued) return to being dynamic.

Examples

The following example permits generic LU pool use:

```
generic-pool permit
```

Related Commands

Command	Description
client ip lu	Defines a specific LU or range of LUs to a client at the IP address or subnet.

idle-time

To specify seconds of logical unit (LU) inactivity, from both host and client, before the TN3270 session is disconnected, use the **idle-time** command in TN3270 server configuration mode. To cancel the idle time period and return to the default, use the **no** form of this command.

idle-time *seconds*

no idle-time

Syntax Description

seconds	Idle time in seconds, from 0 to 65535. A value of 0 means the session is never disconnected.

Defaults

The default in TN3270 server configuration mode is that the session is never disconnected (0).

The default in PU configuration mode is the value configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **idle-time** command is valid only on the virtual channel interface, and can be entered in either TN3270 server configuration mode or PU configuration mode. A value entered in TN3270 mode applies to all PUs for that TN3270 server, except as overridden by values entered in PU configuration mode.

A **no idle-time** command entered in PU configuration mode will restore the idle-time value entered in TN3270 command mode.

The **idle-time** command affects active and future TN3270 sessions. For example, if the **idle-time** value is reduced from 900 seconds to 600 seconds, sessions that have been idle for 600 to 900 seconds are immediately disconnected.

Note For the purposes of idle-time logic, TIMING-MARKs generated by the keepalive logic do not constitute "activity."

In TN3270 server configuration mode, the **idle-time** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **idle-time** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **idle-time** command applies only to the specified PU.

In DLUR PU configuration mode, the **idle-time** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **idle-time** command applies only to the specified PU.

Examples

The following command sets an idle-time disconnect value of 10 minutes:

```
idle-time 600
```

The following command entered in TN3270 server configuration mode sets the default idle-time disconnect value to 0, or never disconnect:

```
no idle-time
```

Related Commands

Command	Description
keepalive (TN3270)	Specifies how many seconds of inactivity elapse before transmission of a DO TIMING-MARK or Telnet no operation (nop) to the TN3270 client.
timing-mark	Selects whether a WILL TIMING-MARK is sent when the host application needs an SNA response (definite or pacing response).

interface bvi

To create the bridge-group virtual interface (BVI) that represents the specified bridge group to the routed interface and links the corresponding bridge group to the other routed interfaces, use the **interface bvi** command in global configuration mode. To delete the BVI, use the **no** form of this command.

interface bvi *bridge-group*

no interface bvi *bridge-group*

Syntax Description

bridge-group	Bridge-group number specified in the **bridge protocol** command.

Command Default

No BVI is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for the *sub slot interface* argument was removed for dynamic interfaces.

Usage Guidelines

You must enable integrated routing and bridging (IRB) before attempting to create a BVI.

When you intend to bridge and route a given protocol in the same bridge group, you must configure the network-layer attributes of the protocol on the BVI. Do not configure protocol attributes on the bridged interfaces. Bridging attributes cannot be configured on the BVI.

Examples

The following example creates a bridge group virtual interface and associates it with bridge group 1:

```
Router(config)# bridge 1 protocol ibm
Router(config)# bridge irb
Router(config)# interface bvi 1
Router(config-if)#
```

Related Commands

Command	Description
bridge irb	Enables Cisco IOS software to route a given protocol between routed interfaces and bridge groups or to route a given protocol between bridge groups.

interface channel

To specify a channel-attached interface and enter interface configuration mode, use the **interface channel** command in global configuration mode.

interface channel *slot*/*port*

Syntax Description

slot	Slot number where the Cisco Mainframe Channel Connection (CMCC) adapter is located. The slash mark is required.
port	Interface where the CMCC adapter is located.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enter interface configuration mode for a CIP in slot 2 and begin configuring port 0:

```
interface channel 2/0
```

Related Commands

Command	Description
channel-protocol	Defines a data rate of either 3 MBps or 4.5 MBps for Parallel Channel Interfaces.
claw (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
cmpc	Configures a Cisco Multipath Channel (CMPC or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
csna	Configures Systems Network Architecture (SNA) support on a CMCC physical channel interface and specifies the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe.

Command	Description
keylen	Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode.
maximum-lus	Specifies the maximum number of LLC2 sessions supported on the CMCC adapter.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.
tg (CMPC)	Defines LLC connection parameters for the CMPC TG.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

interface virtual-tokenring

To create a virtual Token Ring interface, use the **interface virtual-tokenring** command in global configuration mode. To cancel the configuration, use the **no** form of this command.

interface virtual-tokenring *number*

no interface virtual-tokenring

Syntax Description

number	Number of the virtual Token Ring.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the virtual Token Ring interface:

```
interface virtual-tokenring 0
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.
fras ban	Associates bridging over a Frame Relay network using boundary access node (BAN).
fras-host bnn	Enables the FRAS Host function for boundary network node (BNN).

interface vlan

To create a dynamic Switch Virtual Interface (SVI) or configure a Route Switch Module (RSM), use the **interface vlan** command in global configuration mode.

Configuring on an RSM

To configure a Token Ring or Ethernet interface on the RSM, use the **interface vlan** command in global configuration mode.

interface vlan *vlanid* **type** {**trbrf** | **ethernet**}

Creating a Dynamic Switch Virtual Interface

To create or access a dynamic SVI, use the **interface vlan** command in global configuration mode. Use the **no** form of this command to delete an SVI.

interface vlan *vlanid*

no interface vlan *vlanid*

Syntax Description

vlanid	Unique VLAN ID number (1 to 4094) used to create or access a VLAN.
type trbrf	Configures a Token Ring interface on the RSM.
type ethernet	Configures an Ethernet interface on the RSM.

Defaults

Configuring on an RSM

RSM interfaces are not configured.

Creating a Dynamic Switch Virtual Interface

Fast EtherChannel is not specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3(5)T	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to create Layer 2 VLANs when you create an SVI.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Configuring on an RSM

Valid Token Ring VLAN ID numbers are 2 through 1000.

Routing or bridging to a Token Ring VLAN (TrBRF) on the RSM is done by creating a logical interface to a TrBRF VLAN on the RSM with the **interface vlan** command. The TrBRF VLAN must be defined on the Supervisor module prior to creating the TrBRF interface on the RSM.

Creating a Dynamic Switch Virtual Interface

SVIs are created the first time that you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* value corresponds to the VLAN tag that is associated with the data frames on an Inter-Switch Link (ISL), the 802.1Q-encapsulated trunk, or the VLAN ID that is configured for an access port. A message displays whenever you create a new VLAN interface, so that you can check if you entered the correct VLAN number.

If you delete an SVI by entering the **no interface vlan** *vlan-id* command, the associated initial domain part (IDP) pair is forced into an administrative down state and is marked as deleted. The deleted interface will not be visible in the **show interface** command.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but much of the previous configuration is gone.

VLANs 1006 to 1014 are internal VLANs on the Cisco 7600 series router and cannot be used for creating new VLANs.

Examples

Configuring on an RSM

The following example show how to configure an RSM Token Ring interface with VLAN 998:

```
Router(config)# interface vlan 998 type trbrf
 ip address 10.5.5.1 255.255.255.0
```

Creating a Dynamic Switch Virtual Interface

The following example shows the output when you enter the **interface vlan** *vlan-id* command for a new VLAN number:

```
Router(config)# interface vlan 23
% Creating new VLAN interface.
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
show drip	Displays the status of the DRiP database.

ip precedence (TN3270)

To specify the precedence level for voice over IP traffic in the TN3270 server, use the **ip precedence** command in TN3270 server configuration mode. To remove the precedence value, use the **no** form of this command.

ip precedence {**screen** | **printer**} *value*

no ip precedence {**screen** | **printer**}

Syntax Description

screen	Specifies that the precedence is for screen devices.
printer	Specifies that the precedence is for printer devices.
value	Sets the precedence priority. A value from 0 to 7, with 7 being the highest priority. The default is 0.

Defaults

The default is a precedence value of 0 for both screens and printers.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. Precedence values applied in TN3270 PU configuration mode override values applied in TN3270 server configuration mode.

You can enter new or different values for IP precedence without first using the **no** form of this command.

During initial Telnet negotiations to establish, or bind, the session an IP precedence value of 0 and IP ToS value of 0 is used. These values are used until the bind takes place. When the session is a type 2 bind, the TN3270 client is assumed to be a screen; otherwise the client is assumed to be a printer.

In TN3270 server configuration mode, the **ip precedence** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **ip precedence** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **ip precedence** command applies only to the specified PU.

In DLUR PU configuration mode, the **ip precedence** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **ip precedence** command applies only to the specified PU.

Examples

The following example assigns a precedence value of 3 to printers:

```
ip precedence printer 3
```

Related Commands

Command	Description
ip tos	Specifies the ToS level for IP traffic in the TN3270 server.

ip tos

To specify the type of service (ToS) level for IP traffic in the TN3270 server, use the **ip tos** command in TN3270 server configuration mode. To remove the ToS value, use the **no** form of this command.

ip tos {**screen** | **printer**} *value*

no ip tos {**screen** | **printer**}

Syntax Description

screen	Specifies that the ToS is for screen devices.
printer	Specifies that the ToS is for printer devices.
value	Sets the ToS priority. A value from 0 to 15. The default is 0.

Defaults

The default is a ToS value of 0 for both screens and printers.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. ToS values applied in TN3270 PU configuration mode override values applied in TN3270 server configuration mode.

The default ToS values for screen and printer are 0. However, RFC 1349 recommends different default values. Specifically, the RFC recommends a default minimize screen delay value of 8 and a default maximize printer throughput value of 4. You must configure these values using the **ip tos** command if you want to comply to the defaults as stated in the RFC.

Table 13 shows the values described in RFC 1349.

Table 13 ToS Defined Values

Value	Definition	Action
0	All normal.	Use default metric.
8	Minimize delay.	Use delay metric.
4	Maximize throughput.	Use default metric.
2	Maximize reliability.	Use reliability metric.
1	Minimize monetary cost.	Use cost metric.
Other	Not defined.	Reserved for future use.

During initial Telnet negotiations to establish, or bind, the session, an IP precedence value of 0 and IP ToS value of 0 is used. These values are used until the bind takes place. When the session is a type 2 bind, the TN3270 client is assumed to be a screen; otherwise the client is assumed to be a printer.

When you use the **no** form of the command, the ToS value is set to 0 for that configuration mode or the value set at a previous (higher) configuration mode is used. For example, if you are at the TN3270 PU configuration mode and issue a **no ip tos screen** command, any value you configured previously at the TN3270 server configuration mode will take effect.

You can enter new or different values for ToS without first using the **no** form of this command.

In TN3270 server configuration mode, the **ip tos** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **ip tos** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **ip tos** command applies only to the specified PU.

In DLUR PU configuration mode, the **ip tos** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **ip tos** command applies only to the specified PU.

Examples

In the following example, the TN3270 server ToS screen value is set to 10 and a specific PU ToS screen value is set to 0:

```
interface channel 3/2
  tn3270-server
   ip tos screen 8
   ip tos printer 4
  up PUS2
   ip tos screen 0
```

Related Commands

Command	Description
ip precedence (TN3270)	Specifies the precedence level for IP traffic in the TN3270 server.

keepalive (TN3270)

To specify how many seconds of inactivity elapse before the TN3270 server sends a DO TIMING-MARK or Telnet no operation (nop) to the TN3270 client, use the **keepalive** command in TN3270 server configuration mode. To cancel the keepalive period and return to the previously configured siftdown value or the default, use the **no** form of this command.

keepalive *seconds* [**send** {**nop** | **timing-mark** [*max-response-time*]}]

no keepalive

Syntax Description

seconds	Number of elapsed seconds (from 0 to 65535) before the TN3270 server sends a DO TIMING-MARK or Telnet **nop** command to the TN3270 client. A value of 0 means no keepalive signals are sent. The default is 1800 seconds (30 minutes).
send nop	(Optional) Sends the Telnet command for no operation to the TN3270 client to verify the physical connection. No response is required by the client.
send timing-mark [*max-response-time*]	(Optional) Number of seconds (from 0 to 32767) within which the TN3270 server expects a response to the DO TIMING-MARK from the TN3270 client. The default is 30 seconds if the keepalive interval is greater than or equal to 30 seconds. If the value of the keepalive interval is less than 30 seconds, then the default *max-response-time* value is the value of the interval. The value of the *max-response-time* should be less than or equal to the *interval* value.

Defaults

The default behavior is to send timing marks with a keepalive interval of 1800 seconds (30 minutes). If you specify only the keepalive interval, the TN3270 server sends timing marks.

The default value of the **send timing-mark** *max-response-time* command is 30 seconds if the keepalive interval is greater than or equal to 30 seconds. If the value of the keepalive interval is less than 30 seconds, then the default *max-response-time* value is the value of the interval.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The **send** {**nop** | **timing-mark** [*max-response-time*]} keywords and argument were added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **keepalive** command is valid only on the virtual channel interface. This command can be entered in one of four command modes (TN3270 configuration, listen-point configuration, listen-point PU configuration, or PU configuration mode). A value entered in TN3270 mode applies to all PUs for that TN3270 server, except as overridden by values entered in the other supported configuration modes. A **no keepalive** command entered in a subsequent configuration mode will restore the **keepalive** value entered in the previous command mode.

In Cisco IOS releases prior to 12.0(5)T in which the **keepalive** command is supported, you cannot specify the period of time in which the client must respond to the DO TIMING-MARK before the TN3270 server disconnects the session. By default in prior releases, if the client does not reply within 30 minutes of sending the DO TIMING-MARK, the TN3270 server disconnects the TN3270 session. (The DO TIMING-MARK is a Telnet protocol operation that does not affect the client operation.)

With the addition of the **send timing-mark** *max-response-time* keywords in Cisco IOS Release 12.0(5)T, you can specify the period of time in which the client must respond to the DO TIMING-MARK before being disconnected by the server. If you do not specify a value for the *max-response-time* argument, the default value is determined by the size of the keepalive interval. The default is 30 seconds if the keepalive interval is greater than or equal to 30 seconds. If the value of the keepalive interval is less than 30 seconds, then the default *max-response-time* is the value of the interval.

If the IP path to the client is broken, the TCP layer will detect the failure to acknowledge the DO TIMING-MARK and initiate disconnection. This action usually takes much less than 30 seconds.

The **keepalive** command affects active and future TN3270 sessions. For example, reducing the keepalive interval to a lower nonzero value causes an immediate burst of DO TIMING-MARKs on those sessions that have been inactive for a period of time greater than the new, lower value.

Use the **keepalive send nop** command when you are using older TN3270 clients that do not support TIMING-MARK or are DOS-based clients. When you use the **keepalive send nop** command to monitor the client connection, no response is required by the client to the TN3270 server. However, the TCP/IP stack can detect that the physical connection still exists. This command is useful for those clients that can be swapped out when a DO TIMING-MARK has been sent by the TN3270 server. If the client is swapped out and cannot respond to the DO TIMING-MARK from the TN3270 server, the session is disconnected. However, if the client is swapped out and the Telnet **nop** command is sent by the server, the physical connection is still verifiable by the TCP/IP stack and the client remains connected to the server.

If your client supports the use of timing marks and is not subject to being swapped out, then using timing marks is preferable to the Telnet **nop** command for keepalive monitoring. The required response by TN3270 clients to timing marks sent by the server provides a better indication of the health of the client/server connection.

In TN3270 server configuration mode, the **keepalive** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **keepalive** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **keepalive** command applies only to the specified PU.

In DLUR PU configuration mode, the **keepalive** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **keepalive** command applies only to the specified PU.

Examples

The following example specifies that the TN3270 server sends a DO TIMING-MARK in 15-minute (900-second) intervals and the client must respond within 30 seconds (the default value for the **timing-mark** *max-response-time* command when not specified):

```
keepalive 900
```

The following example entered in TN3270 server configuration mode specifies that the TN3270 server sends a DO TIMING-MARK in 30-minute (1800-second) intervals (the default interval) and the client must respond within 30 seconds (the default for the **timing-mark** *max-response-time* command when not specified):

```
no keepalive
```

The following example specifies that the TN3270 server sends a DO TIMING-MARK in 40-minute (2400-second) intervals and the client must respond within 1 minute (60 seconds):

```
keepalive 2400 send timing-mark 60
```

Consider the following example in which the **keepalive** command is configured in more than one command mode. In this example the **keepalive** command is configured in TN3270 server configuration mode, and then in listen-point physical unit (PU) configuration mode. The **keepalive** command values specified under the listen-point PU override the **keepalive** 300 value specified under the tn3270-server for PU1. In this example, all other PUs except PU1 use the value of the **keepalive 300** command specified in TN3270 server configuration mode.

```
tn3270-server
keepalive 300
listen-point 10.10.10.1 tcp-port 40
  pu PU1 94223456 tok 1 08
    keepalive 10 send timing-mark 5
  pu PU2 94223457 tok 2 12
```

Related Commands

Command	Description
idle-time	Specifies how many seconds of LU inactivity, from both host and client, before the TN3270 session is disconnected.
timing-mark	Selects whether a WILL TIMING-MARK is sent when the host application needs an SNA response (definite or pacing response).

keylen

To specify the maximum bit length for the encryption keys for Secure Socket Layer (SSL) Encryption Support, use the **keylen 128** command in profile configuration mode. To disable this specification and thereby set the key length to the default of 40 bits, use the **no** form of this command or **keylen 40**.

keylen {**40** | **128**}

no keylen [**40** | **128**]

Syntax Description

40	Specifies the bit length for the encryption keys to 40.
128	Specifies the bit length for the encryption keys to 128. The default is 40 bits.

Defaults

The default encryption key length is 40 bits.

Command Modes

Profile configuration.

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Exportable software versions cannot accept encryption key lengths greater than 40 bits.

The length is optional on the **no** form of this command. Entering the **no** form of this command with no length resets the length to the default value of 40 bits.

If the key length is changed, all new connections will use the new value. If an active session renegotiates its security specifications, it will use the new key length value.

Examples

The following example specifies the maximum encryption key length value to 128 bits:

```
tn3270-server
 security
 profile DOMESTIC SSL
  encryptorder RC4 DES RC2
  keylen 128
```

lan

To configure an internal LAN on a Cisco Mainframe Channel Connection (CMCC) adapter interface and enter internal LAN configuration mode, use the **lan** command in interface configuration mode. To remove an internal LAN interface, use the **no** form of this command.

lan *type lan-id*

no lan *type lan-id*

Syntax Description

type	Interface type for this internal LAN: **tokenring**.
lan-id	Number from 0 to 31 that uniquely identifies the internal LAN on this CMCC adapter. This value must be unique between all internal LANs of the same interface type on a CMCC adapter.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Token Ring is the only type of internal LAN supported.

This command is valid only on the virtual channel interface. All internal adapters configured on the internal LAN must be removed before the internal LAN can be removed.

A CMCC internal LAN can be configured as a SRB LAN. This allows Logical Link Control (LLC) packets to be bridged between the CMCC adapter and Cisco IOS, providing a means to link the internal LAN to Cisco IOS Systems Network Architecture (SNA) features such as source-route bridging (SRB), data-link switching plus (DLSw+), remote source-route bridging (RSRB), SDLC Logical Link Control (SDLLC), Qualified Logical Link Control (QLLC), Advanced Peer-to-Peer Networking (APPN), and source-route translational bridging (SR/TLB).

An internal LAN can be configured only on a virtual channel interface of a CMCC adapter. You enter first internal LAN configuration mode by issuing the command for an internal LAN that already exists or when you first configure an internal LAN. In internal LAN configuration mode, the router prompt appears as follows:

```
router (cfg-lan-type x) #
```

In this syntax, *type* is the specified internal LAN type and *x* is the specified value for the *lan-id*.

Examples

The following example shows how to configure an internal LAN Token Ring with a LAN ID of 20 on the channel interface 1/2:

```
interface channel 1/2
 lan tokenring 20
```

Related Commands

Command	Description
adapter	Configures internal adapters.
locaddr-priority	Assigns an RSRB priority group to an input interface.
sap-priority	Defines a priority list on an interface.
show extended channel lan	Displays the internal LANs and adapters configured on a CMCC adapter.
source-bridge	Configures an interface for SRB.

lan-name

To specify a name for the LAN that is attached to the interface, use the **lan-name** command in interface configuration mode. This name is included in any Alert sent to the Systems Network Architecture (SNA) host when a problem occurs on this interface or LAN. To revert to the default name, use the **no** form of this command.

lan-name *lan-name*

no lan-name *lan-name*

Syntax Description

lan-name	Name used to identify the LAN when you send Alerts to the SNA host. The default LAN name is the name of the interface.

Defaults

The default name used for the LAN is the name of the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example identifies a LAN:

```
lan-name LAN1
```

Related Commands

Command	Description
show sna	Displays the status of the SNA Service Point feature.

link (TN3270)

To define and activate a link to a host, use the **link** command in Dependent Logical Unit Requestor (DLUR) service access point (SAP) configuration mode. To delete the link definition, use the **no** form of this command.

link *name* [**rmac** *rmac*] [**rsap** *rsap*]

no link *name*

Syntax Description

name	Link name, from one to eight alphanumeric characters. The first character must be alphabetic. The name must be unique within the Dependent Logical Unit Requestor (DLUR) function.
rmac *rmac*	(Optional) Remote MAC address of the form *xxxx.xxxx.xxxx* in hexadecimal. If not specified, a loopback link to another service access point (SAP) on the same internal LAN adapter is assumed.
rsap *rsap*	(Optional) Remote SAP address, 04 to FC in hexadecimal. The *rsap* value should be an even number and should be a multiple of 4, but the latter requirement is not enforced. The default value for the *rsap* argument is 04.

Defaults

No DLUR link is defined.
The default remote SAP address is 04 (hexadecimal).

Command Modes

DLUR SAP configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. The combination of the *rmac* and *rsap* value must be unique within the DLUR SAP function. These values can be changed only by deleting the link definition, using the **no link** command, and recreating the link definition.

For a link via a channel on this Cisco Mainframe Channel Connection (CMCC) adapter, the TN3270 server and the hosts should open different adapters. Using different adapters avoids any contention for SAP numbers, and is also necessary if you configure duplicate MAC addresses for fallback Cisco Systems Network Architecture (CSNA) or Cisco Multipath Channel (CMPC) access to the host.

Examples

The following example defines a link name and a remote SAP address:

```
link LINK5 rsap 08
```

The following example shows different adapter numbers configured on the same internal LAN to avoid SAP contention. The host uses SAP 4 on Token Ring adapter 0.

```
lan tokenring 0
 adapter 0 4000.0000.0001
 adapter 1 4000.0000.0002
tn3270-server
 dlur ...
 lsap token-adapter 1
  link HOST rmac 4000.0000.0001 rsap 4
```

Related Commands

Command	Description
adapter	Configures internal adapters.
client pool	Nails clients to pools.
lsap	Creates a SAP in the SNA session switch and enters DLUR SAP configuration mode.

listen-point

To define an IP address for the TN3270 server, use the **listen-point** command in TN3270 server configuration mode. To remove a listen-point for the TN3270 server, use the **no** form of this command.

listen-point *ip-address* [**tcp-port** *number*]

no listen-point *ip-address* [**tcp-port** *number*]

Syntax Description

ip-address	IP address that the clients should use as the host IP address to map to logical unit (LU) sessions under this physical unit (PU) and listen point.
tcp-port *number*	(Optional) Port number used for the listen operation. The default value is 23.

Defaults

The default **tcp-port** *number* is 23.

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **listen-point** command to create a unique listen point for every IP address and TCP-port pair. In this mode, the IP address and the TCP port are no longer configured in the PU. Configure the PUs under the appropriate listen point. The other siftdown configuration commands remain the same.

For example, in the old configuration the following statements were used to configure the IP address and TCP port in the PU:

```
tn3270-server
  pu PU1 94223456 10.10.10.1 tok 1 08
   tcp-port 40
   keepalive 10
```

In the new listen-point configuration, the following statements are used to configure the IP address and TCP port at the listen point:

```
tn3270-server
  listen-point 10.10.10.1 tcp-port 40
   pu PU1 94223456 tok 1 08
    keepalive 10
```

You can also use the listen-point configuration to assign the same IP address to multiple PUs. In the old configuration the following statements were used:

```
tn3270-server
  pu PU1 94201231 10.10.10.2 tok 1 10
  pu PU2 94201232 10.10.10.3 tok 1 12
  pu PU3 94201234 10.10.10.3 tok 1 14
  pu PU4 94201235 10.10.10.4 tok 1 16
   tcp-port 40
  pu PU5 94201236 10.10.10.4 tok 2 08
```

In the new listen point configuration, the old statements are replaced by the following configuration commands. In this example, PU2 and PU3 are grouped into one listen point because they have the same IP address. Note that even though PU4's IP address is identical to PU5's IP address, they are not configured within the same listen point because the listen point indicates a unique IP address and TCP port pair. If you do not specify the TCP port, the default port value is 23.

```
tn3270-server
 listen-point 10.10.10.2
  pu PU1 94201231 tok 1 10
 listen-point 10.10.10.3
  pu PU2 94201232 tok 1 12
  pu PU3 94201234 tok 1 14
 listen-point 10.10.10.4
  pu PU5 94201236 tok 2 08
 listen-point 10.10.10.4 tcp-port 40
  pu PU4 94201235 tok 1 16
```

The next example shows how the configuration changes for a Dependent Logical Unit Requestor (DLUR) PU. In this mode, the DLUR PU is no longer configured under DLUR, but is configured in the listen point.

In the old configuration, the following statements were used:

```
tn3270-server
 dlur NETA.RTR1 NETA.HOST
  dlus-backup NETA.HOST
  lsap token-adapter 15 08
   link MVS2TN rmac 4000.b0ca.0016
  pu PU1 017ABCDE 10.10.10.6
```

These statements are replaced by the following statements in the new listen-point configuration. The keyword **dlur** differentiates the listen point direct PU from the listen point DLUR PU. The DLUR configuration must be completed before you configure the PU in the listen point. Any siftdown commands configured within the scope of the listen point are automatically inherited by the PUs that are configured within the scope of that listen point. To override the siftdown configurations, you can explicitly configure the siftdown configuration commands within the scope of the listen-point PU.

```
tn3270-server
 dlur NETA.RTR1 NETA.HOST
  dlus-backup NETA.HOST
  lsap token-adapter 15 08
   link MVS2TN rmac 4000.b0ca.0016
 listen-point 10.10.10.6
  pu PU1 017ABCDE dlur
```

Examples

The following example of the **listen-point** command shows PU7 grouped into the listen point at IP address 10.10.10.1 and TCP port 40:

```
tn3270-server
listen-point 10.10.10.1 tcp-port 40
 pu PU7 94201237 tok 1 17
```

Related Commands

Command	Description
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.

llc2 ack-delay-time

To set the amount of time the Cisco IOS software waits for an acknowledgment before sending the next set of information frames, use the **llc2 ack-delay-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 ack-delay-time *milliseconds*

no llc2 ack-delay-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software allows incoming information frames to stay unacknowledged. The minimum is 1 ms and the maximum is 60000 ms. The default is 100 ms.

Defaults

100 ms

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Upon receiving an information frame, each Logical Link Control, type 2 (LLC2) station starts a timer. If the timer expires, an acknowledgment will be sent for the frame, even if the number of received frames in the **llc2 ack-max** command has not been reached. Experiment with the value of the **llc2 ack-delay-time** command to determine the configuration that balances acknowledgment network overhead and quick response time (by receipt of timely acknowledgments).

Use this command in conjunction with the **llc2 ack-max** command to determine the maximum number of information frames the Cisco IOS software can receive before sending an acknowledgment.

Examples

In the following example, the software allows a 100-ms delay before I-frames must be acknowledged:

```
! enter a global command, if you have not already
interface tokenring 0
! sample ack-max command
 llc2 ack-max 3
! allow a 100 millisecond delay before I-frames must be acknowledged
 llc2 ack-delay-time 100
```

At time 0, two information frames are received. The **llc2 ack-max** amount of three has not been reached, so no acknowledgment for these frames is sent. If a third frame, which would force the software to send an acknowledgment, is not received in 100 ms, an acknowledgment will be sent anyway, because the l**lc2 ack-delay** timer expires. At this point, because all frames are acknowledged, the counter for the ack-max purposes will be reset to zero.

Related Commands

Command	Description
llc2 ack-max	Controls the maximum amount of information frames the Cisco IOS software can receive before it must send an acknowledgment.
show llc2	Displays the LLC2 connections active in the router.

llc2 ack-max

To control the maximum amount of information frames the Cisco IOS software can receive before it must send an acknowledgment, use the **llc2 ack-max** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 ack-max *packet-count*

no llc2 ack-max *packet-count*

Syntax Description

packet-count	Maximum number of packets the software will receive before sending an acknowledgment. The minimum is 1 packet and the maximum is 127 packets. The default is 3 packets.

Defaults

Three packets

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An Logical Link Control, type 2 (LLC2)-speaking station can send only a predetermined number of frames before it must wait for an acknowledgment from the receiver. If the receiver waits until receiving a large number of frames before acknowledging any of them, and then acknowledges them all at once, overhead is reduced on the network.

For example, an acknowledgment for five frames can specify that all five have been received, as opposed to sending a separate acknowledgment for each frame. To keep network overhead low, make this parameter as large as possible.

However, some LLC2-speaking stations expect this number to be low. Some NetBIOS-speaking stations expect an acknowledgment to every frame. Therefore, for these stations, this number is best set to 1. Experiment with this parameter to determine the best configuration.

Examples

In the following example, the software is configured to receive up to seven frames before it must send an acknowledgment. Seven frames is the maximum allowed by Systems Network Architecture (SNA) before a reply must be received:

```
! enter a global command, if you have not already
interface tokenring 0
! receive up to seven frames before sending an acknowledgment
```

```
 llc2 ack-max 7
! sample delay-time command
 llc2 ack-delay-time 100
```

Related Commands

Command	Description
llc2 ack-delay-time	Sets the amount of time the Cisco IOS software waits for an acknowledgment before sending the next set of information frames.
llc2 local-window	Controls the maximum number of information frames the Cisco IOS software sends before it waits for an acknowledgment.
show llc2	Displays the LLC2 connections active in the router.

llc2 adm-timer-value

To control the amount of time the Cisco IOS software waits for, in Asynchronous Disconnect Mode (ADM) before giving up, use the **llc2 adm-timer-value** command in interface configuration mode. To restore the default configuration, use the **no** form of this command.

llc2 adm-timer-value *milliseconds*

no llc2 adm-timer-value *milliseconds*

Syntax Description

milliseconds	Time period in milliseconds (ms) the software waits for in ADM. The range is from 0 to 60000 ms. The default is 60000 ms.

Command Default

The default is 60000 ms.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on the feature set, platform, and hardware.

Usage Guidelines

The command **llc2 adm-timer-value** command is used to clear out the Logical Link Control (LLC) sessions that are left in the ADM State for a defined time period, so that the router does not hang.

Examples

This example shows how to control the waiting time with the **llc2 adm-timer-value** command:

```
Router (config-if)# llc2 adm-timer-value 3
```

Related Commands

Command	Description
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.
llc2 xid-neg-val-time	Controls the frequency of XID transmissions by the Cisco IOS software.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 dynwind

To enable dynamic window congestion management, use the **llc2 dynwind** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

llc2 dynwind [**nw** *nw-number*] [**dwc** *dwc-number*]

no llc2 dynwind [**nw** *nw-number*] [**dwc** *dwc-number*]

Syntax Description

nw *nw-number*	(Optional) Specifies a number of frames that must be received to increment the working window value by 1. The default is 4.
dwc *dwc-number*	(Optional) Specifies the number by which the working window value is divided when Systems Network Architecture (SNA) occurs. Valid numbers are 1, 2, 4, 8, and 16; 1 is a special value that indicates that the working window value should be set to 1 when backward explicit congestion notification (BECN) is indicated. The default is 1.

Defaults

The default *nw-number* value is 4.
The default *dwc-number* value is 1.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that to increment the working window six frames must be received, and the working window value should be set to 1 when BECN occurs:

```
llc2 dynwind nw 6 dwc 1
```

llc2 idle-time

To control the frequency of polls during periods of idle time (no traffic), use the **llc2 idle-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 idle-time *milliseconds*

no llc2 idle-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds that can pass with no traffic before the Logical Link Control, type 2 (LLC2) station sends a Receiver Ready frame. The minimum is 1 ms and the maximum is 60000 ms. The default is 10000 ms.

Defaults

10000 ms

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Periodically, when no information frames are being sent during an LLC2 session, LLC2 stations are sent a Receiver Ready frame to indicate that they are available. Set the value for this command low enough to ensure a timely discovery of available stations, but not too low, or you will create a network overhead with too many Receiver Ready frames.

Examples

In the following example, the Cisco IOS software waits 20,000 ms before sending a Receiver Ready (“are you there”) frame:

```
! enter a global command, if you have not already
interface tokenring 0
! wait 20000 milliseconds before sending receiver-ready frames
 llc2 idle-time 20000
```

Related Commands

Command	Description
llc2 tbusy-time	Controls the amount of time the Cisco IOS software waits until repolling a busy remote station.
llc2 tpf-time	Sets the amount of time the Cisco IOS software waits for a final response to a poll frame before resending the poll frame.
show llc2	Displays the LLC2 connections active in the router.

llc2 local-window

To control the maximum number of information frames the Cisco IOS software sends before it waits for an acknowledgment, use the **llc2 local-window** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 local-window *packet-count*

no llc2 local-window *packet-count*

Syntax Description

packet-count	Maximum number of packets that can be sent before the software must wait for an acknowledgment. The minimum is 1 packet and the maximum is 127 packets. The default is 7 packets.

Defaults

Seven packets.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An Logical Link Control, type 2 (LLC2)-speaking station can send only a predetermined number of frames before it must wait for an acknowledgment from the receiver. Set this number to the maximum value that can be supported by the stations with which the router communicates. Setting this value too large can cause frames to be lost, because the receiving station may not be able to receive all of them.

Examples

In the following example, the software will send as many as 30 information frames through Token Ring interface 1 before it must receive an acknowledgment:

```
! enter a global command, if you have not already
interface tokenring 1
 llc2 local-window 30
```

Related Commands

Command	Description
llc2 ack-max	Controls the maximum amount of information frames the Cisco IOS software can receive before it must send an acknowledgment.
show llc2	Displays the LLC2 connections active in the router.

llc2 n1

To specify the maximum size of an I-frame, use the **llc2 n1** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 n1 *bytes*

no llc2 n1

Syntax Description

bytes	Maximum size of an I-frame. The valid range is from 1 to 4105 bytes. The default is 4105 bytes.

Defaults

The default maximum I-frame size is 4105 bytes.

Command Modes

Internal adapter configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the maximum I-frame size to 2057 bytes:

```
! enter a global command, if you have not already
interface tokenring 1
! maximum I-frame size of 2057 bytes
 llc2 n1 2057
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 n2

To control the amount of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations, use the **llc2 n2** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 n2 *retry-count*

no llc2 n2

Syntax Description

retry-count	Number of times the software retries operations. The minimum is 1 retry and the maximum is 255 retries. The default is 8 retries.

Defaults

Eight retries

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An Logical Link Control, type 2 (LLC2) station must have some limit to the number of times it will resend a frame when the receiver of that frame has not acknowledged it. After the software is told that a remote station is busy, it will poll again based on the *retry-count* value. When this retry count is exceeded, the LLC2 station terminates its session with the other station. Set this parameter to a value that balances between frame checking and network performance.

Examples

In the following example, the software will resend a frame up to four times through Token Ring interface 1 before it must receive an acknowledgment. Because you generally do not need to change the retry limit, this example shows you how to reset the limit to the default of 8.

```
! enter a global command, if you have not already
interface tokenring 1
! retry value of 8
 llc2 n2 8
```

Related Commands

Command	Description
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.
llc2 tbusy-time	Controls the amount of time the Cisco IOS software waits until repolling a busy remote station.
llc2 trej-time	Controls the amount of time the Cisco IOS software waits for a correct frame after sending a reject command to the remote LLC2 station.
show llc2	Displays the LLC2 connections active in the router.

llc2 nw

To increase the window size for consecutive good I-frames received, use the **llc2 nw** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

llc2 nw *window-size-increase*

no llc2 nw

Syntax Description

window-size-increase	Number of frames to increase the window size for consecutive good I-frames received (0 is disabled). The allowed range is from 1 to 7. The default is 0.

Defaults

0 (disabled).

Command Modes

Internal adapter configuration

Command History

Release	Modification
11.0	This command was introduced.
12.1	The allowed range was changed to from 0 to 31.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the window size for Token Ring interface 1 is increased by 1 frame when consecutive good I-frames are received:

```
! enter a global command, if you have not already
interface tokenring 1
! increase window size by 1
 llc2 nw 1
```

Related Commands

Command	Description
show llc2	Displays the LLC2 connections active in the router.
llc2 nw	Invokes dynamic windowing logic for a link station when the router receives an RNR from the remote link station.

llc2 recv-window

To control the number of frames in the receive window, use the **llc2 recv-window** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 recv-window *frame-count*

no llc2 recv-window

Syntax Description

frame-count	Specifies the number of frames in the receive window. The default is 7.

Defaults

Seven frames.

Command Modes

Internal adapter configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the receive window for Token Ring interface 1 contains 11 frames:

```
! enter a global command, if you have not already
interface tokenring 1
! 11 frames in the receive window
 llc2 recv-window 11
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 rnr-activated

To invoke dynamic windowing logic for a link station when the router receives an RNR from the remote link station, use the **llc2 rnr-activated** internal adapter configuration command. To disable dynamic windowing logic, use the **no** form of this command.

llc2 rnr-activated

no llc2 rnr-activated

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Internal adapter configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **llc2 nw** command must be enabled before the **llc2 rnr-activated** command can be configured.

Examples

In the following example, the **llc2n rnr-activated** command is enabled on Adapter 0 4000.cafe.0000:

```
interface Channel4/2
 max-llc2-rcvbuffs 750
lan TokenRing 12
 source-bridge 16 1 500
 adapter 0 4000.cafe.0000
  llc2 Nw 31
  llc2 rnr-activated
 adapter 1 4000.cafe.0001
```

Related Commands

Command	Description
llc2 nw	Increases the window size for consecutive good I-frames received.
max-llc2-rcvbuffs	Configures the number of receive DMA buffers that are used by the LLC2 stack on the CIP/XCPA.

llc2 send-window

To control the number of frames in the send window, use the **llc2 send-window** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 send-window *frame-count*

no llc2 send-window

Syntax Description

frame-count	Specifies the number of frames in the send window. The default is 7.

Defaults

Seven frames.

Command Modes

Internal adapter configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the send window for Token Ring interface 1 contains 11 frames:

```
! enter a global command, if you have not already
interface tokenring 1
! 11 frames in the send window
 llc2 send-window 11
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 t1-time

To control the amount of time the Cisco IOS software will wait before resending unacknowledged information frames, use the **llc2 t1-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 t1-time *milliseconds*

no llc2 t1-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software waits before resending unacknowledged information frames. The minimum is 1 ms and the maximum is 60000 ms. The default is 1000 ms.

Defaults

1000 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in conjunction with the **llc2 n2** command to provide a balance of network monitoring and performance. Ensure that enough time is allowed to account for the round trip between the router and its Logical Link Control, type 2 (LLC2)-speaking stations under heavy network loading conditions.

Examples

In the following example, the software will wait 4000 ms before resending an unacknowledged frame through Token Ring interface 2:

```
! enter a global command, if you have not already
interface tokenring 2
! wait 4000 milliseconds before retransmitting a frame through tokenring 2
 llc2 t1-time 4000
```

Related Commands

Command	Description
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
llc2 tpf-time	Sets the amount of time the Cisco IOS software waits for a final response to a poll frame before resending the poll frame.
llc2 xid-retry-time	Sets the amount of time the Cisco IOS software waits for a reply to XID frames before dropping the session.
show llc2	Displays the LLC2 connections active in the router.

llc2 tbusy-time

To control the amount of time the Cisco IOS software waits until repolling a busy remote station, use the **llc2 tbusy-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 tbusy-time *milliseconds*

no llc2 tbusy-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software waits before repolling a busy remote station. The minimum is 1 ms and the maximum is 60000 ms. The default is 9600 ms.

Defaults

9600 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An Logical Link Control, type 2 (LLC2) station can to notify other stations that it is temporarily busy, so the other stations will not attempt to send any new information frames. The frames sent to indicate this are called Receiver Not Ready (RNR) frames. Change the value of this parameter only to increase the value for LLC2-speaking stations that have unusually long busy periods before they clear their busy status. Increasing the value will prevent the stations from timing out.

Examples

In the following example, the software will wait up to 12,000 ms before attempting to poll a remote station through Token Ring interface 0 to learn the station’s status:

```
! enter a global command, if you have not already
interface tokenring 0
! wait 12000 milliseconds before polling a station through tokenring 0
 llc2 tbusy-time 12000
```

Related Commands

Command	Description
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
llc2 idle-time	Controls the frequency of polls during periods of idle time (no traffic).
show llc2	Displays the LLC2 connections active in the router.

llc2 tpf-time

To set the amount of time the Cisco IOS software waits for a final response to a poll frame before resending the poll frame, use the **llc2 tpf-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 tpf-time *milliseconds*

no llc2 tpf-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) the software waits for a final response to a poll frame before resending the poll frame. The minimum is 1 ms and the maximum is 60000 ms. The default is 1000 ms.

Defaults

1000 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a command is sent that must receive a response, a poll bit is sent in the frame. This is the receiving station's clue that the sender is expecting some response from it, be it an acknowledgment of information frames or an acknowledgment of more administrative tasks, such as starting and stopping the session. Once a sender gives out the poll bit, it cannot send any other frame with the poll bit set until the receiver replies with a frame containing a final bit set. If the receiver is faulty, it may never return the final bit to the sender. Therefore, the sender could be waiting for a reply that will never come. To avoid this problem, when a poll-bit-set frame is sent, a transmit-poll-frame (TPF) timer is started. If this timer expires, the software assumes that it can send another frame with a poll bit.

Usually, you will not want to change this value. If you do, the value should be larger than the T1 time, set with the **llc2 t1-time** command. The T1 time determines how long the software waits for receipt of an acknowledgment before sending the next set of frames.

Examples

Although you generally will not want to change the transmit-poll-frame (TPF) time, this example sets the TPF time to 3000 ms. Because the TPF time should be larger than the Logical Link Control, type 2 (LLC2) T1 time, this example shows the TPF time as double the LLC2 T1 time.

```
! enter a global command, if you have not already
interface tokenring 0
```

```
! send a poll bit set through tokenring 0 after a 3000 ms delay
 llc2 tpf-time 3000
! wait 1500 milliseconds for an acknowledgment before resending I-frames
 llc2 t1-time 1500
```

Related Commands

Command	Description
llc2 idle-time	Controls the frequency of polls during periods of idle time (no traffic).
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.
show llc2	Displays the LLC2 connections active in the router.

llc2 trej-time

To control the amount of time the Cisco IOS software waits for a correct frame after sending a reject command to the remote Logical Link Control, type 2 (LLC2) station, use the **llc2 trej-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 trej-time *milliseconds*

no llc2 trej-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software waits for a resend of a rejected frame before sending a reject command to the remote station. The minimum is 1 milliseconds (ms) and the maximum is 60000 ms. The default is 3200 ms.

Defaults

3200 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an LLC2 station sends an information frame, a sequence number is included in the frame. The LLC2 station that receives these frames will expect to receive them in order. If it does not, it can reject a frame and indicate which frame it is expecting to receive instead. Upon sending a reject, the LLC2 station starts a reject timer. If the frames are not received before this timer expires, the session is disconnected.

Examples

In the following example, the software will wait up to 1000 ms to receive a previously rejected frame before resending its reject message to the station that sent the frame:

```
! enter a global command, if you have not already
interface tokenring 0
! wait 1000 milliseconds before resending a reject message through tokenring 0
 llc2 trej-time 1000
```

Related Commands

Command	Description
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 xid-neg-val-time

To control the frequency of exchange of identification (XID) transmissions by the Cisco IOS software, use the **llc2 xid-neg-val-tim** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 xid-neg-val-time *milliseconds*

no llc2 xid-neg-val-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms)) after which the software sends XID frames to other Logical Link Control, type 2 (LLC2)-speaking stations. The minimum is 0 ms and the maximum is 60000 ms. The default is 0 ms.

Defaults

0 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Do not change the **llc2 xid-neg-val-time** value unless requested by your technical support representative.

LLC2-speaking stations can communicate XID frames to each other. These frames identify the stations at a higher level than the MAC address and also can contain information about the configuration of the station. These frames are typically sent only during setup and configuration periods when it is deemed that sending them is useful. The greatest frequency at which this information is transferred is controlled by this timer.

Examples

The following example shows how to reset the frequency of XID transmissions to the default of 0 ms:

```
! enter a global command, if you have not already
interface tokenring 0
! set the frequency of XID transmissions to 0
 llc2 xid-neg-val-time 0
```

Related Commands

Command	Description
llc2 xid-retry-time	Sets the amount of time the Cisco IOS software waits for a reply to XID frames before dropping the session.
show llc2	Displays the LLC2 connections active in the router.

llc2 xid-retry-time

To set the amount of time the Cisco IOS software waits for a reply to exchange of identification (XID) frames before dropping the session, use the **llc2 xid-retry-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 xid-retry-time *milliseconds*

no llc2 xid-retry-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) the software waits for a reply to XID frames before dropping a session. The minimum is 1 ms and the maximum is 60000 ms. The default is 60000 ms.

Defaults

60000 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Set this value greater than the value of the T1 time or the time the software waits for an acknowledgment before dropping the session. T1 time is set with the **llc2 t1-time** command.

Examples

The following example sets the software to wait up to 60,000 ms for a reply to XID frames it sent to remote stations (which resets the value to its default):

```
! enter a global command, if you have not already
interface tokenring 0
! wait 60000 milliseconds for a reply to XID frames
 llc2 xid-retry-time 60000
```

Related Commands

Command	Description
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.

Command	Description
llc2 xid-neg-val-time	Controls the frequency of XID transmissions by the Cisco IOS software.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

lnm alternate

Note Effective with Cisco IOS release 12.3(4)T, the **lnm alternate** command is no longer available in Cisco IOS 12.3T releases.

To specify the threshold reporting link number, use the **lnm alternate** command in interface configuration mode. In order for a LAN Reporting Manager (LRM) to change parameters, it must be attached to the reporting link with the lowest reporting link number, and that reporting link number must be lower than this threshold reporting link number. To restore the default of 0, use the **no** form of this command.

lnm alternate *number*

no lnm alternate

Syntax Description

number	Threshold reporting link number. It must be in the range from 0 to 3.

Defaults

The default threshold reporting link number is 0.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

LAN Network Manager (LNM) employs the concepts of reporting links and reporting link numbers. A reporting link is simply a connection (or potential connection) between an LRM and a bridge. A reporting link number is a unique number used to identify a reporting link. An IBM bridge allows four simultaneous reporting links numbered 0 to 3. Only the LRM attached to the lowest number connection is allowed to change any parameters, and then only when that connection number falls below a certain configurable number. In the default configuration, the LRM connected through link 0 is the only LRM allowed to change parameters.

Note Setting the threshold reporting link number on one interface in a source-route bridge will cause it to appear on the other interface of the bridge, because the command applies to the bridge itself and not to either of the interfaces.

Examples

The following example permits LRMs connected through links 0 and 1 to change parameters:

```
! provide appropriate global configuration command if not currently in your config.
!
! permit 0 and 1
lnm alternate 1
```

The following example permits all LRMs to change parameters in the Cisco IOS software:

```
! provide appropriate global configuration command if not currently in your config.
!
! permit 0, 1, 2, and 3
lnm alternate 3
```

Related Commands

Command	Description
lnm password	Sets the password for the reporting link.

lnm crs

Note Effective with Cisco IOS release 12.3(4)T, the **lnm crs** command is no longer available in Cisco IOS 12.3T releases.

To monitor the current logical configuration of a Token Ring, use the **lnm crs** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm crs

no lnm crs

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Configuration Report Server service tracks the current logical configuration of a Token Ring and reports any changes to LAN Network Manager (LNM). It also reports on various other activities such as the change of the Active Monitor on a Token Ring.

For more information about the Active Monitor, refer to the *IBM Token Ring Architecture Reference Manual* or the IEEE 802.5 specification.

Examples

The following example disables monitoring of the current logical configuration of a Token Ring:

```
interface tokenring 0
 no lnm crs
```

Related Commands

Command	Description
lnm rem	Monitors errors reported by any station on the ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm disabled

Note Effective with Cisco IOS release12.3(4)T, the **lnm disable** command is no longer available in Cisco IOS 12.3T releases.

To disable LAN Network Manager (LNM) functionality, use the **lnm disabled** command in global configuration mode. To restore LNM functionality, use the **no** form of this command.

lnm disabled

no lnm disabled

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Under some circumstances, you can disable all LNM server functions on the router without having to determine whether to disable a specific server, such as the ring parameter server or the ring error monitor on a given interface.

This command can be used to terminate all LNM server input and reporting links. In normal circumstances, this command should not be necessary because it is a superset of the functions normally performed on individual interfaces by the **no lnm rem** and **no lnm rps** commands.

Examples

The following example disables LNM functionality:

```
lnm disabled
```

Related Commands

Command	Description
lnm pathtrace-disabled	Disables pathtrace reporting to LNM stations.
lnm rem	Monitors errors reported by any station on the ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm express-buffer

Note Effective with Cisco IOS release 12.3(4)T, the **lnm express-buffer** command is no longer available in Cisco IOS 12.3T releases.

To enable the LAN Network Manager (LNM) Ring Parameter Server (RPS) express buffer function, use the **lnm express-buffer** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm express-buffer

no lnm express-buffer

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The RPS express buffer function allows the router to set the express buffer bit to ensure priority service for frames required for ring station initiation. When this function is enabled, the router sets the express buffer bit in its initialize ring station response, which allows Token Ring devices to insert into the ring during bursty conditions.

Examples

The following example enables the LNM RPS express buffer function:

```
lnm express-buffer
```

lnm loss-threshold

Note Effective with Cisco IOS release 12.3(4)T, the **lnm loss-threshold** command is no longer available in Cisco IOS 12.3T releases.

To set the threshold at which the Cisco IOS software sends a message informing all attached LAN Network Manager (LNM)s that it is dropping frames, use the **lnm loss-threshold** command in interface configuration mode. To return to the default value, use the **no** form of this command.

lnm loss-threshold *number*

no lnm loss-threshold

Syntax Description

number	Single number expressing the percentage loss rate in hundredths of a percent. The valid range is from 0 to 9999. The default is

Defaults

10 (0.10 percent).

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The software sends a message to all attached LNMs whenever it begins to drop frames. The point at which this report is generated (threshold) is a percentage of the number of frames dropped compared with the number of frames forwarded.

When setting this value, remember that 9999 would mean 100 percent of your frames could be dropped before the message is sent. A value of 1000 would mean 10 percent of the frames could be dropped before sending the message. A value of 100 would mean 1 percent of the frames could be dropped before the message is sent.

Examples

In the following example, the loss threshold is set to 0.02 percent:

```
interface tokenring 0
 lnm loss-threshold 2
```

lnm password

Note Effective with Cisco IOS release 12.3(4)T, the **lnm password** command is no longer available in Cisco IOS 12.3T releases.

To set the password for the reporting link, use the **lnm password** command in interface configuration mode. To return the password to its default value of 00000000, use the **no** form of this command.

lnm password *number string*

no lnm password *number*

Syntax Description

number	Number of the reporting link to which to apply the password. This value must be in the range from 0 to 3.
string	Password you enter at the keyboard. In order to maintain compatibility with LAN Network Manager (LNM), the parameter *string* should be a six- to eight-character string of the type listed in the "Usage Guidelines" section.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

LNM employs the concepts of reporting links and reporting link numbers. A reporting link is simply a connection (or potential connection) between a LAN Reporting Manager (LRM) and a bridge. A reporting link number is a unique number used to identify a reporting link. An IBM bridge allows four simultaneous reporting links numbered 0 to 3. Only the LRM attached to the lowest number connection is allowed to change any parameters, and then only when that connection number falls below a certain configurable number. In the default configuration, the LRM connected through link 0 is the only LRM allowed to change parameters.

Each reporting link has its own password. Passwords are used not only to prevent unauthorized access from an LRM to a bridge, but also to control access to the different reporting links. This is important because of the different abilities associated with the various reporting links.

Characters allowable in the *string* are the following:

- Letters
- Numbers
- Special characters @, #, $, or %

Passwords are displayed only through use of the privileged EXEC **show running-config** command.

Note Two parameters in an IBM bridge have no corresponding parameter in the Cisco IOS software. This means that any attempt to modify these parameters from LNM will fail and display an error message. The LNM names of these two parameters are *route active status* and *single route broadcast mode*.

Examples

In the following example, the password Zephyr@ is assigned to reporting link 2:

```
! provide appropriate global configuration command if not currently in your config.
!
lnm password 2 Zephyr@
```

Related Commands

Command	Description
lnm alternate	Specifies the threshold reporting link number. In order for an LRM to change parameters, it must be attached to the reporting link with the lowest reporting link number, and that reporting link number must be lower than this threshold reporting link number.

lnm pathtrace-disabled

Note Effective with Cisco IOS release 12.3(4)T, the **lnm pathtrace-dsiabled** command is no longer available in Cisco IOS 12.3T releases.

To disable pathtrace reporting to LAN Network Manager (LNM) stations, use the **lnm pathtrace-disabled** command in global configuration mode. To restore pathtrace reporting functionality, use the **no** form of this command.

lnm pathtrace-disabled [**all** | **origin**]

no lnm pathtrace-disabled

Syntax Description

all	(Optional) Disable pathtrace reporting to the LNM and originating stations.
origin	(Optional) Disable pathtrace reporting to originating stations only.

Defaults

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Under some circumstances, such as when new hardware has been introduced into the network and is causing problems, the automatic report pathtrace function can be disabled. The new hardware may be setting bit-fields B1 or B2 (or both) of the routing control field in the routing information field embedded in a source-route bridged frame. This condition may cause the network to be flooded by report pathtrace frames if the condition is persistent. The **lnm pathtrace-disabled** command, along with its options, allows you to alleviate network congestion that may be occurring by disabling all or part of the automatic report pathtrace function within LNM.

Examples

The following example disables all pathtrace reporting:

```
lnm pathtrace-disabled
```

Related Commands

Command	Description
lnm disabled	Disables LNM functionality.

lnm rem

Note Effective with Cisco IOS release 12.3(4)T, the **lnm rem** command is no longer available in Cisco IOS 12.3T releases.

To monitor errors reported by any station on the ring, use the **lnm rem** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm rem

no lnm rem

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Ring Error Monitor (REM) service monitors errors reported by any station on the ring. It also monitors whether the ring is in a functional state or in a failure state.

Examples

The following example shows the use of the **lnm rem** command:

```
interface tokenring 0
 lnm rem
```

Related Commands

Command	Description
lnm crs	Monitors the current logical configuration of a Token Ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm rps

Note Effective with Cisco IOS release 12.3(4)T, the **lnm rps** command is no longer available in Cisco IOS 12.3T releases.

To ensure that all stations on a ring are using a consistent set of reporting parameters, use the **lnm rps** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm rps

no lnm rps

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Ring Parameter Server (RPS) service ensures that all stations on a ring are using a consistent set of reporting parameters and are reporting to LAN Network Manager (LNM) when any new station joins a Token Ring.

Examples

The following example shows the use of the **lnm rps** command:

```
interface tokenring 0
 lnm rps
```

Related Commands

Command	Description
lnm crs	Monitors the current logical configuration of a Token Ring.
lnm rem	Monitors errors reported by any station on the ring.

lnm snmp-only

Note Effective with Cisco IOS release 12.3(4)T, the **lnm snmp-only** command is no longer available in Cisco IOS 12.3T releases.

To prevent any LAN Network Manager (LNM) stations from modifying parameters in the Cisco IOS software, use the **lnm snmp-only** command in global configuration mode. To allow modifications, use the **no** form of this command.

lnm snmp-only

no lnm snmp-only

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring a router for LNM support is very simple. It happens automatically as a part of configuring the router to act as a source-route bridge. Several commands are available to modify the behavior of the LNM support, but none of them are necessary for it to function.

Because there is now more than one way to remotely change parameters in the Cisco IOS software, this command was developed to prevent them from detrimentally interacting with each other.

This command does not affect the ability of LNM to monitor events, only to modify parameters in the Cisco IOS software.

Examples

The following command prevents any LNM stations from modifying parameters in the software:

```
lnm snmp-only
```

lnm softerr

Note Effective with Cisco IOS release 12.3(4)T, the **lnm softerr** command is no longer available in Cisco IOS 12.3T releases.

To set the time interval in which the Cisco IOS software will accumulate error messages before sending them, use the **lnm softerr** command in interface configuration mode. To return to the default value, use the **no** form of this command.

lnm softerr *ten-illiseconds*

no lnm softerr

Syntax Description

ten-milliseconds	Time interval in tens of milliseconds between error messages. The valid range is from 0 to 65535.

Defaults

200 ms (2 seconds).

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All stations on a Token Ring notify the ring error monitor (REM) when they detect errors on the ring. To prevent an excessive number of messages, error reports are not sent immediately, but are accumulated for a short period of time and then reported. A station learns this value from a router (configured as a source-route bridge) when it first enters the ring.

Examples

The following example changes the error-reporting frequency to once every 5 seconds:

```
lnm softerr 500
```

Related Commands

Command	Description
lnm rem	Monitors errors reported by any station on the ring.

locaddr-priority

To assign a remote source-route bridging (RSRB) priority group to an input interface, use the **locaddr-priority** command in interface configuration mode. To remove the RSRB priority group assignment from the interface, use the **no** form of this command.

locaddr-priority *list-number*

no locaddr-priority *list-number*

Syntax Description

list-number	Priority list number of the input interface.

Defaults

No RSRB priority group is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must use the **priority-list protocol** command to assign priorities to the ports as shown in Table 14.

Table 14 Common RSRB Services and Their Port Numbers

Service	Port
RSRB high priority	1996
RSRB medium priority	1987
RSRB normal priority	1988
RSRB low priority	1989

Examples

In the following example, Token Ring interface 0 is assigned the RSRB priority group 1; LU 01 is assigned a medium priority and maps to TCP port 1996; LU 02 has been assigned a normal priority and maps to TCP port 1987; LU 03 has been assigned a low priority and maps to TCP port 1988; and LU 04 has been assigned high priority and maps to TCP port 1989:

```
source-bridge ring-group 2624
source-bridge remote-peer 2624 tcp 10.0.0.1
source-bridge remote-peer 2624 tcp 10.0.0.2 local-ack priority
locaddr-priority-list 1 01 medium
```

```
locaddr-priority-list 1 02 normal
locaddr-priority-list 1 03 low
locaddr-priority-list 1 04 high
!
priority-list 1 protocol ip low tcp 1996
priority-list 1 protocol ip high tcp 1987
priority-list 1 protocol ip medium tcp 1988
priority-list 1 protocol ip normal tcp 1989
!
interface tokenring 0
 source-bridge 2576 8 2624
 locaddr-priority 1
```

Related Commands

Command	Description
locaddr-priority-list	Maps LUs to queueing priorities as one of the steps to establishing queueing priorities based on LU addresses.
priority-list protocol	Establishes queueing priorities based on the protocol type.

locaddr-priority-list

To map logical units (LUs) to queueing priorities as one of the steps to establishing queueing priorities based on LU addresses, use the **locaddr-priority-list** command in global configuration mode. To remove that priority queueing assignment, use the **no** form of this command. You use this command in conjunction with the **priority list** command.

locaddr-priority-list *list-number address-number queue-keyword* [**dsap** *ds*] [**dmac** *dm*] [**ssap** *ss*] [**smac** *sm*]

no locaddr-priority-list *list-number address-number queue-keyword* [**dsap** *ds*] [**dmac** *dm*] [**ssap** *ss*] [**smac** *sm*]

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the LU address priority list selected by the user.
address-number	Value of the LOCADDR= parameter on the LU macro, which is a 1-byte address of the LU in hexadecimal.
queue-keyword	Enables a priority queue type: Valid queue keyword values and their equivalent priority queue type level are: • **high**—Priority queue type is high. • **medium**—Priority queue type is medium. • **normal**—Priority queue type is normal. • **low**—Priority queue type is low.
dsap *ds*	(Optional) Indicates that the next argument, *ds*, represents the destination service access point address. The argument *ds* is a hexadecimal value.
dmac *dm*	(Optional) Indicates that the next argument, *dm*, is the destination MAC address. The argument *dm* is written as a dotted triple of four-digit hexadecimal numbers.
ssap *ss*	(Optional) Indicates that the next argument, *ss*, is the source service access point address. If this is not specified, the default is all source service access point addresses.
smac *sm*	(Optional) Indicates that the next argument, *sm*, is the source MAC address, written as a dotted triple of four-digit hexadecimal numbers. If this is not specified, the default is all source MAC addresses.

Defaults

No mapping.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The following keywords were added: • **ssap** • **smac**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to map LUs to queueing priorities. Once you establish the priority for each LU, you can assign a priority to a TCP port. Hence you establish a mapping between the LUs and queueing priorities, and queueing priorities and TCP ports.

It is preferable to prioritize NetBIOS traffic below Systems Network Architecture (SNA) traffic, but by default NetBIOS traffic is assigned the high priority on TCP port 1996.

Examples

In the following example, Token Ring interface 0 is assigned the remote source-route bridging (RSRB) priority group 1; LU 01 is assigned a medium priority and maps to TCP port 1996; LU 02 has been assigned a normal priority and maps to TCP port 1987; LU 03 has been assigned a low priority and maps to TCP port 1988; and LU 04 has been assigned high priority and maps to TCP port 1989:

```
source-bridge ring-group 2624
source-bridge remote-peer 2624 tcp 10.0.0.1
source-bridge remote-peer 2624 tcp 10.0.0.2 local-ack priority
locaddr-priority-list 1 01 medium
locaddr-priority-list 1 02 normal
locaddr-priority-list 1 03 low
locaddr-priority-list 1 04 high
!
priority-list 1 protocol ip low tcp 1996
priority-list 1 protocol ip high tcp 1987
priority-list 1 protocol ip medium tcp 1988
priority-list 1 protocol ip normal tcp 1989
!
interface tokenring 0
 source-bridge 2576 8 2624
 locaddr-priority 1
```

The following example shows how to establish queueing priorities based on the address of the serial link on a serial tunnel (STUN) connection. Note that you must use the **priority-group** command in interface configuration mode to assign a priority group to an input interface.

```
stun peer-name 10.108.254.6
stun protocol-group 1 sdlc
locaddr-priority-list 1 02 high
locaddr-priority-list 1 03 high
locaddr-priority-list 1 04 medium
locaddr-priority-list 1 05 low
!
interface serial 0
 no ip address
 encapsulation stun
```

```
stun group 1
stun route address 4 interface serial 0 direct
locaddr priority 1
priority-group 1
```

Related Commands

Command	Description
locaddr-priority	Assigns an RSRB priority group to an input interface.
priority-list protocol	Establishes queueing priorities based on the protocol type.

lsap

To create a service access point (SAP) in the Systems Network Architecture (SNA) session switch and enter Dependent Logical Unit Requestor (DLUR) SAP configuration mode, use the **lsap** DLUR configuration command. To delete a SAP and all SNA session switch links using the internal LAN interface, use the **no** form of this command.

lsap *type adapter-number* [*lsap*]

no lsap *type adapter-number* [*lsap*]

Syntax Description

type	Internal adapter type on the Channel Interface Processor (CIP) card, which corresponds to the value specified in the **lan** internal LAN configuration command. The currently supported value for the *type* argument is **token-adapter**.
adapter-number	Internal adapter interface on the CIP card, which is the same value specified in the **adapter** internal LAN configuration command.
lsap	(Optional) Local SAP number, 04 to FC, in hexadecimal. The value must be even number and should normally be a multiple of four. It must be an unique within the internal adapter in that no other 802.2 clients of that adapter, in the router or in a host, should be allocated the same SAP. The default value is C0.

Defaults

The default value for the *lsap* argument is hexadecimal C0.

Command Modes

DLUR configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **lsap** command is valid only on the virtual channel interface. If the SAP in the SNA session switch function is already created, the **lsap** command with no arguments puts you in DLUR SAP configuration mode.

The **lsap** command can be entered only in DLUR configuration mode.

The **lsap** command uses values that are defined in two other commands: the **lan** internal LAN configuration command and the **adapter** internal LAN configuration command. The **lan** *type* and **adapter** *adapter-number* values configured on the Cisco Mainframe Channel Connection (CMCC) internal LAN interface are used in the **lsap** command. However, the **lan** *type* keyword is a little different.

Where the value for the *type* argument on the **lan** command is **tokenring**, the corresponding value for the *type* argument on **lsap** is **token-adapter**. This emphasizes that the number that follows is an **adapter** number, not a **lan** number.

The **no lsap** command hierarchically deletes any links using it. Any sessions using those links are lost.

Examples

The following example defines an adapter type, an adapter number, and a local SAP:

```
lsap token 0 B0
```

Related Commands

Command	Description
adapter	Configures internal adapters.
client pool	Nails clients to pools.
keylen	Specifies the maximum bit length for the encryption keys for SSL Encryption Support.

lu deletion

To specify whether the TN3270 server sends a REPLY-PSID poweroff request to virtual telecommunications access method (VTAM) to delete the corresponding logical unit (LU) when a client disconnects, use the **lu deletion** command in TN3270 server configuration mode. To remove LU deletion from the current configuration scope, use the **no** form of this command.

lu deletion {**always** | **normal** | **non-generic** | **never** | **named**}

no lu deletion

Syntax Description

always	Always delete dynamic LUs upon disconnect.
normal	Delete screen LUs only upon disconnect.
non-generic	Delete only specified LUs upon disconnect.
never	Never delete LUs upon disconnect. The default is never.
named	Delete only named LUs upon disconnect.

Defaults

The default keyword is **never**.

Command Modes

TN3270 server configuration—The **lu deletion** command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **lu deletion** command at this level applies to all PUs defined at the listen point.

Listen-point PU configuration—The **lu deletion** command at this level applies only to the specified PU.

Dependent Logical Unit Requestor (DLUR) PU configuration—The **lu deletion** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **lu deletion** command at this level applies only to the specified PU.

Note The **lu deletion** command is a siftdown command, so it can be used at any of the configuration command modes shown. The most recent **lu deletion** command in the PU configuration takes precedence.

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to add the **named** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **always** keyword of the **lu deletion** command when you have only screen LUs, and they are all different sizes. This prevents screen LUs from attaching to a previously used LU with an incompatible screen size.

Use the **normal** keyword of the **lu deletion** command when you have both screen and printer LUs. This is important because printers are acquired by the host application, and not logged on manually. If VTAM deletes the LU, then there is nothing for a host application (such as CICS) to acquire.

You can use the **non-generic** mode of LU deletion if VTAM can support deletion of specifically named LUs. (The support of this mode is not available in VTAM, as of VTAM version 4.4.1.)

Use the **never** mode of LU deletion when you have only screen LUs and they all use the same screen size.

Use the **named** keyword of the **lu deletion** command when you have configured dynamic LU names from the TN3270 server side.

Examples

Following is an example of the **lu deletion** command specifying that the TN3270 server send a REPLY-PSID poweroff request to delete only screen LUs upon session disconnect for any PUs supported by the TN3270 server:

```
tn3270-server
 lu deletion normal
```

Following is an example of the **lu deletion** command configuring a listen-point PU to define Dependent Logical Unit Requestor (DLUR) PUs using dynamic LU naming:

```
tn3270-server
listen-point 172.18.4.18
pu pu1 05D9901 dlur
 lu deletion named
```

Related Commands

Command	Description
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.

lu termination

To specify whether a TERMSELF or UNBIND request/response unit (RU) is sent by the TN3270 server when a client turns off a device or disconnects, use the **lu termination** command in TN3270 server configuration mode. To remove LU termination from the current configuration scope, use the **no** form of this command.

lu termination {**termself** | **unbind**}

no lu termination

Syntax Description

termself	Orders termination of all sessions and session requests associated with a logical unit (LU) upon disconnect.
unbind	Requests termination of the session by the application upon LU disconnect. This value is the default.

Defaults

unbind is the default.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Note The **lu termination** command is a siftdown command, so it can be used at any of the configuration command modes shown. The most recent **lu termination** command in the PU configuration takes precedence.

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **termself** keyword when you want to be sure that the application terminates the session when the LU disconnects. This is important for certain applications such as Customer Information Control System (CICS).

If you use the **unbind** keyword for session termination with applications such as CICS, virtual telecommunications access method (VTAM) security problems can arise. When CICS terminates a session from an UNBIND request, the application may reestablish a previous user's session with a new user, who is now assigned to the same freed LU.

In TN3270 server configuration mode, the **lu termination** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **lu termination** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **lu termination** command applies only to the specified PU.

In DLUR PU configuration mode, the **lu termination** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **lu termination** command applies only to the specified PU.

Examples

Following is an example of the **lu termination** configuration command to force termination of the session when an LU disconnects for any PUs supported by the TN3270 server:

```
tn3270-server
 lu termination termself
```

mac-address

To modify the default MAC address of an interface to some user-defined address, use the **mac-address** command in interface configuration mode. To return to the default MAC address on the interface, use the **no** form of this command.

mac-address *ieee-address*

no mac-address *ieee-address*

Syntax Description

ieee-address	48-bit IEEE MAC address written as a dotted triple of four-digit hexadecimal numbers.

Defaults

The interface uses a default MAC address that is derived from the base address stored in the electrically erasable programmable read-only memory (EEPROM).

Command Modes

Interface configuration

Usage Guidelines

Be sure that no other interface on the network is using the MAC address that you assign.

There is a known defect in earlier forms of this command when the Texas Instruments Token Ring MAC firmware is used. This implementation is used by Proteon, Apollo, and IBM RTs. A host using a MAC address whose first two bytes are zeros (such as a Cisco router) will not properly communicate with hosts using that form of this command of TI firmware.

There are two solutions. The first involves installing a static Routing Information Field (RIF) entry for every faulty node with which the router communicates. If there are many such nodes on the ring, this may not be practical. The second solution involves setting the MAC address of the Cisco Token Ring to a value that works around the problem.

This command forces the use of a different MAC address on the specified interface, thereby avoiding the Texas Instrument MAC firmware problem. It is up to the network administrator to ensure that no other host on the network is using that MAC address.

Examples

The following example sets the MAC layer address, where *xx.xxxx* is an appropriate second half of the MAC address to use:

```
interface tokenring 0
 mac-address 5000.5axx.xxxx
```

The following example changes the default MAC address on the interface to 1111.2222.3333:

```
Router# configure terminal
Router(config)# interface fastethernet 2/1/1
Router(config-if)# mac-address 1111.2222.3333
```

Related Commands

Command	Description
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

maximum-lus

To limit the number of logical unit (LU) control blocks that will be allocated for the TN3270 server, use the **maximum-lus** command in TN3270 server configuration mode. To restore the default value, use the **no** form of this command.

maximum-lus *number*

no maximum-lus

Syntax Description

number	Maximum number of LU control blocks allowed. The allowed range is from 0 to 32000. However, the practical upper limit for concurrently operating TN3270 sessions depends on the hardware and usage characteristics. The default is 2100.

Defaults

Because of the license structure, the default is 2100, which represents the limit of the lower-priced license (2000) plus a 5 percent buffer. If you configure a value greater than the default, a license reminder is displayed.

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **maximum-lus** command is valid only on the virtual channel interface. Although the value may be varied at any time, reducing it below the current number of LU control blocks will not release those blocks until a physical unit (PU) is inactivated by Deactivate Physical Unit (DACTPU) or by using the **no pu** command.

If the number of LUs in use reaches 94 percent of the current setting, a warning message is displayed on the console. To prevent redundant messages, the threshold for generating such messages is raised for a period.

The TN3270 server attempts to allocate one LU control block for each LU activated by the hosts. In the case of dynamic definition of dependent LU (DDDLU) the control block is allocated when the client requests the LU, in anticipation of an activate logical unit (ACTLU) from the system services control points (SSCP) host.

By limiting the number of LU control blocks allocated, you can make sure enough memory is available to support other Cisco Mainframe Channel Connection (CMCC) functions. The control blocks themselves take about 1K bytes per LU. During session activity, a further 2K per LU may be needed for data. On a Channel Interface Processor (CIP), 32 MB of memory will support 4000 LUs. To support more than 4000 LUs, we recommend 64 MB of memory. On an XCPA, 8 MB of memory supports 1000 LUs.

Examples

The following example allows 5000 LU control blocks to be allocated:

```
maximum-lus 5000
```

Related Commands

Command	Description
client ip	Adds an IP subnet to a client subnet response-time group.
pu (TN3270)	Creates a PU entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters DLUR PU configuration mode.

max-llc2-rcvbuffs

To configure the number of receive DMA buffers that are used by the LLC2 stack on the CIP/XCPA, use the **max-llc2-rcvbuffs** internal adapter configuration command. Use the **no** form of this command to revert to the default setting.

max-llc2-rcvbuffs *buffers*

no max-llc2-rcvbuffs *buffers*

Syntax Description

buffers	The number of receive DMA buffers that are used by the LLC2 stack on the CIP/XCPA. The allowed range is from 500 to 1250 in multiples of 50. The default is 500.

Defaults

500 buffers

Command Modes

Virtual interface configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the **max-llc2-rcvbuffs** for 750 buffers on Channel interface 4/2:

```
interface Channel4/2
 max-llc2-rcvbuffs 750
lan TokenRing 12
 source-bridge 16 1 500
 adapter 0 4000.cafe.0000
  llc2 Nw 31
  llc2 rnr-activated
 adapter 1 4000.cafe.0001
```

Related Commands

Command	Description
llc2 nw	Increases the window size for consecutive good I-frames received.
llc2 rnr-activated	Invokes dynamic windowing logic for a link station when the router receives an RNR from the remote link station.

max-llc2-sessions

To specify the maximum number of Logical Link Control, type 2 (LLC2) sessions supported on the Cisco Mainframe Channel Connection (CMCC) adapter, use the **max-llc2-sessions** command in interface configuration mode. To restore the default value, use the **no** form of this command.

max-llc2-sessions *number*

no max-llc2-sessions *number*

Syntax Description

number	A value in the range from 1 to 6000 Logical Link Control (LLC) sessions. If this command is not configured, the default is 256 sessions.

Defaults

The default number of sessions is 256.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is configured on the virtual interface of a Channel Interface Processor (CIP), and the physical interface of a Channel Port Adapter (CPA). If you do not configure this parameter on the CMCC adapter, then the limit of LLC2 sessions is 256.

This command will fail if not enough memory is available on the CMCC adapter to support the specified number of LLC2 sessions.

Note A value of 0 sets the maximum number of LLC2 sessions to the default value of 256. In this case, the value does not appear in your configuration when you use the **show run** command.

Examples

The following example limits the maximum number of LLC2 sessions to 212:

```
max-llc2-sessions 212
```

multiring

To enable collection and use of Routing Information Field (RIF) information, use the **multiring** command in interface configuration mode. To disable the use of RIF information for the protocol specified, use the **no** form of this command.

multiring {*protocol* [**all-routes** | **spanning**] | **all** | **other**}

no multiring {*protocol* [**all-routes** | **spanning**] | **all** | **other**}

Syntax Description

protocol	Specifies a protocol. The following protocols are supported: • **appletalk**—AppleTalk Phase 1 and 2 • **clns**—ISO CLNS • **decnet**—DECnet Phase IV • **ip**—IP • **ipx**—Novell IPX
all-routes	(Optional) Uses all-routes explorers.
spanning	(Optional) Uses spanning-tree explorers.
all	Enables the multiring for *all* frames.
other	Enables the multiring for *any* routed frame not included in the previous list of supported protocols.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The following keywords were added: • **all-routes** • **spanning**
12.2(13)T	The following values for the *protocol* argument were removed: • **apollo** • **vines** • **xns**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Level 3 routers that use protocol-specific information (for example, Novell IPX or XNS headers) rather than MAC information to route datagrams also must be able to collect and use RIF information to ensure that they can send datagrams across a source-route bridge. The software default is to not collect and use RIF information for routed protocols. This allows operation with software that does not understand or properly use RIF information.

Note When you are configuring DLSw+ over FDDI, the **multiring** command supports only IP and IPX.

The **multiring** command allows for per-protocol specification of the interface's ability to append RIFs to routed protocols. When it is enabled for a protocol, the router will source packets that include information used by source-route bridges. This allows a router with Token Ring interfaces, for the protocol or protocols specified, to connect to a source-bridged Token Ring network. If a protocol is not specified for multiring, the router can route packets only to nodes directly connected to its local Token Ring.

Examples

The following example enables IP and Novell IPX bridging on a Token Ring interface. RIFs will be generated for IP frames, but not for the Novell IPX frames.

```
! commands that follow apply to interface token 0
interface tokenring 0
! enable the Token Ring interface for IP
 ip address 131.108.183.37 255.255.255.0
! generate RIFs for IP frames
 multiring ip
! enable the Token Ring interface for Novell IPX
 novell network 33
```

Related Commands

Command	Description
clear rif-cache	Clears the entire RIF cache.
rif	Enters static source-route information into the RIF cache.
rif timeout	Determines the number of minutes an inactive RIF entry is kept.
show rif	Displays the current contents of the RIF cache.
xns encapsulation	Selects the type of encapsulation used on a Token Ring interface.

name

To assign a name to the internal adapter, use the **name** command in internal adapter configuration mode. To remove the name assigned to an internal adapter, use the **no** form of this command.

name *name*

no name *name*

Syntax Description

name	Name that identifies this internal adapter. The name consists of up to eight characters (not including blank spaces).

Defaults

No default behavior or values

Command Modes

Internal adapter configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example assigns a name to an internal adapter interface:

```
name VTAM_B14
```

Related Commands

Command	Description
adapter	Configures internal adapters.

ncia

To stop or start a native client interface architecture (NCIA) server, use the **ncia** command in privileged EXEC mode.

ncia {**start** | **stop**}

Syntax Description

start	Starts the NCIA server when it has been stopped using the **ncia stop** command.
stop	Stops the NCIA server. When the server is stopped, all clients are disconnected, all circuits are dropped, and no clients can connect to the server.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

As soon as the NCIA server is configured, it begins running. If an NCIA server is configured and the configuration is stored in the NVRAM of the router, when the router boots up, the server is started automatically. Issuing the **ncia start** command when a server is already running causes the router to display the message:

```
NCIA server is running already!
```

There is not a **no** form for this command.

Examples

The following example stops an active NCIA server:

```
Router# ncia stop
```

Related Commands

Command	Description
ncia server	Configures an NCIA server on a Cisco router.

ncia client

To configure a native client interface architecture (NCIA) client on a Cisco router, use the **ncia client** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ncia client *server-number client-ip-address virtual-mac-address* [**sna** | **all**]

no ncia client *server-number client-ip-address virtual-mac-address* [**sna** | **all**]

Syntax Description

server-number	Number assigned to identify the server. Currently, the server number must be configured with a value of 1.
client-ip-address	IP address of the client.
virtual-mac-address	Virtual MAC address of the client.
sna	(Optional) NCIA client only supports Systems Network Architecture (SNA) traffic.
all	(Optional) NCIA client supports all types of traffic. If you do not specify **all** as the supported traffic type when you configure an NCIA client, the client supports only SNA traffic.

Defaults

No NCIA client is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must use the **ncia server** command to configure an NCIA server on the router before using the **ncia client** command to configure an NCIA client.

The purpose in configuring a client is so the NCIA server can connect outward to a client. When an end station on the LAN side tries to connect to a client, the end station sends an explorer. When the server receives this explorer, the server tries to match the MAC address in the client database. If it finds a match, the server then connects to that client. If the ability for the server to connect outward to clients is not needed, there is no reason to configure any clients.

Each client is assigned a MAC address from the pool created by the **ncia server** command. There are two exceptions to this guideline:

- A MAC address outside the pool created by the **ncia server** command can be defined in the **ncia client** command.

When a client configured with a MAC address outside the pool connects to the server, the client's configured MAC address is used, rather than allocating a new one from the pool.

- If a client has its own MAC address, it uses that address.

  The MAC address is recognized during the "capability exchange" period when the client establishes a session with the NCIA server. Normally, it is not necessary to configure any client. The server accepts a connection from any unconfigured client. If the unconfigured client does not have its own MAC address, a MAC address from the pool will be assigned to it. If the unconfigured client has its own MAC address, that MAC address is used. If the client has its own MAC address and it is configured using the **ncia client** command, the two MAC addresses must match; otherwise, the connection will not be established.

If you do not specify the **all** keyword as the supported traffic type when you configure an NCIA client, the client only supports only SNA traffic.

Examples

The following example configures an NCIA client on a router:

```
ncia client 1 10.2.20.5 1111.2222.3333
```

Related Commands

Command	Description
ncia server	Configures an NCIA server on a Cisco router.
dlsw local-peer	Defines the parameters of the data-link switching plus (DLSw+) local peer.

ncia rsrb

To configure an remote source-route bridging (RSRB) ring to associate with an native client interface architecture (NCIA) server on a Cisco router, use the **ncia rsrb** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ncia rsrb *virtual-ring local-bridge local-ring ncia-bridge ncia-ring virtual-mac-address*

no ncia rsrb

Syntax Description

virtual-ring	RSRB ring group number. This number corresponds to the **ring-number** keyword defined by a **source-bridge ring-group** command.
local-bridge	Number of the bridge connecting the virtual ring and the local ring.
local-ring	Number of the virtual ring connecting the virtual ring and the NCIA ring.
ncia-bridge	Number of the bridge connecting the local ring and the NCIA ring.
ncia-ring	NCIA ring group number. This number corresponds to the **ring-number** keyword defined by a **source-bridge ring-group** command.
virtual-mac-address	Local ring virtual MAC address.

Defaults

No RSRB ring is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must use the **ncia server** command to configure an NCIA server on the router before using the **ncia rsrb** command to configure an RSRB ring to associate with the server.

Examples

The following example configures a virtual ring to associate with an NCIA server on a Cisco router:

```
source-bridge ring-group 22
source-bridge ring-group 44
ncia rsrb 44 4 33 3 22 1111.1111.2222
```

Related Commands

Command	Description
ncia server	Configures an NCIA server on a Cisco router.
source-bridge ring-group	Defines or removes a ring group from the configuration.

ncia server

To configure an native client interface architecture (NCIA) server on a Cisco router, use the **ncia server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ncia server *server-number server-ip-address server-virtual-mac-address virtual-mac-address virtual-mac-range* [**inbound-only**] [**keepalive** *seconds*] [**tcp_keepalive** *minutes*]

no ncia server

Syntax Description

server-number	Number assigned to identify the server. Currently, the server number must be configured with a value of 1.
server-ip-address	IP address used to accept the incoming connection, or to make an outgoing connection.
server-virtual-mac-address	MAC address of the server.
virtual-mac-address	The first MAC address of the virtual MAC address pool.
virtual-mac-range	The range of virtual MAC addresses that can be assigned to the client. The valid range is from 1 to 4095. This number sets the upper limit on the number of contiguous MAC addresses that make up the MAC address pool.
inbound-only	(Optional) When the **inbound-only** keyword is configured, the NCIA server cannot make an outgoing connection.
keepalive *seconds*	(Optional) Keepalive interval in seconds. The valid range is from 0 to 1200. Setting the value to 0 turns the **keepalive** off.
tcp_keepalive *minutes*	(Optional) TCP keepalive processing interval in minutes. The valid range is from 0 to 99 minutes. Setting the value to 0 stops TCP from sending keepalive packets when an NCIA client is idle. If no **tcp_keepalive** value is set, the default waiting period for TCP keepalive packets is 20 minutes.

Defaults

No NCIA server is configured.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before configuring an NCIA server, you must use the **dlsw local-peer** command to configure a data-link switching plus (DLSw+) local peer on this router. Depending on your network design, you may need to use the **ncia client** command to configure an NCIA client on this router (optional), or use the **ncia rsrb** command to configure an remote source-route bridging (RSRB) ring to associate with this router (optional).

If you use the **inbound-only** keyword, there is no need to configure any NCIA clients (the server does not make out-going connections).

In a downstream physical unit (DSPU) configuration, before a client can establish a connection to a downstream physical unit (PU), such as a PC or workstation, the MAC address of the server (*server-virtual-mac-address*) must be defined at the PC or workstation as the destination MAC address. This MAC address appears as the server MAC address in the output of the **show ncia circuits** command.

Examples

The following example configures an NCIA server on a Cisco router:

```
ncia server 1 10.2.20.4 4000.3174.0001 4000.0000.0001 128 keepalive 0 tcp_keepalive 0
```

Related Commands

Command	Description
dlsw local-peer	Defines the parameters of the DLSw+ local peer.
ncia client	Configures an NCIA client on a Cisco router.
ncia rsrb	Configures an RSRB ring to associate with an NCIA server on a Cisco router.

netbios access-list bytes

To define the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets, use the **netbios access-list bytes** command in global configuration mode. To remove an entire list or the entry specified with the *pattern* argument, use the **no** form of this command.

netbios access-list bytes *name* {**permit** | **deny**} *offset pattern*

no netbios access-list bytes *name* [**permit** | **deny**]

Syntax Description

name	Name of the access list being defined.
permit	Permits the condition.
deny	Denies the condition.
offset	Decimal number indicating the number of bytes into the packet where the byte comparison should begin. An offset of zero points to the very beginning of the NetBIOS header. Therefore, the NetBIOS delimiter string (0xFFEF), for example, begins at offset 2.
pattern	Hexadecimal string of digits representing a byte pattern. The *pattern* argument must conform to certain conventions described in the "Usage Guidelines" section.

Defaults

No offset or pattern is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For offset pattern matching, the byte pattern must be an even number of hexadecimal digits in length.

The byte pattern must be no more than 16 bytes (32 hexadecimal digits) in length.

As with all access lists, the NetBIOS access lists are scanned in order.

You can specify a wildcard character in the byte string indicating that the value of that byte does not matter in the comparison. This is done by specifying two asterisks (**) in place of digits for that byte. For example, the following command would match 0xabaacd, 0xab00cd, and so on:

```
netbios access-list bytes marketing permit 3 0xab**cd
```

Examples

The following example shows how to configure for offset pattern matching:

```
netbios access-list bytes marketing permit 3 0xabcd
```

In the following example, the byte pattern would not be accepted because it must be an even number of hexadecimal digits:

```
netbios access-list bytes marketing permit 3 0xabc
```

In the following example, the byte pattern would not be permitted because the byte pattern is longer than 16 bytes in length:

```
netbios access-list bytes marketing permit 3 00112233445566778899aabbccddeeff00
```

The following example would match 0xabaacd, 0xab00cd, and so on:

```
netbios access-list bytes marketing permit 3 0xab**cd
```

The following example deletes the entire marketing NetBIOS access list named marketing:

```
no netbios access-list bytes marketing
```

The following example removes a single entry from the list:

```
no netbios access-list bytes marketing deny 3 0xab**cd
```

In the following example, the first line serves to deny all packets with a byte pattern starting in offset 3 of 0xab. However, this denial would also include the pattern 0xabcd because the entry permitting the pattern 0xabcd comes after the first entry:

```
netbios access-list bytes marketing deny 3 0xab
netbios access-list bytes marketing permit 3 0xabcd
```

Related Commands

Command	Description
netbios input-access-filter bytes	Defines a byte access list filter on incoming messages. T
netbios output-access-filter bytes	Defines a byte access list filter on outgoing messages.

netbios access-list host

To assign the name of the access list to a station or set of stations on the network, use the **netbios access-list host** command in global configuration mode. The NetBIOS station access list contains the station name to match, along with a permit or deny condition. To remove either an entire list or just a single entry from a list, depending upon the value given for *pattern* argument, use the **no** form of this command.

netbios access-list host *name* {**permit** | **deny**} *pattern*

no netbios access-list host *name* {**permit** | **deny**} *pattern*

Syntax Description

name	Name of the access list being defined.
permit	Permits the condition.
deny	Denies the condition.
pattern	A set of characters. The characters can be the name of the station, or a combination of characters and pattern-matching symbols that establish a pattern for a set of NetBIOS station names. This combination can be especially useful when stations have names with the same characters, such as a prefix. Table 15 in the "Usage Guidelines" section explains the pattern-matching symbols that can be used.

Defaults

No access list is assigned.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Table 15 explains the pattern-matching characters that can be used.

Table 15 Station Name Pattern-Matching Characters

Character	Description
*	Used at the end of a string to match any character or string of characters.
?	Matches any single character. If this wildcard is used as the first letter of the name, you must precede it with a Cntl-V key sequence. Otherwise it will be interpreted by the router as a request for help.

Examples

The following example specifies a full station name to match:

```
netbios access-list host marketing permit ABCD
```

The following example specifies a prefix where the pattern matches any name beginning with the characters DEFG:

```
!The string DEFG itself is included in this condition.
netbios access-list host marketing deny DEFG*
```

The following example permits any station name with the letter W as the first character and the letter Y as the third character in the name. The second and fourth character in the name can be any character. This example would allow stations named WXYZ and WAYB; however, stations named WY and WXY would not be allowed because the question mark (?) must match specific characters in the name:

```
netbios access-list host marketing permit W?Y?
```

The following example illustrates how to combine wildcard characters. In this example the marketing list denies any name beginning with AC that is not at least three characters in length (the question mark [?] would match any third character). The string ACBD and ACB would match, but the string AC would not:

```
netbios access-list host marketing deny AC?
```

In the following example, a single entry in the marketing NetBIOS access list is removed:

```
no netbios access-list host marketing deny AC?*
```

In the following example, the entire marketing NetBIOS access list is removed:

```
no netbios access-list host marketing
```

Related Commands

Command	Description
netbios input-access-filter host	Defines a station access list filter on incoming messages.
netbios output-access-filter host	Defines a station access list filter on outgoing messages.

netbios enable-name-cache

To enable NetBIOS name caching, use the **netbios enable-name-cache** command in interface configuration mode. To disable the name-cache behavior, use the **no** form of this command.

netbios enable-name-cache

no netbios enable-name-cache

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command enables the NetBIOS name cache on the specified interface. By default the name cache is disabled for the interface. Proxy explorers must be enabled on any interface that is using the NetBIOS name cache.

Examples

The following example enables NetBIOS name caching for Token Ring interface 0:

```
interface tokenring 0
 source-bridge proxy-explorer
 netbios enable-name-cache
```

Related Commands

Command	Description
clear netbios-cache	Clears the entries of all dynamically learned NetBIOS names.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.
show netbios-cache	Displays a list of NetBIOS cache entries.

netbios input-access-filter bytes

To define a byte access list filter on incoming messages, use the **netbios input-access-filter bytes** command in interface configuration mode. The actual access filter byte offsets and patterns used are defined in one or more **netbios-access-list bytes** commands. To remove the entire access list, use the **no** form of this command with the appropriate name.

netbios input-access-filter bytes *name*

no netbios input-access-filter bytes *name*

Syntax Description

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list bytes** global configuration commands.

Defaults

No access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example applies a previously defined filter named *marketing* to packets coming into Token Ring interface 1:

```
interface tokenring 1
 netbios input-access-filter bytes marketing
```

Related Commands

Command	Description
netbios access-list bytes	Defines the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets.

netbios input-access-filter host

To define a station access list filter on incoming messages, use the **netbios input-access-filter host** command in interface configuration mode. To remove the entire access list, use the **no** form of this command with the appropriate argument.

netbios input-access-filter host *name*

no netbios input-access-filter host *name*

Syntax Description

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list host** global configuration commands.

Defaults

No access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The access lists of station names are defined in **netbios access-list host** commands.

Examples

The following example filters packets coming into Token Ring interface 1 using the NetBIOS access list named *marketing*:

```
interface tokenring 1
 netbios access-list host marketing permit W?Y?
 netbios input-access-filter host marketing
```

Related Commands

Command	Description
netbios access-list host	Assigns the name of the access list to a station or set of stations on the network.
netbios output-access-filter host	Defines a station access list filter on outgoing messages.

netbios name-cache

To define a static NetBIOS name cache entry, tying the server with the name *netbios-name* to the *mac-address*, and specifying that the server is accessible either locally through the *interface-name* specified, or remotely, through the **ring-group** *group-number* specified, use the **netbios name-cache** command in global configuration mode. To remove the entry, use the **no** form of this command.

netbios name-cache *mac-address netbios-name* {*interface-name intetrface-number* | **ring-group** *group-number*}

no netbios name-cache *mac-address netbios-name*

Syntax Description

mac-address	The MAC address.
netbios-name	Server name linked to the MAC address.
interface-name	Name of the interface by which the server is accessible locally.
interface-umber	Number of the interface by which the server is accessible locally.
ring-group	Specifies that the link is accessible remotely.
group-number	Number of the ring group by which the server is accessible remotely. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.

Defaults

No entry is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To specify an entry in the static name cache, first specify a Routing Information Field (RIF) that leads to the server's MAC address. The Cisco IOS software displays an error message if it cannot find a static RIF entry for the server when the NetBIOS name-cache entry is attempted or if the server's type conflicts with that given for the static RIF entry.

Note The names are case sensitive; therefore "Cc" is not the same as "cC."

Examples

The following example indicates the syntax usage of this command if the NetBIOS server is accessed locally:

```
source-bridge ring-group 2
 rif 0220.3333.4444 00c8.042.0060 tokenring 0
 netbios name-cache 0220.3333.4444 DEF tokenring 0
```

The following example indicates the syntax usage of this command if the NetBIOS server is accessed remotely:

```
source-bridge ring-group 2
 rif 0110.2222.3333 0630.021.0030 ring group 2
 netbios name-cache 0110.2222.3333 DEF ring-group 2
```

Related Commands

Command	Description
show netbios-cache	Displays a list of NetBIOS cache entries.

netbios name-cache name-len

To specify how many characters of the NetBIOS type name the name cache will validate, use the **netbios name-cache name-len** command in global configuration mode.

netbios name-cache name-len *length*

no netbios name-cache name-len *length*

Syntax Description

length	Length of the NetBIOS type name. The range is from 8 to 16 characters.

Defaults

15 characters

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that the name cache will validate 16 characters of the NetBIOS type name:

```
netbios name-cache name-len 16
```

Related Commands

Command	Description
netbios enable-name-cache	Enables NetBIOS name caching.
netbios name-cache	Defines a static NetBIOS name cache entry.
netbios name-cache proxy-datagram	Enables the Cisco IOS software to act as a proxy and send NetBIOS datagram type frames.
netbios name-cache query-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process.

Command	Description
netbios name-cache recognized-timeout	Specifies the "dead" time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is only effective at the time of the login negotiation process.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.

netbios name-cache proxy-datagram

To enable the Cisco IOS software to act as a proxy and send NetBIOS datagram type frames, use the **netbios name-cache proxy-datagram** command in global configuration mode. To return to the default value, use the **no** form of this command.

netbios name-cache proxy-datagram *seconds*

no netbios name-cache proxy-datagram *seconds*

Syntax Description

seconds	Time interval, in seconds, that the software forwards a route broadcast datagram type packet. The valid range is any number greater than 0.

Defaults

There is no default time interval.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that the software will forward a NetBIOS datagram type frame in 20-second intervals:

```
netbios name-cache proxy-datagram 20
```

Related Commands

Command	Description
netbios enable-name-cache	Enables NetBIOS name caching.
netbios name-cache	Defines a static NetBIOS name cache entry, tying the server with the name netbios-name to the mac-address, and specifying that the server is accessible either locally through the interface-name specified, or remotely through the ring-group group-number specified.

Command	Description
netbios name-cache query-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process.
netbios name-cache recognized-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is only effective at the time of the login negotiation process.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.

netbios name-cache query-timeout

To specify the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame, use the **netbios name-cache query-timeout** command in global configuration mode. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process. To restore the default of 6 seconds, use the **no** form of this command.

netbios name-cache query-timeout *seconds*

no netbios name-cache query-timeout

Syntax Description

seconds	Dead time period in seconds. Default is 6 seconds.

Defaults

6 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the timeout to 15 seconds:

```
netbios name-cache query-timeout 15
```

Related Commands

Command	Description
netbios name-cache recognized-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is only effective at the time of the login negotiation process.

netbios name-cache recognized-timeout

To specify the "dead" time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame, use the **netbios name-cache recognized-timeout** command in global configuration mode. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is effective only at the time of the login negotiation process. To restore the default of 6 seconds, use the **no** form of this command.

netbios name-cache recognized-timeout *seconds*

no netbios name-cache recognized-timeout

Syntax Description

seconds	Dead time period in seconds. Default is 6 seconds.

Defaults

6 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the timeout to 15 seconds:

```
netbios name-cache recognized-timeout 15
```

Related Commands

Command	Description
netbios name-cache query-timeout	Specifies the "dead" time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process.

netbios name-cache timeout

To enable NetBIOS name caching and to set the time that entries can remain in the NetBIOS name cache, use the **netbios name-cache timeout** command in global configuration mode. To restore the default of 15 minutes, use the **no** form of this command.

netbios name-cache timeout *minutes*

no netbios name-cache timeout *minutes*

Syntax Description

minutes	Time, in minutes, that entries can remain in the NetBIOS name cache. Default is 15 minutes.

Defaults

15 minutes

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to establish NetBIOS name caching. NetBIOS name-caching does not apply to static entries. Once the time expires, the entry will be deleted from the cache.

Examples

The following example sets the timeout to 10 minutes:

```
interface tokenring 0
 netbios name-cache timeout 10
```

Related Commands

Command	Description
show netbios-cache	Displays a list of NetBIOS cache entries.

netbios output-access-filter bytes

To define a byte access list filter on outgoing messages, use the **netbios output-access-filter bytes** command in interface configuration mode. To remove the entire access list, use the **no** form of this command.

netbios output-access-filter bytes *name*

no netbios output-access-filter bytes *name*

Syntax Description

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list bytes** global configuration commands.

Defaults

No access list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example filters packets leaving Token Ring interface 1 using the NetBIOS access list named engineering:

```
interface tokenring 1
 netbios access-list bytes engineering permit 3 0xabcd
 netbios output-access-filter bytes engineering
```

Related Commands

Command	Description
netbios access-list bytes	Defines the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets.
netbios input-access-filter bytes	Defines a byte access list filter on incoming messages.

netbios output-access-filter host

To define a station access list filter on outgoing messages, use the **netbios output-access-filter host** command in interface configuration mode. To remove the entire access list, use the **no** form of this command.

netbios output-access-filter host *name*

no netbios output-access-filter host *name*

Syntax Description

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list host** global configuration commands.

Defaults

No access list filter is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example filters packets leaving Token Ring interface 1 using the NetBIOS access list named *engineering*:

```
interface tokenring 1
 netbios access-list host engineering permit W?Y?
 netbios output-access-filter host engineering
```

Related Commands

Command	Description
netbios access-list host	Assigns the name of the access list to a station or set of stations on the network.
netbios input-access-filter host	Defines a station access list filter on incoming messages.

offload (backup)

To configure a backup group of offload devices, use the **offload** command in IP host backup configuration mode. To cancel the offload task on the Cisco Mainframe Channel Connection (CMCC) adapter, use the **no** form of this command.

offload *device-address ip-address host-name device-name host-ip-link device-ip-link host-api-link device-api-link* [**broadcast**]

no offload *path device-address*

Syntax Description

device-address	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
ip-address	Hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even-numbered value.
host-name	Host name specified in the device statement in the host TCP/IP application configuration file.
device-name	Common Link Access for Workstations (CLAW) workstation name specified in the device statement in the host TCP/IP application configuration file.
host-ip-link	Host link name for the IP link as specified by the host application. For IBM virtual machine (VM) and Multiple Virtual Systems (MVS) TCP/IP stacks, this value is **tcpip**. When used with other applications, this value must match the value coded in the host application.
device-ip-link	Workstation link name for the IP link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is **tcpip**. When used with other applications, this value must match the value coded in the host application.
host-api-link	Host link name for the application program interface (API) link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is **tcpip**. When used with other applications, this value must match the value coded in the host application.
device-api-link	Offload link name for the API link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is **api**. When used with other applications, this value must match the value coded in the host application.
broadcast	(Optional) Enables broadcast processing for this subchannel.

Defaults

No default behavior or values

Command Modes

IP host backup configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Along with the **path** command, the **offload** backup command provides a quick way to configure an offload backup group.

Offload devices provide IP connectivity to a mainframe while offloading a large part of the TCP/IP processing to the CMCC adapter. Not every mainframe TCP/IP stack supports offload.

Th**e offload** command in IP host backup configuration mode uses the same underlying configuration parameters as the **claw** command in IP host backup configuration mode.

Examples

The following examples show two methods for entering the same IP host backup group information. The first group of commands is the long form, using the **offload** interface configuration command. The second group is the shortcut, using the **path** interface configuration command and an **offload** IP host backup configuration command.

Long form:

```
offload c000 00 10.92.10.5 sysa router1 tcpip tcpip tcpip api backup
offload c100 00 10.92.10.5 sysa router1 tcpip tcpip tcpip api backup
offload c200 00 10.92.10.5 sysa router1 tcpip tcpip tcpip api backup
```

Shortcut form:

```
path c000 c100 c200
  offload 00 10.92.10.5 sysa router1 tcpip tcpip tcpip api
```

Related Commands

Command	Description
show extended channel ip-stack	Displays information about the IP stack running on CMCC channel interfaces.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel tcp-connections	Displays information about the TCP sockets on a channel interface.

Command	Description
show extended channel tcp-stack	Displays information about the TCP stack running on CMCC adapter interfaces.
offload (primary) (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
security (TN3270)	Displays CLAW packing names and their connection state.

offload (primary)

To configure an offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and configure individual members of an offload backup group for the IP Host Backup feature, use the **offload** command in interface configuration mode. To cancel the offload task on the Cisco Mainframe Channel Connection (CMCC) adapter, use the **no** form of this command.

offload *path device-address ip-address host-name device-name host-ip-link device-ip-link host-api-link device-api-link* [**broadcast**] [**backup**]

no offload *path device-address*

Syntax Description

path	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
device-address	Hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even-numbered value.
ip-address	IP address specified in the host TCP/IP application configuration file.
host-name	Host name specified in the device statement in the host TCP/IP application configuration file.
device-name	Common Link Access for Workstations (CLAW) workstation name specified in the device statement in the host TCP/IP application configuration file.
host-ip-link	Common Link Access for Workstations (CLAW) host link name for the IP link as specified by the host application. For IBM virtual machine (VM) and VMS TCP/IP stacks, this value is **tcpip**. When used with other applications, this value must match the value coded in the host application.
device-ip-link	CLAW workstation link name for the IP link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is **tcpip**. When used with other applications, this value must match the value coded in the host application.
host-api-link	CLAW host link name for the application program interface (API) link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is **tcpip**. When used with other applications, this value must match the value coded in the host application.
device-api-link	Offload link name for the API link as specified by the host application. For IBM VM and MVS TCP/IP stacks, this value is **api**. When used with other applications, this value must match the value coded in the host application.
broadcast	(Optional) Enables broadcast processing for this subchannel.
backup	(Optional) Enables this offload connection to be used as part of a backup group of offload connections for the specified IP address.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0	The **backup** keyword was added**.**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Offload devices provide IP connectivity to a mainframe while offloading a large part of the TCP/IP processing to the CMCC adapter. Not every mainframe TCP/IP stack supports offload.

The **offload** command uses the same underlying configuration parameters as does the **claw** command.

Examples

The following example shows how to enable IBM channel attach offload processing on a CMCC adapter's physical channel interface that is supporting a directly connected ESCON channel:

```
interface channel 3/0
ip address 10.92.0.1 255.255.255.0
offload 0100 00 10.92.0.21 CISCOVM EVAL TCPIP TCPIP TCPIP API
```

The following example shows how an IP host backup group is specified using the **backup** keyword:

```
interface Channel3/0
 no ip address
 no keepalive
 shutdown
 offload 0100 C0 10.30.1.2 TCPIP OS2TCP TCPIP TCPIP TCPIP API backup
 offload 0110 C0 10.30.1.2 TCPIP OS2TCP TCPIP TCPIP TCPIP API backup
 offload 0120 C0 10.30.1.2 TCPIP OS2TCP TCPIP TCPIP TCPIP API backup
 offload 0110 C2 10.30.1.3 TCPIP OS2TCP TCPIP TCPIP TCPIP API
```

Related Commands

Command	Description
offload (backup)	Configures a backup group of Offload devices.
security (TN3270)	Displays CLAW packing names and their connection state.
show extended channel ip-stack	Displays information about the IP stack running on CMCC channel interfaces.
show extended channel statistics	Displays statistical information about subchannels on the physical interface of a CMCC adapter and displays information that is specific to the interface channel devices. The information generally is useful only for diagnostic tasks performed by technical support personnel.
show extended channel subchannel	Displays information about the CMCC adapter physical interfaces and displays information that is specific to the interface channel connection. The information displayed generally is useful only for diagnostic tasks performed by technical support personnel.

Command	Description
show extended channel tcp-connections	Displays information about the TCP sockets on a channel interface.
show extended channel tcp-stack	Displays information about the TCP stack running on CMCC adapter interfaces.
show extended channel udp-listeners	Displays information about the UDP listener sockets running on the CMCC adapter interfaces.
show extended channel udp-stack	Displays information about the UDP stack running on the CMCC adapter interfaces.

offload alias

To assign a virtual IP address to a real IP address for an offload device on a Cisco Mainframe Channel Connection (CMCC) adapter, use the **offload alias** command in interface configuration mode. To remove the alias IP address, use the **no** form of this command.

offload alias *real-ip alias-ip*

no offload alias *real-ip alias-ip*

Syntax Description

real-ip	Real IP address of the offload-supported device.
alias-ip	Virtual IP address for the offload-supported device.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configure the **offload alias** command after you configure TCP/IP offload support on a CMCC adapter.

You can configure up to 8 different alias IP addresses for each real IP address of an offload device. You can assign the same alias IP address to multiple real IP addresses.

Examples

The following example configures TCP/IP offload support on a CMCC adapter for a host located at real IP address 10.10.21.3 with an alias IP address of 10.2.33.88:

```
interface channel 3/1
 offload E180 80 10.10.21.3 IPCLUST IPCLUST TCPIP TCPIP TCPIP API
 offload alias 10.10.21.3 10.2.33.88
```

path

Command	Description
name (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
show extended channel icmp-stack	Displays information about the ICMP stack running on the CMCC channel interfaces.
show extended channel ip-stack	Displays information about the IP stack running on CMCC channel interfaces.

To specify one or more data paths for the IP host backup, use the **path** command in interface configuration mode. To delete a single path, use the **no** form of this command.

path *path*

no path *path*

Syntax Description

path	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default values for channel logical address and control unit logical address is 0. Up to 16 values for the *path* argument can be specified in the **path** command.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Up to 16 values for the *path* argument can be specified in the **path** command.

The path command places the router in IP host backup configuration mode, where additional commands can be entered to define backup groups for Common Link Access for Workstations (CLAW) and offload connections.

Examples

The following examples show two methods for entering the same IP host backup group information. The first group is the long form, using the **offload** command in interface configuration mode. The second group of commands is the shortcut, using the **path** interface configuration command and an **offload** IP host backup configuration command.

Long form:

```
offload c000 00 198.92.10.5 sysa router1 tcpip tcpip backup
offload c100 00 198.92.10.5 sysa router1 tcpip tcpip backup
offload c200 00 198.92.10.5 sysa router1 tcpip tcpip backup
```

Shortcut form:

```
path c000 c100 c200
  offload 00 198.92.10.5 sysa router1 tcpip tcpip
```

Related Commands

Command	Description
claw (backup)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.

ping sna

To initiate an Advanced Program-to-Program Communication (APPC) session with a named destination logical unit (LU) to run the APING transaction program to check network integrity and timing characteristics, use the **ping sna** command in privileged EXEC mode.

ping sna [**-1**] [**-c** *consecutive-packets*] [**-i** *number-iterations*] [**-m** *mode*] [**-n**] [**-r**] [**-s** *size*] [**-t** *tpname*] [**-u** *userid* **-p** *password*] *destination*

Syntax Description

-1	(Optional) Sends data from client to server only (no echo).
-c *consecutive-blocks*	(Optional) Specifies the number of data blocks sent per iteration. The default is 1.
-i *number-iterations*	(Optional) Specifies the number of iterations. The default is 2.
-m *mode*	(Optional) Specifies the APPC mode to use. The default is #INTER.
-n	(Optional) Omits any security (SECURITY=NONE).
-r	(Optional) Displays the route taken by APPC PING.
-s *size*	(Optional) Specifies the size of the data block to be sent. The default is 100 bytes.
-t *tpname*	(Optional) Specifies transaction program (TP) to start on the server. The default is APINGD.
-u *userid*	(Optional) Specifies USERID.
-p *password*	(Optional) Specifies the password associated with the userid specified after **-u**. Required when **-u** is specified. Password must be one to eight characters in length.
destination	Specifies the fully qualified name of the destination logical unit or control point with which an APING transaction should be initiated.

Defaults

If **-1** is not specified, the **ping sna** command will send the quantity of data represented by the **-s** *size*, **-i** *number-iterations*, and **-c** *consecutive blocks* options. It will be first sent in the direction from the **ping sna** requester to the receiver, then in the opposite direction.

If **-c** is not specified, consecutive data blocks per iteration defaults to 1.

If **-i** is not specified, number of iterations defaults to 2.

If **-m** is not specified, the mode defaults to #INTER.

If **-s** is not specified, the size of each block of data transferred defaults to 100 bytes.

If **-t** is not specified, the default transaction program name on the receiver is APINGD.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ping sna** command requires the destination to support the APING transaction program for the ping to succeed.

Examples

The following is an example of the **ping sna** command contact the destination NETA.CP001:

```
Router# ping sna NETA.CP001
```

Related Commands

Command	Description
show snasw session	Displays the SNASw session objects.

pool

To define pool names for the TN3270 server and specify the number of screens and printers in each logical cluster, use the **pool** command in TN3270 server configuration mode. To remove a client IP pool, use the **no** form of this command.

pool *poolname* [**cluster layout** *layout-spec-string*]

no pool *poolname*

Syntax Description

poolname	Unique pool name that cannot exceed eight characters in length. Valid characters are (alphabetic characters are not case sensitive): • First character—Alphabetic (A–Z) and national characters "@”, “#”, and “$” • Second through eighth characters—Alphabetic (A–Z), numeric (0–9), and national characters "@”, “#”, and “$”
cluster layout *layout-spec-string*	(Optional) Name for the cluster and to indicate a cluster of logical unit (LU)s such as printers. The sum of the numbers must be less than or equal to 255. No spaces are used between the entries in the *layout-spec-string* argument. The default value is 1a.

Defaults

The default value for the *layout-spec-string* argument is 1a.

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **pool** and **allocate lu** commands enable the TN3270 server to know the relationships between screen and printer LUs. These commands are an alternative to the logical unit (LU) nailing feature that allows clients to be nailed to LUs.

The **pool** command is configured in the TN3270 scope. The **pool** command provides the pool names and the definitions of the number of screens and printers in one logical cluster. Each pool statement must have a unique pool name.

The TN3270 server validates pool names when configuring a pool name and when processing the name received on a CONNECT request from the client. The TN3270 server rejects an invalid name and truncates the name received in the CONNECT request from the client to eight characters or at an invalid character (whichever comes first) when processing the CONNECT request.

When using a **pool** command to create a cluster, use a combination of the following values in the *layout-spec-string* argument:

s (screen)

p (printer)

a (any, or wildcard) (refers to a printer or a screen)

Examples

Use the following format to define the *layout-spec-string* argument, where the *decimal-num* argument is a decimal number from 1 to 255:

```
pool poolname cluster layout {decimal-nums}{decimal-nump}{decimal-numa}
```

The total sum of the numbers must be less than or equal to 255. No spaces are used between the entries in the *layout-spec-string* argument. The default is 1a, which defines one screen or one printer. A screen, printer, or a wildcard definition cannot be followed by a definition of the same type. A screen definition can be followed only by a printer or wildcard. Similarly, a printer definition can be followed only by a wildcard or a screen definition.

The following are examples of invalid *layout-spec-string* values, and the corresponding corrected specification:

- A *layout-spec-string* of 3s6s is invalid. The correct specification is 9s.
- A *layout-spec-string* of 3s6p7a8a is invalid. The correct specification is 3s6p15a.
- A *layout-spec-string* of 255s10p is invalid. Although the decimal number for any portion of the *layout-spec-string* can be from 1 to 255, the total number across all parameters cannot exceed 255. To correct this example, you can reduce the screens to 245 as 245s10p.

The combination of a screen, printer, and wildcard constitute a group. The *layout-spec-string* argument can support a maximum of four groups.

Consider the following example:

```
pool CISCO cluster layout 2s3p4a5s6a7s8p9s
```

There are four groups in this definition: 2s3p4a, 5s6a, 7s8p and 9s.

Pools must be defined before any pool references under the listen points are defined. Also, pools must be defined before they are referenced by other statements in the configuration. Failure to define the pool before it is referenced will cause the referencing configuration to be rejected.

Pools that are deleted (using the **no** form of the command) will cause all statements referencing the pool to be deleted.

The following criteria apply to the creation of pool names and local addresses:

- Pool and LU names must be unique; they cannot be identical.
- Local address ranges for pools must not overlap.
- Local address ranges for LU pools must not overlap with the existing client nailing configuration.
- Pool configurations made while LUs are in use do not affect the current LU configuration.

The following example uses the **pool** command to create two pools, pcpool and unixpool:

```
tn3270-server
```

```
 pool pcpool cluster layout 4s1p
 pool unixpool cluster layout 49s1p
listen-point 10.20.30.40
 client ip 10.10.10.2 pool pcpool
 pu PU1 91903315 dlur
  allocate lu 1 pool pcpool clusters 50
 pu PU2 91903345 dlur
  allocate lu 1 pool unixpool clusters 5
```

In this example, the pcpool contains a cluster of 4 screens and 1 printer per cluster. The total number of devices in a cluster cannot exceed 255, therefore the pcpool contains a total of 50 clusters with each cluster containing 5 LUs. Note that the remaining 5 LUs automatically go to the generic pool.

The unixpool contains 49 screens and 1 printer per cluster. The total number of devices in a cluster cannot exceed 255, therefore the unixpool contains a total of 5 clusters with each cluster containing 50 LUs. Again, note that the last 5 LUs automatically go to the generic pool.

Related Commands

Command	Description
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

ppp bcp tagged-frame

To enable the negotiation of IEEE 802.1Q-tagged packets over PPP links, use the **ppp bcp tagged-frame** command in interface configuration mode. To disable the negotiation of IEEE 802.1Q-tagged packets over PPP links, use the **no** form of this command.

ppp bcp tagged-frame

no ppp bcp tagged-frame

Syntax Description

This command has no arguments or keywords.

Defaults

The **ppp bcp tagged-frame** command is enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command provides flexibility in specifying which Bridge Control Protocol (BCP) options will be negotiated with the peer.

Examples

The following example configures Ethernet interface 0 to bridge packets using VLAN ID 100, and assigns the interface to bridge group 1:

```
interface serial 4/0
 ppp bcp tagged-frame
```

preferred-nnserver

To specify a preferred network node (NN) as server, use the **preferred-nnserver** command in Dependent Logical Unit Requestor (DLUR) configuration mode. To remove the preference, use the **no** form of this command.

preferred-nnserver *name*

no preferred-nnserver

Syntax Description

name	Fully qualified name of an NN.

Defaults

No default behavior or values

Command Modes

DLUR configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **preferred-nnserver** command is valid only on the virtual channel interface. Fully qualified names consist of two case-insensitive alphanumeric strings, separated by a period. However, for compatibility with existing Advanced Peer-to-Peer Networking (APPN) products, including virtual telecommunications access method (VTAM), the characters “#” (pound), “@” (at), and “$” (dollar) are allowed in the fully qualified name strings. Each string is from one to 8 characters long; for example, RA12.NODM1PP. The portion of the name before the period is the network entity title (NET) ID and is shared between entities in the same logical network.

When no preferred server is specified, the Dependent Logical Unit Requestor (DLUR) will request NN server support from the first suitable node with which it makes contact. If refused, it will try the next one, and so on.

If a preferred server is specified, then DLUR will wait a short time to allow a link to the preferred server to materialize. If the preferred server is not found in that time, any suitable node can be used.

DLUR will not relinquish the current NN server merely because the preferred server becomes available.

Examples

The following example selects SYD.VMX as the preferred NN server:

```
preferred-nnserver SYD.VMX
```

Related Commands

Command	Description
client pool	Nails clients to pools.

priority-list protocol bstun

To establish block serial tunnel (BSTUN) queueing priorities based on the BSTUN header, use the **priority-list protocol bstun** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

priority-list *list-number* **protocol bstun** *queue* [**gt** | **lt** *packetsize*] [**address** *bstun-group bsc-addr*]

no priority-list *list-number* **protocol bstun** *queue* [**gt** | **lt** *packetsize*] [**address** *bstun-group bsc-addr*]

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the priority list selected by the user.
queue	Priority queue type: **high**, **medium**, **normal**, or **low**.
gt | **lt** *packetsize*	(Optional) Output interface examines header information *and* packet size and places packets with the BSTUN header that match criteria (gt or lt specified packet size) on specified output.
address *bstun-group bsc-addr*	(Optional) Output interface examines header information and Bisync address and places packets with the BSTUN header that match Bisync address on the specified output queue.

Defaults

Prioritize based on BSTUN header.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the output interface examines the header information and places packets with the BSTUN header on the output queue specified as medium:

```
priority-list 1 protocol bstun medium
```

Related Commands

Command	Description
encapsulation bstun	Configures BSTUN on a particular serial interface.

priority-list protocol ip tcp

To establish block serial tunnel (BSTUN) or serial tunnel (STUN) queueing priorities based on the TCP port, use the **priority-list protocol ip tcp** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

priority-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*

no priority-list *list***-***number* **protocol ip** *queue* **tcp** *tcp-port-number*

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the priority list selected by the user.
queue	Priority queue type: **high**, **medium**, **normal**, or **low**. The default *queue* value is **normal**.
tcp-port-number	BSTUN port and priority settings are as follows: • High—BSTUN port 1976 • Medium—BSTUN port 1977 • Normal—BSTUN port 1978 • Low—BSTUN port 1979 STUN port and priority settings are as follows: • High—STUN port 1994 • Medium—STUN port 1990 • Normal—STUN port 1991 • Low—STUN port 1992

Defaults

The default *queue* value is **normal**.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **priority-list protocol stun address** command first. Priority settings created with this command are assigned to Synchronous Data Link Control (SDLC) ports.

Note SDLC local acknowledgment with the priority option must be enabled using the **stun route address tcp** command.

Examples

In the following example, queueing priority for address C1 using priority list 1 is set to high. A priority queue of high is assigned to the SDLC port 1994.

```
priority-list 1 stun high address 1 c1
priority-list 1 protocol ip high tcp 1994
```

In the following example, queueing priority for address C1 using priority list 1 is set to high. A priority queue of high is assigned to BSTUN port 1976.

```
priority-list bstun high address 1 c1
priority-list 1 protocol ip high 1976
```

Related Commands

Command	Description
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
encapsulation bstun	Configures BSTUN on a particular serial interface.
encapsulation stun	Enables STUN encapsulation on a specified serial interface.
priority-list protocol bstun	Establishes BSTUN queueing priorities based on the BSTUN header.
priority-list protocol stun address	Establishes STUN queueing priorities based on the address of the serial link.
stun route address tcp	Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for STUN.

priority-list protocol stun address

To establish serial tunnel (STUN) queueing priorities based on the address of the serial link, use the **priority-list protocol stun address** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

priority-list *list-number* **protocol stun** *queue* **address** *group-number address-number*

no priority-list *list-number* **protocol stun** *queue-keyword* **address** *group-number address-number*

Syntax Description

list-number	Arbitrary integer from 1 to 16 that identifies the priority list selected by the user.
queue	Enables a priority queue type: Valid queue values and their equivalent priority queue type level are: • **high**—Priority queue type is high. • **medium**—Priority queue type is medium. • **normal**—Priority queue type is normal. • **low**—Priority queue type is low. The default *queue* value is **normal**.
group-number	Group number that is used in the **stun group** command.
address-number	Address of the serial link. For an Synchronous Data Link Control (SDLC) link, the format is a 1-byte hexadecimal value (for example, C1). For a non-SDLC link, the address format can be specified by the **stun schema** command.

Defaults

The default *queue* value is **normal**.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Note SDLC local acknowledgment with the priority option must be enabled using the **stun route address interface serial** command.

The **priority-list** command is described in greater detail in the "Performance Management Commands" chapter in the *Cisco IOS Configuration Fundamentals Command Reference*.

Examples

In the following example, queueing priority for address C1 using priority list 1 is set to high:

```
priority-list 1 stun high address 1 c1
```

Related Commands

Command	Description
priority-list protocol ip tcp	Establishes BSTUN or STUN queueing priorities based on the TCP port.
stun group	Places each STUN-enabled interface on a router in a previously defined STUN group.
stun route address interface serial	Forwards all HDLC traffic on a serial interface.
stun schema offset length format	Defines a protocol other than SDLC for use with STUN.

profile

To specify a name and a security protocol for a security profile or to modify a profile and enter profile configuration mode, use the **profile** command in security configuration mode. To remove this name and protocol specification, use the **no** form of this command.

profile *profilename* [**ssl** | **none**]

no profile *profilename* {**ssl** | **none**}

Syntax Description

profilename	String of alphanumeric characters that specify a name for a security profile. The character range is from 1 to 24. Profile names cannot be duplicated.
ssl	Specifies that this profile will use the ssl 3.0 security protocol. This implies that the initial exchange between the client and the server is the "Client Hello" message.
none	Specifies that this profile will not use a security protocol. Sessions using this profile will not use any security.

Defaults

No default behavior or values

Command Modes

Security configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command creates or modifies a security profile. To create a profile, specify the name of the new profile along with the security type. To modify a security profile, specify the name of the profile without the security type. The security type is required only when creating a profile. Using the security type when modifying a profile will result in an error.

Profile names cannot be duplicated.

Entering the **no** form of this command deletes the profile definition and all of its subcommand definitions **(encryptorder**, **servercert**, **keylen**, **certificate reload** commands). Entering the **no** form of this command deletes the **sec-profile** command specifications on all listen points where it is defined.

Entering the **profile** command places the router in profile configuration mode. Entering the **no** form of the command places the user into the security configuration mode.

This command has no retroactive effect.

Examples

The following example specifies LAM as the profile name and ssl as the security protocol. When the **no profile LAM** command is configured, all new client connections will be nonsecure.

```
tn3270-server
 security
 profile LAM ssl
  keylen 40
  servercert slot0:lam
  certificate reload
listen-point 10.10.10.1
 sec-profile LAM
 pu DIRECT 012ABCDE tok 0 04
 no profile LAM none
```

Related Commands

Command	Description
security (TN3270)	Enables security on the TN3270 server.
sec-profile	Specifies the security profile to be associated with a listen point.
default-profile	Specifies the name of the profile to be applied to the listen points by default.

pu (DLUR)

To create a physical unit (PU) entity that has no direct link to a host or to enter PU configuration mode, use the **pu** command in DLUR configuration mode. To remove the PU entity, use the **no** form of this command.

pu *pu-name idblk-idnum ip-address*

no pu *pu-name*

Syntax Description

pu-name	Name that uniquely identifies this PU.
idblk-idnum	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server enforces uniqueness only within the set of Dependent Logical Unit Requestor (DLUR) PUs.
ip-address	IP address that the clients should use as host IP address to map to logical unit (LU) sessions under this PU.

Defaults

No PU is defined.

Command Modes

DLUR configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the PU is already created, the **pu** *pu-name* command with no arguments places the router in PU configuration mode. In this mode you can modify an existing PU DLUR entity.

A typical usage for the IP address is to reserve an IP address per host application. For example, clients wanting to connect to Time Sharing Option (TSO) specify an IP address that will be defined with PUs that have LOGAPPL=TSO.

Examples

The following example defines three PUs. Two of the PUs share the same IP address and the third PU has a separate IP address:

```
pu p0  05D99001 192.195.80.40
pu p1  05D99002 192.195.80.40
pu p2  05D99003 192.195.80.41
```

Related Commands

Command	Description
client pool	Nails clients to pools.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.

pu (listen-point)

To create a physical unit (PU) entity that has a direct link to a host or to enter listen-point PU configuration mode, use the **pu** command in listen-point configuration mode. To remove the PU entity, use the **no** form of this command.

pu *pu-name idblk-idnum type adapter-number lsap* [**rmac** *rmac*] [**rsap** *rsap*]
[**lu-seed** *lu-name-stem*]

no pu *pu-name*

Syntax Description

pu-name	Name that uniquely identifies this PU.
idblk-idnum	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server enforces uniqueness only within the set of Dependent Logical Unit Requestor (DLUR) PUs.
type	Internal adapter type on the Channel Interface Processor (CIP) card, which corresponds to the value specified in the **lan** internal LAN configuration command. The currently supported type is **token-adapter**.
adapter-number	Internal adapter interface on the CIP card, which is the same value specified in the **adapter** internal LAN configuration command.
lsap	Local service access point (SAP) number in hexadecimal, ranging from 04 to DE. The value must be even, and must be unique within the internal adapter so that no other 802.2 clients of that adapter, in the router or in a host, are allocated the same SAP. Other direct links from TN3270 server direct PUs may use the same value on the internal adapter as long as the remote MAC or SAP is different.
rmac *rmac*	(Optional) Remote MAC address. The remote MAC address in the form *xxxx.xxxx.xxxx* hexadecimal, specifying the MAC address of the remote host. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.
rsap *rsap*	(Optional) Remote SAP address. The remote SAP address is a one- or two-character hexadecimal string, ranging from 04 to FC, that specifies the SAP address of the remote host. The default is 04.
lu-seed *lu-name-stem*	(Optional) logical unit (LU) name that the client uses when a specific LU name request is needed. The format is *x...x*## or *x...x*### where *x...x* is an alphanumeric string. When ## is specified, it is replaced with the LU local address in hexadecimal digits to form the complete LU name. When ### is specified, decimal digits are used, padded with leading zeros to make three characters. The first *x* must be alphabetic and the entire string, including the # symbols, must not exceed eight characters in length.

Defaults

The default remote SAP address is 04 (hexadecimal).

Command Modes

Listen-point configuration

Command History

Release	Modification
11.2	This command was introduced.
11.2(18)BC	Listen-point PU configuration was added.
12.0(5)T	This command was integrated into Cisco IOS Releas12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **pu** *pu-name* command is valid only on the virtual channel interface. If the PU is already created, the **pu** *pu-name* command with no arguments puts you in listen-point PU configuration mode, where you can modify an existing PU entity.

The **pu** listen-point command uses values that are defined in two other commands: the **lan** internal LAN configuration command and the **adapter** internal LAN configuration command. The **lan** *type* and **adapter** *adapter-number* values configured on the CIP internal LAN interface are used in the **pu** command.

For a link via a channel on this Cisco Mainframe Channel Connection (CMCC) adapter, the TN3270 server and the hosts should open different adapters. Using different adapters avoids contention for SAP numbers and is also necessary if you configure duplicate MAC addresses for fallback Cisco Systems Network Architecture (CSNA) or Cisco Multipath Channel (CMPC) access to the host.

Examples

The following example configures the TN3270 server to be active and has one PU, CAPPU1, trying to connect. An LU seed using hexadecimal digits is defined.

```
tn3270-server
pu CAPPU1 05D18101 token-adapter 3 04 rmac 4000.0501.0001 lu-seed CAP01L##
```

The following example shows different adapter numbers configured on the same internal LAN to avoid SAP contention. The host uses SAP 4 on Token Ring adapter 0.

```
lan tokenring 0
 adapter 0 4000.0000.0001
 adapter 1 4000.0000.0002
tn3270-server
 listen-point 10.20.30.40
  pu PU1 05d00001 token-adapter 1 8 rmac 4000.0000.0001 rsap 4
```

Related Commands

Command	Description
adapter	Configures internal adapters.
lan	Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode.
listen-point	Defines an IP address for the TN3270 server.
show extended channel tn3270-server	Displays current server configuration parameters and the status of the PUs defined for the TN3270 server.

pu (TN3270)

To create a physical unit (PU) entity that has its own direct link to a host and enter PU configuration mode, use the **pu** command in TN3270 server configuration mode. To remove the PU entity, use the **no** form of this command.

pu *pu-name idblk-idnum ip-address type adapter-number lsap* [**rmac** *rmac*] [**rsap** *rsap*] [**lu-seed** *lu-name-stem*]

no pu *pu-name*

Syntax Description

pu-name	Name that uniquely identifies this PU.
idblk-idnum	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server enforces uniqueness only within the set of Dependent Logical Unit Requestor (DLUR) PUs.
ip-address	IP address that the clients should use as host the IP address to map to logical unit (LU) sessions under this PU.
type	Internal adapter type on the Channel Interface Processor (CIP) card, which corresponds to the value specified in the **lan** internal LAN configuration command. The currently supported type is **token-adapter.**
adapter-number	Internal adapter interface on the CIP card, which is the same value specified in the **adapter** internal LAN configuration command.
lsap	Local service access point (SAP) number in hexadecimal, ranging from 04 to FC. The value must be an even number, and must be unique within the internal adapter so that no other 802.2 clients of that adapter, in the router or in a host, should be allocated the same SAP. Other direct links from TN3270 server direct PUs may use the same value on the internal adapter as long as the remote MAC or SAP is different.
rmac *rmac*	(Optional) Remote MAC address. The remote MAC address of the form *xxxx.xxxx.xxxx* hexadecimal, specifying the MAC address of the remote host. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.
rsap *rsap*	(Optional) Remote SAP address. The remote SAP address is a one- or two-character hexadecimal string, ranging from 04 to FC, specifying the SAP address of the remote host. The default is 04.
lu-seed *lu-name-stem*	(Optional) logical unit (LU) name that the client uses when a specific LU name request is needed. The format is *x...x*## or *x...x*### where *x...x* is an alphanumeric string. When ## is specified, it is replaced with the LU local address in hexadecimal digits to form the complete LU name. When ### is specified, decimal digits are used, padded with leading zeros to make three characters. The first *x* must be alphabetic and the entire string, including the # symbols, must not exceed eight characters in length.

Defaults

No PU is defined.
The default remote SAP address is 04 (hexadecimal).

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **pu** *pu-name* command is valid only on the virtual channel interface. If the PU is already created, the **pu** *pu-name* command with no arguments puts you in PU configuration mode, where you can modify an existing PU entity.

The **pu** (TN3270) command uses values that are defined in two other commands: the **lan** internal LAN configuration command and the **adapter** internal LAN configuration command. The **lan** *type* and **adapter** *adapter-number* values configured on the CIP internal LAN interface are used in the **pu** command.

For a link via a channel on this Cisco Mainframe Channel Connection (CMCC) adapter, the TN3270 server and the hosts should open different adapters. Using different adapters avoids any contention for SAP numbers, and is also necessary if you configure duplicate MAC addresses for fallback Cisco Systems Network Architecture (CSNA) or Cisco Multipath Channel (CMPC) access to the host.

Examples

The following example configures the TN3270 server to be active, and has one PU, CAPPU1, trying to connect in. An LU seed using hexadecimal digits is defined.

```
tn3270-server
pu CAPPU1 05D18101 10.14.20.34 token-adapter 3 04 rmac 4000.0501.0001 lu-seed CAP01L##
```

The following example shows different adapter numbers configured on the same internal LAN to avoid SAP contention. The host uses SAP 4 on token ring adapter 0.

```
lan tokenring 0
 adapter 0 4000.0000.0001
 adapter 1 4000.0000.0002
tn3270-server
 pu PU1 05d00001 10.0.0.1 token-adapter 1 8 rmac 4000.0000.0001 rsap 4
```

Related Commands

Command	Description
adapter	Configures internal adapters.
keylen	Specifies the maximum bit length for the encryption keys for SSL Encryption Support.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

pu dlur (listen-point)

To create a physical unit (PU) entity that has no direct link to a host or to enter listen-point PU configuration mode, use the **pu dlur** command in listen-point configuration mode. To remove the PU entity, use the **no** form of this command.

pu *pu-name idblk-idnum* **dlur** [**lu-seed** *lu-name-stem*]

no pu *pu-name idblk-idnum* **dlur** [**lu-seed** *lu-name-stem*]

Syntax Description

pu-name	Name that uniquely identifies this PU.
idblk-idnum	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server enforces uniqueness only within the set of Dependent Logical Unit Requestor (DLUR) PUs.
lu-seed *lu-name-stem*	(Optional) Logical unit (LU) name that the client uses when a specific LU name request is needed. The format is *x...x*## or *x...x*### where *x...x* is an alphanumeric string. When ## is specified, it is replaced with the LU local address in hexadecimal digits to form the complete LU name. When ### is specified, decimal digits are used, padded with leading zeroes to make three characters. The first *x* must be alphabetic (A through Z), or one of the following symbols: $, #, @. The entire string, including the # symbols, must not exceed eight characters in length. The # symbols are allowed within of the lu-seed string. For example, NC##RAL or USA###NC are valid strings. The # symbols cannot be the first characters in the string. For example, ##CISCO is not valid because the first character of the LU name cannot be a number. But ####DOT is valid because the # symbols in the second, third, and fourth place are used for LU names. There must be at least two to three consecutive # symbols in the string. For example, SH# or CD#D is not valid. A string without # symbols is not valid. For example, CISCONC is not valid. You must not split the # symbols. For example, SH#NC# and SH#D#NC# are not valid. **Note** The # sign can signify a value or be used as a symbol.

Defaults

No PU is defined.

Command Modes

Listen-point configuration

Command History

Release	Modification
11.2	This command was introduced.
11.2(18)BC	Listen-point PU configuration was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(5)T	This command was integrated in Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to add the **lu-seed** option and *lu-name-stem* argument. The Luseed naming format was modified.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the PU is already created, the **pu dlur** command without any arguments starts listen-point PU configuration mode. In this mode you can modify an existing listen-point Dependent Logical Unit Requestor (DLUR) PU entity.

You should define the DLUR before you configure the listen-point DLUR PU.

A typical usage for the IP address is to reserve an IP address for each application. For example, clients wanting to connect to Time Sharing Option (TSO) specify an IP address that is defined with PUs that have LOGAPPL=TSO.

If the **lu-seed** option is not configured, the PU name is used as the implicit Luseed to generate the LU name. If the **lu-seed** option is configured, then there is an explicit LU name.

If the explicit LU names conflict, the TN3270 server will reject the PU configuration. If the implicit LU names (that is, the PU names) conflict, the TN3270 server will accept the PU definitions, but the LU names will consist of a modified, truncated version of the PU name and the local address. Valid and invalid LU seed syntax is shown in Table 16.

Table 16 LU Seed Syntax

Valid LU Seed Syntax	Invalid LU Seed Syntax
NC##RAL	NC#RAL
USA##NC	#GEORGE
#####	—

Examples

The following example defines three PUs in the listen point with an IP address of 172.18.4.18:

```
tn3270-server
listen-point 172.18.4.18
 pu p0  05D99001 dlur
 pu p1  05D99002 dlur
 pu p2  05D99003 dlur
```

The following is an example of the TN3270 server configured with LU pooling. A listen-point PU is configured to define DLUR PUs using the dynamic LU naming. Note that the **lu deletion** command must be configured with the **named** option. The PU pu1 is defined with lu-seed abc##pqr. Using hexadecimal numbers for ##, the LU names for this PU are ABC01PQR, ABC02PQR, ABC0APQR.... up to ABCFFPQR. Similarly, the PU pu2 is defined with lu-seed pqr###. Using decimal numbers for ###, the LU names for this PU are PQR001, PQR002... up to PQR255.

The LUs ABC01PQR through ABC32PQR and PQR100 through PQR199 are allocated to the pool SIMPLE. The LUs ABC64PQR through ABC96PQR and PQR010 through PQR035 are allocated to the pool PCPOOL. The remaining LUs are in the generic pool.

```
tn3270-server
 pool simple cluster layout 1s
 pool pcpool cluster layout 4s1p
 lu deletion named
 dlur neta.shek neta.mvsd
  lsap tok 15 04
    link she1 rmac 4000.b0ca.0016
 listen-point 172.18.4.18
 pu pu1 91903315 tok 16 08 lu-seed abc##pqr
   allocate lu 1 pool simple clusters 50
   allocate lu 100 pool pcpool clusters 10
 pu pu2 91913315 dlur lu-seed pqr###
   allocate lu 10 pool pcpool clusters 5
   allocate lu 100 pool simple clusters 100
```

Related Commands

Command	Description
dlur	Enables the SNA session switch function on the CMCC adapter and enters DLUR configuration mode.
listen-point	Defines an IP address for the TN3270 server.

qllc accept-all-calls

To enable the router to accept a call from any remote X.25 device, use the **qllc accept-all-calls** command in interface configuration mode. To cancel the request, use the **no** form of this command.

qllc accept-all-calls

no qllc accept-all-calls

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows Qualified Logical Link Control (QLLC) to accept all inbound X.25 calls, provided that the QLLC Call User Data (CUD) is in the call packet and the destination X.121 address in the call packet matches the serial interface's configured destination X.121 address or subaddress. When this command is used, the source X.121 address need not be configured via an **x25 map qllc** command for the call to be accepted.

This command is applicable to QLLC support for data-link switching plus (DLSw+), Advanced Peer-to-Peer Networking (APPN), and downstream physical unit (DSPU). It is not applicable to QLLC support for source-route bridging (SRB) and remote source-route bridging (RSRB).

Examples

The following example enables QLLC connectivity for DLSw+ and allows QLLC to accept all inbound X.25 calls. Every X.25 connection request for X.121 address 0308 with QLLC CUD is directed to DLSw+. The first switched virtual circuit (SVC) to be established will be mapped to virtual MAC address 4000.0B0B.0001. If a call comes in with an X.121 address of 0308, the call will be forwarded to MAC address 4001.1161.1234.

```
interface serial 0
 encapsulation x25
 x25 address 0308
 qllc accept-all-calls
 qllc dlsw vmac 4000.0B0B.0001 500 partner 4001.1161.1234
```

Related Commands

Command	Description
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.

qllc dlsw

To enable data-link switching plus (DLSw+) over Qualified Logical Link Control (QLLC), use the **qllc dlsw** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

qllc dlsw {**subaddress** *subaddress* | **pvc** *pvc-low* [*pvc-high*]} [**vmac** *vmacaddr poolsize*] [**partner** *partner-macaddr*] [**sap** *ssap dsap*] [**xid** *xidstring*] [**npsi-poll**]

no qllc dlsw {**subaddress** *subaddress* | **pvc** *pvc-low* [*pvc-high*]} [**vmac** *vmacaddr poolsize*] [**partner** *partner-macaddr*] [**sap** *ssap dsap*] [**xid** *xidstring*] [**npsi-poll**]

Syntax Description

subaddress *subaddress*	An X.121 subaddress.
pvc	Map one or more permanent virtual circuits (PVCs) to a particular QLLC service (in this case DLSw+). QLLC will attempt to reach the partner by sending and ID.STN.IND to DLSw+.
pvc-low	Lowest logical channel number (LCN) for a range of X.25 PVCs. Acceptable values for PVCs are decimal numbers from 1 to 4095.
pvc-high	(Optional) Highest LCN. If not specified, the range of PVCs consists of just one PVC.
vmac *vmacaddr*	(Optional) Defines either the only virtual MAC address used for DLSw+ or the lowest virtual MAC address in a pool of virtual MAC addresses.
poolsize	(Optional) Specify the number of contiguous virtual MAC addresses that have been reserved for DLSw+. If the parameter is not present, then only one virtual MAC address is available.
partner *partner-macaddr*	(Optional) Virtual MAC address to which an incoming call wants to connect. The **qllc dlsw** command must be repeated for each different partner. Each partner is identified by a unique subaddress.
sap *ssap dsap*	(Optional) Overrides the default service access point (SAP) values (04) for a Token Ring connection. *dsap* refers to the partner's SAP address; *ssap* applies to the virtual MAC address that corresponds to the X.121 device.
xid *xidstring*	(Optional) Exchange identification (XID) format 0 type 2 string.
npsi-poll	(Optional) Inhibits forwarding a null XID on the X.25 link. Instead the Cisco IOS software will send a null XID response to the device that sent the null XID command.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Any incoming call whose X.121 destination address matches the router's X.121 address and this subaddress will be dispatched to DLSw+ (with an ID.STN IND). If a router is providing several QLLC services, different subaddresses must be used to discriminate between them. Subaddresses can be used even if a remote X.25 device is not explicitly mapped to a specific virtual MAC address. This is most useful when PU 2.1 devices are connecting to a host because the X.25 device's control point name and network name are used to validate the connection, rather than some virtual MAC address. The subaddress is optional. If no subaddress is provided, any incoming call that matches the router's X.121 address will be dispatched to DLSw+. On outgoing calls the subaddress is concatenated to the interface's X.121 address.

When DLSw+ receives a Can You Reach inquiry about a virtual MAC address in the pool, the QLLC code will attempt to set up a virtual circuit to the X.121 address that maps to the virtual MAC address specified. If an incoming call is received, QLLC sends an ID.STN.IND with a virtual MAC address from the pool to DLSw+. If there is no virtual MAC address, then the **x25 map qllc** or **x25 pvc qllc** command must provide a virtual MAC address.

The **npsi-poll** keyword is needed to support PU 2.0 on the partner side that wants to connect to a front-end processor (FEP) on the X.25 side. In a Token Ring or DLSw+ environment, the PU 2.0 will send a null XID to the FEP. If the software forwards this null XID to an X.25 attached FEP, the FEP will assume that it is connecting to PU2.1, and will break off the connection when the PU 2.0 next sends an XID Format 0 Type 2.

Examples

The following commands assign virtual MAC address 1000.0000.0001 to a remote X.25-attached 3174, which is then mapped to the X.121 address of the 3174 (31104150101) in an X.25-attached router:

```
interface serial 0
 x25 address 3110212011
 x25 map qllc 1000.000.0001 31104150101
 qllc dlsw partner 4000.1161.1234
```

qllc largest-packet

To indicate the maximum size of the Systems Network Architecture (SNA) packet that can be sent or received on an X.25 interface configured for Qualified Logical Link Control (QLLC) conversion, use the **qllc largest-packet** command in interface configuration mode. To restore the default largest packet size, use the **no** form of this command.

qllc largest-packet *virtual-mac-addr max-size*

no qllc largest-packet *virtual-mac-addr max-size*

Syntax Description

virtual-mac-addr	Virtual MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
max-size	Maximum size, in bytes, of the SNA packet that can be sent or received on the X.25 interface configured for QLLC conversion. This value must agree with the value configured in the remote SNA device. The valid range is from 0 to 1024.

Defaults

Maximum size is 265 bytes.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNA packets that are larger than the largest value allowed on the X.25 connection and are received on the Logical Link Control, type 2 (LLC2) interface are segmented before being sent on the X.25 interface. When a segmented packet is received on the X.25 interface, it is passed immediately to the LLC2 interface, and no effort is made to wait for the segment to be completed.

When the remote X.25 device has a limit on the maximum total length of recombined X.25 segments it will support, you can use the **qllc largest-packet** command to ensure that the length is not exceeded. For example, a device whose maximum SNA packet size is limited to 265 bytes might not be able to handle a series of X.25 packets that it has to recombine to make a 4, 8, or 17 KM SNA packet, such as one often encounters in an LLC2 environment.

You use the **qllc largest-packet** command in conjunction with the **x25 map qllc** and **qllc srb** commands.

Note Do not configure the maximum SNA packet size on an X.25 interface to be larger than the maximum SNA packet size allowed on the LLC2 interface.

Consult your IBM documentation to set the maximum packet size on the remote X.25 device.

Examples

In the following example, the maximum packet size that has been established for the virtual circuit is used as the maximum packet size that can be sent or received on the X.25 interface:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
!
 qllc partner 0100.0000.0001 4000.0101.0132
 qllc xid 0100.0000.0001 01720001
 qllc largest-packet 0100.0000.0001 521
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc npsi-poll

To enable a connection between a physical unit (PU) 2 on the LAN side and a front-end processor (FEP) running Network Control Program (NCP) Packet Switching Interface (NPSI) on the X.25 side, use the **qllc npsi-poll** command in interface configuration mode. To disable this capability, use the **no** form of this command.

qllc npsi-poll *virtual-mac-addr*

no qllc npsi-poll *virtual-mac-addr*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **qllc npsi-poll** command is necessary only when the upstream device is a front-end processor (FEP) running NPSI and the downstream device is a PU 2.

This command is necessary because in a Token Ring or remote source-route bridging (RSRB) environment the LAN attached devices start up by sending a null exchange ID packet upstream. If the Cisco IOS software forwards this null exchange identification (XID) to an X.25-attached FEP, the FEP responds as if it were connecting to a PU2.1 device, and breaks the connection when the PU 2 next sends an XID Format 0 Type 2. The **qllc npsi-poll** command intercepts any null XID packet that the software receives on the LAN interface, and returns a null XID response to the downstream device. It continues to allow XID Format 3 and XID Format 0 packets through the X.25 device.

Examples

The following example facilitates a connection between a FEP running NPSI and a downstream PU 2.0:

```
qllc npsi-poll 0100.0000.0001
```

Related Commands

Command	Description
qllc srb	Enables Qualified Logical Link Control (QLLC) conversion on a serial interface configured for X.25 communication.
sdlc qllc-prtnr	Establishes correspondence between an Synchronous Data Link Control (SDLC) and QLLC connection.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc partner

To enable a router configured for Qualified Logical Link Control (QLLC) conversion to open a connection to the local Token Ring device on behalf of the remote X.25 device when an incoming call is received, use the **qllc partner** command in interface configuration mode. To disable this capability, use the **no** form of this command.

qllc partner *virtual-mac-addr mac-addr*

no qllc partner *virtual-mac-addr mac-addr*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
mac-addr	48-bit MAC address of the Token Ring host that will communicate with the remote X.25 device.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the Cisco IOS software receives an incoming call from the designated X.121 address, it opens a Logical Link Control, type 2 (LLC2) connection with the device at the given MAC address. Both the MAC address of the Token Ring device and the virtual MAC address for the remote X.25 device with which it is to communicate are required in order for the software to initiate connections with the Token Ring device. This allows the Token Ring host to be permanently ready to accept a connection rather than requiring operator action at the host to initiate the connection with the X.25 device.

You must issue the **qllc partner** command for each remote X.25 device that will communicate with the local Token Ring host through this interface.

You use the **qllc partner** command in conjunction with the **x25 map qllc** and **qllc srb** commands.

Examples

In the following example, the **qllc partner** command is used to associate the virtual MAC address 0100.0000.0001, as defined in the previous **x25 map qllc** entry, with the MAC address of the Token Ring host that will communicate with the remote X.25 device:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
 qllc partner 0100.0000.0001 4000.0101.0132
 qllc xid 0100.0000.0001 01720001
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
sdlc qllc-prtnr	Establishes correspondence between an SDLC and QLLC connection.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc sap

To associate a service access point (SAP) value other than the default SAP value with a serial interface configured for X.25 communication and Qualified Logical Link Control (QLLC) conversion, use the **qllc sap** command in interface configuration mode. To return this SAP value to its default state, use the **no** form of this command.

qllc sap *virtual-mac-addr ssap dsap*

no qllc sap *virtual-mac-addr ssap dsap*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
ssap	Source SAP value. It can be a decimal number in the range from 2 to 254. The default is 4.
dsap	Destination SAP value. It can be a decimal number in the range from 2 to 254. The default is 4.

Defaults

The default source SAP value is 4.
The default destination SAP value is 4.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A SAP can be viewed as a port through which a higher-layer application can communicate with its counterpart (peer) operating on another system. Although the standard SAP value for IBM devices is 4, other values are allowed.

You use the **qllc sap** command in conjunction with the **x25 map qllc** and **qllc srb** interface configuration commands.

Examples

In the following example, source SAP and destination SAP values of 2 are specified for the remote X.25 device at the X.121 address 31370054065:

```
interface serial 0
 x25 map qllc 31370054065 4000.0122.0001
 qllc srb 9 100
qllc sap 4000.0122.0001 02 02
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc srb

To enable Qualified Logical Link Control (QLLC) conversion on a serial interface configured for X.25 communication, use the **qllc srb** command in interface configuration mode. To disable QLLC conversion on the interface, use the **no** form of this command.

qllc srb *virtual-mac-addr srn trn*

no qllc srb *srn trn*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. It must be 1 to 15 digits long.
srn	Source ring number. This value defines a virtual ring for all of the remote X.25 devices attached to the QLLC interface.
trn	Target ring number. It must be a virtual ring group that has been defined with the **source-bridge sdllc-local-ack** global configuration command.

Defaults

QLLC conversion is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Any number of QLLC conversion connections using the same X.25 serial interface can share a source ring. However, this source ring must be a unique hexadecimal ring number within the source-bridged network.

If the router has only one Token Ring interface and is bridging from the remote X.25 devices to this interface, then the *trn* value is the number of the ring on that Token Ring interface. If the router has several Token Ring interfaces and interconnects them by means of the **source-bridge sdllc-local-ack** command, then the *trn* value is the number of that virtual ring group, as assigned using the **source-bridge sdllc-local-ack**

Use the **qllc srb** command to associate the ring number and bridge number that have been assigned to the interface with a virtual ring group of which the interface will be a part. The serial interface appears to be a ring, or source ring number, on a source-route bridge network, and ties in to the virtual ring group, or target ring number. The target ring number provides access to other real rings that have been designated using the **source-bridge** global configuration command. Note that you can configure QLLC conversion on a router containing no Token Ring interface cards, such as a router connecting a serial-attached device to an X.25 public data network (PDN).

The **qllc srb** command automatically turns on the Logical Link Control, type 2 (LLC2) process with default values. To change any of the LLC2 parameters (described in the "LLC2 and Synchronous Data Link Control (SDLC) Commands" chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*.), apply their values to the serial interface that has been configured for QLLC conversion. This is done on the serial interface, even though LLC2 does not run on the serial interface, but on the virtual ring associated with the serial interface.

You use the **qllc srb** command in conjunction with the **x25 map qllc** command.

Examples

In the following example, the **qllc srb** command is used to define a virtual ring number of 201 for the remote X.25 device, and an actual or virtual ring number of 100 for the Token Ring interface:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
```

Related Commands

Command	Description
source-bridge	Configures an interface for source-route bridging (SRB).
source-bridge sdllc-local-ack	Activates local acknowledgment for SDLLC sessions on a particular interface.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc xid

To associate an exchange ID (XID) value with the remote X.25 device that communicates through the Cisco IOS software using Qualified Logical Link Control (QLLC) conversion, use the **qllc xid** command in interface configuration mode. To disable XID processing for this address, use the **no** form of this command.

qllc xid *virtual-mac-addr xid*

no qllc xid *virtual-mac-addr xid*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
xid	Combined XID IDBLK and XID IDNUM you are associating with the X.25 device at this X.121 address. This hexadecimal value must be four bytes (eight digits) in length.

Defaults

XID processing is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Most QLLC installations do not need the **qllc xid** configuration command. It is needed only if the remote X.25 device is not configured to send its own XID. This is only possible for a device that is attached via a permanent virtual circuit (PVC). Even so, most devices that are connected via X.25 will send their own XIDs. Use the **qllc xid** command when the Token Ring host requires login validation for security purposes and the remote X.25 device does not send an XID. The XID value is used to reply to XID requests received on the Token Ring Logical Link Control, type 2 (LLC2) side of the connection. XID requests and responses are usually exchanged before sessions are started. The XID response to the XID request from the Token Ring host will contain the information you configure using the **qllc xid** command. The host will check the XID response it receives with the IDBLK and IDNUM parameters (configured in virtual telecommunications access method [VTAM]). If they match, the Token Ring host will initiate a session with the router. If they do not match, the host will not initiate a session with the router.

You use the **qllc xid** command in conjunction with the **x25 map qllc** and the **qllc srb** commands.

Examples

In the following example, the X.25 device at X.121 address 31104150101 must use an XID IDBLK of 017 and XID IDNUM of 20001 to access the Token Ring host whose MAC address is associated with the remote X.25 device, as applied using the sdlc partner command:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
!
 qllc partner 0100.0000.0001 4000.0101.0132
 qllc xid 0100.0000.0001 01720001
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
sdllc partner	Enables device-initiated connections for SDLLC. Must be specified for the serial interface that links to the serial line device.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

queue-list protocol bstun

To customize block serial tunnel (BSTUN) queueing priorities based on the BSTUN header, use the **queue-list protocol bstun** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

queue-list *list-number* **protocol bstun** *queue* [**gt** | **lt** *packetsize*] [**address** *bstun-group bsc-addr*]

no queue-list *list-number* **protocol bstun** *queue* [**gt** | **lt** *packetsize*] [**address** *bstun-group bsc-addr*]

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the priority list selected by the user.
queue	Enables a priority queue type: Valid **queue** keyword values and their equivalent priority queue type level are: • **high**—Priority queue type is high. • **medium**—Priority queue type is medium. • **normal**—Priority queue type is normal. • **low**—Priority queue type is low.
gt | **lt** *packetsize*	(Optional) Output interface examines header information *and* packet size and places packets with the BSTUN header that match criteria (**gt** or **lt** specified packet size) on specified output.
address *bstun-group bsc-addr*	(Optional) Output interface examines header information and Bisync address and places packets with the BSTUN header that match Bisync address on the specified output queue.

Defaults

Prioritize based on BSTUN header.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the output interface examines the header information and places packets with the BSTUN header on the output queue specified as medium.

```
queue-list 1 protocol bstun medium
```

Related Commands

Command	Description
encapsulation bstun	Configures BSTUN on a particular serial interface.

queue-list protocol ip tcp

To customize block serial tunnel (BSTUN) queueing priorities based on the TCP port, use the **queue-list protocol ip tcp** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

queue-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*

no queue-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the priority list selected by the user.
queue	Enables a priority queue type: Valid **queue** keyword values and their equivalent priority queue type level are: • **high**—Priority queue type is high. • **medium**—Priority queue type is medium. • **normal**—Priority queue type is normal. • **low**—Priority queue type is low. The default *queue* value is **normal**.
tcp-port-number	BSTUN port and priority settings are as follows: • High—BSTUN port 1976 • Medium—BSTUN port 1977 • Normal—BSTUN port 1978 • Low—BSTUN port 1979 Serial tunnel (STUN) port and priority settings are as follows: • High—STUN port 1994 • Medium—STUN port 1990 • Normal—STUN port 1991 • Low—STUN port 1992

Defaults

The default *queue* value is **normal**.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, queueing priority for address C1 using priority list 1 is set to high. A priority queue of high is assigned to BSTUN port 1976.

```
queue-list bstun high address 1 c1
queue-list 1 protocol ip high 1976
```

Related Commands

Command	Description
encapsulation bstun	Configures BSTUN on a particular serial interface.

response-time group

To configure a client subnet group for response-time measurements, use the **response-time group** TN3270 server configuration command. To remove a client subnet group from response-time measurements, use the **no** form of this command.

response-time group *name* [**bucket boundaries** *t1 t2 t3 t4*] [**multiplier** *m*]

no response-time group *name*

Syntax Description

name	Alphanumeric string for the response-time group name. The maximum length of the name is 24 characters. Lower or uppercase letters can be used.
bucket boundaries *t1 t2 t3 t4*	(Optional) Unsigned 32-bit quantity that defines a bucket boundary in tenths of seconds. For other types of client groups, the bucket boundaries and multiplier values are fixed to the following defaults: • Bucket boundaries—10, 20, 50, 100 • Multiplier—30
multiplier *m*	(Optional) Number, in the range from 1 to 5760, which when multiplied by the sample interval of 20 seconds, determines the collection interval.

Defaults

Bucket boundaries and the multiplier value are fixed to the following defaults:

- Bucket boundaries—10, 20, 50, 100
- Multiplier—30

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Multiple response-time groups can be configured within the scope of available memory. When this command is used, up to 1024 IP subnets can be defined per response-time group with the **client ip** command. All TN3270 clients belonging to subnets configured within a specific response-time group are added to the response-time group when they connect as clients.

If the IP address and mask combination already exists within any response-time group, the following error message is displayed:

```
Subnet 10.1.1.0 255.255.255.248 already exists in client group MYSUBNET
```

Examples

In the following example, the response-time group MYSUBNET is configured:

```
tn3270-server
response-time group MYSUBNET bucket boundaries 15 25 60 120 multiplier 35
 client ip 10.1.1.0 255.255.255.248
 client ip 10.1.2.0 255.255.255.248
```

Related Commands

Command	Description
client ip	Adds an IP subnet to a client subnet response-time group.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

rif

To enter static source-route information into the Routing Information Field (RIF) cache, use the **rif** command in global configuration mode. If a Token Ring host does not support the use of IEEE 802.2 TEST or XID datagrams as explorer packets, you may need to add static information to the RIF cache of the router. To remove an entry from the cache, use the **no** form of this command.

rif *mac-address rif-string* {*interface-name* | **ring-group** *ring*}

no rif *mac-address rif-string* {*interface-name* | **ring-group** *ring*}

Syntax Description

mac-address	12-digit hexadecimal string written as a dotted triple of four-digit hexadecimal numbers; for example, 0010.0a00.20a6.
rif-string	Series of 4-digit hexadecimal numbers separated by a period (.). This RIF string is inserted into the packets sent to the specified MAC address.
interface-name	Interface name (for example, tokenring 0) that indicates the origin of the RIF.
ring-group	Specifies the origin of the RIF is a ring group.
ring	Ring group number that indicates the origin of the RIF. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.

Defaults

No static source-route information is entered.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must specify either an interface name or a ring group number to indicate the origin of the RIF. You specify an interface name (for example, tokenring 0) with the *interface-name* argument, and you specify a ring group number with the **ring-group** *ring* keyword and argument. The ring group number must match the number you specified with the **source-bridge ring-group** command. Ring groups are explained in the “Configuring Source-Route Bridging” chapter of the *Bridging and IBM Networking Configuration Guide*.

Using the command **rif** *mac-address* without any other arguments puts an entry into the RIF cache indicating that packets for this MAC address should not have RIF information.

Do not configure a static RIF with any of the *all rings* type codes. Doing so causes traffic for the configured host to appear on more than one ring and leads to unnecessary congestion.

Note Input to the **source-bridge** interface configuration command is in decimal format. RIF displays and input are in hexadecimal format, and IBM source-route bridges use hexadecimal for input. It is essential that bridge and ring numbers are consistent for proper network operation. This means you must explicitly declare the numbers to be hexadecimal by preceding the number with 0x, or you must convert IBM hexadecimal numbers to a decimal equivalent when entering them. For example, IBM hexadecimal bridge number 10 would be entered as hexadecimal number 0x10 or decimal number 16 in the configuration commands. In the displays, these commands always will be in decimal.

Examples

The following example configuration sets up a static RIF:

```
! insert entry with MAC address 1000.5A12.3456 and RIF of
! 0630.0081.0090 into RIF cache
rif 1000.5A12.3456 0630.0081.0090 tokenring 0
```

Related Commands

Command	Description
multiring	Enables collection and use of RIF information.
source-bridge ring-group	Defines or removes a ring group from the configuration.

rif timeout

To determine the number of minutes an inactive Routing Information Field (RIF) entry is kept, use the **rif timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

rif timeout *minutes*

no rif timeout

Syntax Description

minutes	Number of minutes an inactive RIF entry is kept. The value must be greater than 0. Default is 15 minutes.

Defaults

15 minutes

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A RIF entry is cached based on the MAC address and the interface.

RIF information is maintained in a cache whose entries are aged. A RIF entry can be aged out even if there is active traffic, but the traffic is fast or autonomously switched. Until a RIF entry is removed from the cache, no new information is accepted for that RIF entry.

A RIF entry is refreshed only if a RIF field of an incoming frame is identical to the RIF information of the RIF entry in the cache.

Examples

The following example changes the timeout period to 5 minutes:

```
rif timeout 5
```

Related Commands

Command	Description
clear rif-cache	Clears the entire RIF cache.
rif validate-enable	Enables RIF validation for entries learned on an interface (Token Ring or FDDI).
show rif	Displays the current contents of the RIF cache.

rif validate-age

To define the validation time when the Cisco IOS software is acting as a proxy for NetBIOS NAME_QUERY packet or for explorer frames, use the **rif validate-age** command in global configuration mode.

rif validate-age *seconds*

no rif validate-age *seconds*

Syntax Description

seconds	Interval, in seconds, at which a proxy is sent. The valid range is any number greater than 0. Default is 2 seconds.

Defaults

2 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the timer expires before the response is received, the Routing Information Field (RIF) entry or the NetBIOS cache entry is marked as invalid and is flushed from the cache table when another explorer or NAME_QUERY packet is received.

Examples

The following example specifies the interval at which a proxy is sent to be 3 seconds:

```
rif validate-age 3
```

Related Commands

Command	Description
rif	Enters static source-route information into the RIF cache.
rif timeout	Determines the number of minutes an inactive RIF entry is kept.

rif validate-enable

To enable Routing Information Field (RIF) validation for entries learned on an interface (Token Ring or Fiber Distributed Data Interface [FDDI]), use the **rif validate-enable** command in global configuration mode. To disable the specification, use the **no** form of this command.

rif validate-enable

no rif validate-enable

Syntax Description

This command has no arguments or keywords.

Defaults

RIF validation is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A RIF validation algorithm is used for the following cases:

- To decrease convergence time to a new source-route path when an intermediate bridge goes down.
- To keep a valid RIF entry in a RIF cache even if a RIF entry is not refreshed either because traffic is fast or autonomously switched, or because there is no traffic.

A directed IEEE TEST command is sent to the destination MAC address. If a response received in the time specified by the **rif validate-age** command, the entry is refreshed and is considered valid. Otherwise, the entry is removed from the cache. To prevent sending too many TEST commands, any entry that has been refreshed in fewer than 70 seconds is considered valid.

Validation is triggered as follows:

- When a RIF entry is found in the cache.
- When a RIF field of an incoming frame and the RIF information of the RIF entry is not identical. If, as the result of validation, the entry is removed from the cache, the RIF field of the next incoming frame with the same MAC address is cached.
- When the RIF entry is not refreshed for the time specified in the **rif timeout** command.

Note If the RIF entry has been in the RIF cache for 6 hours, and has not been refreshed for the time specified in the **rif timeout** command, the entry is removed unconditionally from the cache.

Note The **rif validate-enable** commands have no effect on remote entries learned over RSRB.

Examples

The following example enables RIF validation:

```
rif validate-enable
```

Related Commands

Command	Description
rif timeout	Determines the number of minutes an inactive RIF entry is kept.
rif validate-age	Defines the validation time when the Cisco IOS software is acting as a proxy for NetBIOS NAME_QUERY packet or for explorer frames.
rif validate-enable-age	Enables RIF validation for stations on a source-route bridge network that do not respond to an IEEE TEST command.
rif validate-enable-route-cache	Enables synchronization of the RIF cache with the protocol route cache.

rif validate-enable-age

To enable Routing Information Field (RIF) validation for stations on a source-route bridge network that do not respond to an IEEE TEST command, use the **rif validate-enable-age** command in global configuration mode. To disable the specification, use the **no** form of this command.

rif validate-enable-age

no rif validate-enable-age

Syntax Description

This command has no arguments or keywords.

Defaults

RIF validation is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must first issue the **rif validate-enable** command.

When this command is enabled, a RIF entry is not removed from the cache even if it becomes invalid. If the entry is refreshed, it becomes valid again.

If a RIF field of an incoming frame and the RIF information of the invalid RIF entry are not identical, the old RIF information is replaced by the new information.

Note The **rif validate-enable** commands have no effect on remote entries learned over remote source-route bridging (RSRB).

Examples

The following example enables RIF validation:

```
rif validate-enable-age
```

Related Commands

Command	Description
rif validate-enable	Enables RIF validation for entries learned on an interface (Token Ring or FDDI).

rif validate-enable-route-cache

To enable synchronization of the Routing Information Field (RIF) cache with the protocol route cache, use the **rif validate-enable-route-cache** command in global configuration mode. To disable the specification, use the **no** form of this command.

rif validate-enable-route-cache

no rif validate-enable-route-cache

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a RIF entry is removed from the RIF cache, or the RIF information in the RIF entry is changed, the protocol route caches are synchronized with the RIF cache.

Note The **rif validate-enable** commands have no effect on remote entries learned over remote source-route bridging (RSRB).

Examples

The following example synchronizes the RIF cache with the protocol route cache:

```
rif validate-enable-route-cache
```

Related Commands

Command	Description
rif validate-enable	Enables RIF validation for entries learned on an interface (Token Ring or FDDI).

rsrb remote-peer lsap-output-list

To define service access point (SAP) filters by local SAP (LSAP) address on the remote source-route bridging WAN interface, use the **rsrb remote-peer lsap-output-list** command in global configuration mode. To remove a SAP filter on the remote source-route bridging (RSRB) WAN interface, use the **no** form of this command.

rsrb remote-peer *ring-group* {**tcp** *ip-address* | **fst** *ip-address* | **interface** *name*} **lsap-output-list** *access-list-number*

no rsrb remote-peer *ring-group* {**tcp** *ip-address* | **fst** *ip-address* | **interface** *name*} **lsap-output-list** *access-list-number*

Syntax Description

ring-group	Virtual ring number of the remote peer.
tcp	TCP encapsulation.
ip-address	IP address.
fst	Fast Sequenced Transport (FST) encapsulation.
ip-address	IP address.
interface	Direct encapsulation.
name	Interface name.
access-list-number	Number of the access list.

Defaults

No filters are assigned.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies SAP filters by LSAP address:

```
rsrb remote-peer 1000 tcp 10.108.2.30 lsap-output-list 201
```

Related Commands

Command	Description
priority-list protocol	Establishes queueing priorities based on the protocol type.

Command	Description
sap-priority	Defines a priority list on an interface.
sap-priority-list	Defines a priority list.

rsrb remote-peer netbios-output-list

To filter packets by NetBIOS station name on a remote source-route bridging WAN interface, use the **rsrb remote-peer netbios-output-list** command in global configuration mode. To remove a filter on an remote source-route bridging (RSRB) WAN interface, use the **no** form of this command.

rsrb remote-peer *ring-group* {**tcp** *ip-address* | **fst** *ip-address* | **interface** *type*} **netbios-output-list host** *name*

no rsrb remote-peer *ring-group* {**tcp** *ip-address* | **fst** *ip-address* | **interface** *type*} **netbios-output-list host** *name*

Syntax Description

ring-group	Virtual ring number of the remote peer.
tcp	TCP encapsulation.
fst	Fast Sequenced Transport (FST) encapsulation.
ip-address	IP address.
interface	Direct encapsulation.
type	Interface name.
name	Name of a NetBIOS access filter previously defined with one or more **netbios access-list host** global configuration commands.

Defaults

No filter is assigned.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example filters packets by NetBIOS station name:

```
rsrb remote-peer 1000 tcp 10.108.2.30 netbios-output-list host engineering
```

Related Commands

Command	Description
netbios access-list host	Assigns the name of the access list to a station or set of stations on the network. The NetBIOS station access list contains the station name to match, along with a permit or deny condition.
priority-list protocol	Establishes queueing priorities based on the protocol type.

Command	Description
sap-priority	Defines a priority list on an interface.
sap-priority-list	Defines a priority list.

sap-priority

To define a priority list on an interface, use the **sap-priority** command in interface configuration mode. To remove a priority list on an interface, use the **no** form of this command.

sap-priority *list-number*

no sap-priority *list number*

Syntax Description

list-number	Priority list number you specified in the **sap-priority-list** command.

Defaults

No priority list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies priority list number 1:

```
sap-priority 1
```

Related Commands

Command	Description
sap-priority-list	Defines a priority list.
source-bridge	Configures an interface for source-route bridging (SRB).

sap-priority-list

To define a priority list, use the **sap-priority-list** command in global configuration mode. To remove a priority list, use the **no** form of this command.

sap-priority-list *list-number queue-keyword* [**dsap** *ds*] [**ssap** *ss*] [**dmac** *dm*] [**smac** *sm*]

no sap-priority-list *list-number queue-keyword* [**dsap** *ds*] [**ssap** *ss*] [**dmac** *dm*] [**smac** *sm*]

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the priority list.
queue-keyword	Priority queue name or a remote source-route bridge TCP port name.
dsap *ds*	(Optional) Destination service access point address. The *ds* argument is a hexadecimal number.
ssap *ss*	(Optional) Source service access point address. The *ss* argument is a hexadecimal number.
dmac *dm*	(Optional) Destination MAC address. The *dm* argument *dm* is written as a dotted triple of four-digit hexadecimal numbers.
smac *sm*	(Optional) Source MAC address. The *sm* argument *sm* is written as a dotted triple of four-digit hexadecimal numbers.

Defaults

No priority list is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To give precedence to traffic on a particular Logical Link Control, type 2 (LLC2) session, you must specify all four keywords (**dsap**, **ssap**, **dmac**, and **smac**) to uniquely identify the LLC2 session.

Examples

The following example defines priority list 1 and specifies source service access point (SSAP) and destination service access point (DSAP) addresses:

```
sap-priority-list 1 high dsap 04 ssap 04
```

sdlc address

To assign a set of secondary stations attached to the serial link, use the **sdlc address** command in interface configuration mode. To remove an assigned secondary station use the **no** form of this command.

sdlc address *hexbyte* [**echo**] [**ack-mode**] [**xid-poll**] [**switched**] [**seconly**] [**xid-passthru**] [**passive**] [**K** *number*] [**vmac** *vmac-address*]

no sdlc address *hexbyte* [**echo**] [**ack-mode**] [**xid-poll**] [**switched**] [**seconly**] [**xid-passthru**] [**passive**] [**K** *number*] [**vmac** *vmac-address*]

Syntax Description

hexbyte	Hexadecimal number (base 16) that indicates the address of the serial link. The range is from 1 to ff. If ff is configured, the **ack-mode** option must be specified.
echo	(Optional) Treats non-echo and echo Synchronous Data Link Control (SDLC) addresses as the same address.
ack-mode	(Optional) Supports applications that require local termination of an SDLC connection with address FF. This option should be used only if you use the SDLC address ff as a regular (not a broadcast) address.
xid-poll	(Optional) Configures the router to send a null exchange identification (XID) to the Token Ring-attached host device. This tells the host device to start the session.
switched	(Optional) Configures the router to send an XID to an SDLC attached device. When the device answers, then a proxy XID is sent to the peer.
seconly	(Optional) Eliminates the need for counting PU4 lines on the Network Control Program (NCP) to determine the correct poll address. Because the router is always secondary, when **seconly** is coded, the polling address will be determined by the router.
xid-passthru	(Optional) Allows the router to pass the XID through the interface in both the host and end device's direction.
passive	(Optional) Causes the router to wait before sending a Set Normal Response (SNRM) until it receives an XID from the host. This keyword is valid only when the role is primary, and it requires the **sdlc partner** command with keyword **inbound** specified.
K number	(Optional) Specifies the maximum number of information frames (I-frames) that a router can send before it expects an acknowledgment from the end device. The minimum window-size is 1 and the maximum size is 7. The default is 7.
vmac *vmac-address*	(Optional) Assigns a virtual MAC address to a specific SDLC address on an SDLC interface.

Defaults

No secondary stations are assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The SDLC address **ack-mode** option was introduced.
11.3	The command was modified to include the **switched**, **passive**, **xid-poll**, and **xid-passthru** keywords.
11.3(T)	The command was modified to include the **seconly** keyword.
12.1(5)T	The **sdlc address** and **sdlc address ff ack-mode** commands were combined. The **K** keyword was added.
12.3(7)T	The **vmac** *vmac-address* keyword and argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To assign the IBM reserved address ff as a nonbroadcast valid local address, configure the **sdlc address** interface configuration command with a hexbyte value of *ff* and specify the **ack-mode** option. To deactivate, use the **no** form of the command.

Before you can use this command, you must specify the encapsulation on the interface on which you want to enable SDLC; then, establish the router link station role. Next, assign secondary station addresses using the **sdlc address** command. The addresses are given one per line in hexadecimal (base 16).

The **sdlc address ff ack-mode** command is used to support applications that require local termination on an SDLC connection with address ff. This command should be used only if you use the SDLC address ff as a regular (not a broadcast) address.

The optional **echo** keyword is valid only for TG interfaces. When you use the **echo** keyword, the *hexbyte* argument is the non-echo SDLC address.

The optional **passive** keyword is valid only when the role is primary. When you use the **passive** keyword, the **sdlc partner** command is required with keyword **inbound** specified.

Examples

The following example shows how to configure serial interface 0 with two SDLC secondary stations attached to it through a modem-sharing device with addresses C1 and C2:

```
interface serial 0
 encapsulation sdlc
 sdlc role primary
 sdlc address c1
        sdlc address c2
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
encapsulation sdlc-primary	Configures the router as the primary SDLC station if you plan to configure the SDLLC media translation feature.
encapsulation sdlc-secondary	Configures the router as a secondary SDLC station if you plan to configure the SDLLC media translation feature.

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.
stun route address tcp	Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for serial tunnel (STUN).
sdlc role	Establishes a router to be either a primary or secondary SDLC station.

sdlc dlsw

To attach Synchronous Data Link Control (SDLC) addresses to data-link switching plus (DLSw+), use the **sdlc dlsw** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

sdlc dlsw {*sdlc-address* | **default** | **partner** *mac-address* [**inbound** | **outbound**]}

no sdlc dlsw {*sdlc-address* | **default** | **partner** *mac-address* [**inbound** | **outbound**]}

Syntax Description

sdlc-address	SDLC addresses are in hexadecimal. Multiple addresses can be assigned. The valid range is from 1 to FE.
default	Allows the user to configure an unlimited number of SDLC addresses to DLSw+.
partner *mac-address*	MAC address for default partner
inbound	(Optional) Partner will initiate connection.
outbound	(Optional) Initiate connection to partner.

Defaults

No correspondence is defined between SDLC addresses and DLSw+.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command attaches SDLC address d2 to DLSw+:

```
sdlc dlsw d2
```

The following command attaches SDLC addresses d2, d5, e3, e4, e6, b1, c3, d4, a1 and a5:

```
sdlc dlsw d2 d5 e3 e4 e6 b1 c3 d4 a1 a5
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
sdlc address	Assigns a set of secondary stations attached to the serial link.
sdlc role	Establishes the router to be either a primary or secondary SDLC station.

sdlc dte-timeout

To adjust the amount of time a DTE interface waits for the DCE to assert a Clear To Send (CTS) signal before dropping a Request To Send (RTS), use the **sdlc dte-timeout** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc dte-timeout *unit*

no sdlc dte-timeout *unit*

Syntax Description

unit	Timeout wait interval in microseconds. The valid range is from 10 to 64000. Each unit is approximately 5 microseconds. The default is 10 units (approximately 50 microseconds).

Defaults

10 units (approximately 50 microseconds)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command on an interface that is in half-duplex mode and that has been configured for DTE.

Examples

The following example sets the amount of time that the DTE waits for the DCE to assert a CTS to 100 units (approximately 500 microseconds):

```
sdlc dte-timeout 100
```

Related Commands

Command	Description
half-duplex	Specifies half-duplex mode on an Synchronous Data Link Control (SDLC) interface or on the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers.
half-duplex timer	Tunes half-duplex timers.

sdlc frmr-disable

To indicate that secondary stations on a particular serial link do not support Frame Rejects (FRMRs) or error indications, use the **sdlc frmr-disable** command in interface configuration mode. To specify that the secondary station does support FRMRs, use the **no** form of this command.

sdlc frmr-disable

no sdlc frmr-disable

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled, which means that secondary stations support FRMRs or error indications.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

FRMRs are error indications that can be sent to a Synchronous Data Link Control (SDLC) station indicating that a protocol error has occurred. Not all SDLC stations support FRMRs. If this command is enabled, when the Cisco IOS software receives an error, it drops the line by sending a disconnect request to the remote station.

Examples

In the following example, the software is set to drop the serial line when it receives a protocol error:

```
interface serial 0
 sdlc frmr-disable
```

Related Commands

Command	Description
show llc2	Displays the LLC2 connections active in the router.

sdlc holdq

To control the maximum number of packets that can be held in a buffer before being sent to a remote Synchronous Data Link Control (SDLC) station, use the **sdlc holdq** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc holdq *address queue-size*

no sdlc holdq *address queue-size*

Syntax Description

address	SDLC address for which you are specifying a queue size.
queue-size	Local send window size. The minimum is 1 packet. No maximum value has been established. The default is 200 packets.

Defaults

200 packets

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is particularly useful with the SDLC Logical Link Control. Cisco (SDLLC) feature that allows a SDLC Logical Link Control. Cisco (SDLLC)-speaking Systems Network Architecture (SNA) station on a Token Ring to communicate with an SDLC-speaking SNA station on a serial link. Frame sizes and window sizes on Token Rings are often much larger than those acceptable for serial links. The fact that serial links are often much slower than Token Rings often makes this problem worse. Therefore, temporary backlogs can exist in periods of high data transfer from the Token Ring station to the serial station. A buffer creates a holding place for backlogged frames waiting to be sent on the serial link. This command is specified for each SDLC address, and therefore, for each SDLC secondary station on the serial link.

Examples

The following example shows how to change the output hold queue length to 30 frames on an SDLC station of address C1 off serial interface 0:

```
interface serial 0
 encapsulation sdlc-primary
 sdlc address c1
 sdlc holdq c1 30
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc k

To set the window size in order to control the maximum number of information frames the Cisco IOS software sends before it must stop sending and wait for an acknowledgment from the receiving router, use the **sdlc k** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc k *window-size*

no sdlc k *window-size*

Syntax Description

window-size	Local send window size. The minimum is one frame. The maximum is seven frames, which is the default.

Defaults

Seven frames

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the Cisco IOS software is communicating with Synchronous Data Link Control (SDLC), it must have a parameter that controls the maximum number of information frames it will send before it must stop sending and wait for an acknowledgment. The **k** parameter keyword controls this window of acceptable frames. Use this command in conjunction with the **sdlc n1** command to create a balance between frame checking and network performance.

Examples

In the following example, the software can send up to five frames before it must receive an acknowledgment:

```
! enter a global command, if you have not already
interface tokenring 0
!send up to 5 frames, then wait for acknowledgment
 sdlc k 5
```

Related Commands

Command	Description
sdlc n1	Controls the maximum size of an incoming frame.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc line-speed

To enable adaptive Synchronous Data Link Control (SDLC) T1, use the **sdlc line-speed** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

sdlc line-speed *rate*

no sdlc line-speed *rate*

Syntax Description

rate	Clock rate in bits per second.

Defaults

No default rate

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used to calculate the adjusted SDLC T1 value. The adjusted T1 is used to compensate for the delay between the time the system software passes a packet to the microcode, and the time the packet is actually sent out on the line. For a DCE device, this should be equal to the clock rate on the interface. For a DTE device, it should be equal to the clock rate on the DCE device to which the DTE is connected.

Examples

In the following example, the SDLC line-speed rate is set to rate:

```
sdlc line-speed rate
```

Related Commands

Command	Description
sdlc n2	Determines the number of times that the Cisco IOS software resends a frame before terminating the SDLC session.
sdlc t1	Controls the amount of time the Cisco IOS software waits for an acknowledgment to a frame or sequence of frames.

sdlc n1

To control the maximum size of an incoming frame, use the **sdlc n1** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc n1 *bit-count*

no sdlc n1 *bit-count*

Syntax Description

bit-count	Number indicating bit size. Frames that exceed this size are rejected. The minimum is 1 bit. The maximum value depends on the configured maximum maximum transmission unit (MTU) value for the interface. The default is 12000 bits.

Defaults

12000 bits

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use with the **sdlc k** command to reduce network overhead while continuing to check the sending of frames.

The formula for determining the maximum allowed value for the *bit-count* argument is the maximum MTU value of the interface + 2 bytes (for the Synchronous Data Link Control [SDLC] header) multiplied by 8 (to convert from bytes to bits). For example, if the maximum MTU of the interface is 1500 bytes, then the largest value for the *bit-count* argument is (1500 + 2) * 8 = 12016 bits. Usually, the default maximum MTU size is 1500 bytes, but it can be configured as high as 18,000 bytes.

Examples

In the following example, the Cisco IOS software rejects frames larger than 10,000 bits:

```
interface serial 0
 sdlc n1 10000
```

Related Commands

Command	Description
sdlc k	Sets the window size in order to control the maximum number of information frames the Cisco IOS software sends before it must stop sending and wait for an acknowledgment from the receiving router
show llc2	Displays the LLC2 connections active in the router.

sdlc n2

To determine the number of times that the Cisco IOS software resends a frame before terminating the Synchronous Data Link Control (SDLC) session, use the **sdlc n2** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc n2 *retry-count*

no sdlc n2 *retry-count*

Syntax Description

retry-count	Number of retry attempts. When this number is exceeded, the SDLC station terminates its session with the other station. The minimum is 1 and the maximum is 255. The default is 20 retries.

Defaults

20 retries

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **sdlc n2** command with the **sdlc t1** command to reduce network overhead while continuing to check the sending of data.

Examples

In the following example, the software is set to drop an SDLC station after five unsuccessful attempts to receive an acknowledgment for a frame:

```
interface serial 0
 sdlc n2 5
```

Related Commands

Command	Description
sdlc t1	Controls the amount of time the Cisco IOS software waits for an acknowledgment to a frame or sequence of frames.
show llc2	Displays the LLC2 connections active in the router.

sdlc partner

To specify the destination address with which a Logical Link Control (LLC) session is established for the Synchronous Data Link Control (SDLC) station, use the **sdlc partner** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

sdlc partner *mac-address sdlc-address* {**inbound** | **outbound**}

no sdlc partner *mac-address sdlc-address* {**inbound** | **outbound**}

Syntax Description

mac-address	The 48-bit MAC address of the Token Ring host.
sdlc-address	SDLC address of the serial device that will communicate with the Token Ring host. The valid range is from 1 to FE.
inbound	Prevents the router from sending proxy exchange identification (XID)s to the remote end station on behalf of the station specified. The remote end station must initiate the connection. When the router is configured for SDLC role secondary, the default is inbound (the router does not send proxy XIDs until it is polled). The **inbound** keyword is required if you want the router to wait before sending an SNRM until it receives an XID from the host. See the **passive** keyword on the **sdlc address** command for more details.
outbound	Causes the router to send proxy XIDs to the partner end station. If the remote end station responds, then (for physical unit [PU] 2.1 local devices) a NULL XID is sent on the SDLC line. The default behavior for SDLC role primary is outbound, and for SDLC role secondary is inbound.

Defaults

No partner is defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
11.2	The following keywords were added: • **inbound** • **outbound**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **inbound** keyword prevents unwanted messages on the host operator console from inbound XIDs to inactive virtual telecommunications access method (VTAM) Switched Major Nodes. It directs SDLC to not send Test or XID frames to the host, front-end processor (FEP), or 3172 even after the connection to a downstream PU2 is complete. The **inbound** keyword is required for System88 support.

Examples

The following example establishes the correspondence between an SDLC and Qualified Logical Link Control (QLLC) connection:

```
sdlc partner 1000.5aed.1f53 d2 inbound
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
sdlc address	Assigns a set of secondary stations attached to the serial link.
sdlc dlsw	Attaches SDLC addresses to data-link switching plus (DLSw+).
sdlc vmac	Configures a MAC address for the serial interface.

sdlc poll-limit-value

To control how many times a single secondary station can be polled for input before the next station must be polled, use the **sdlc poll-limit-value** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc poll-limit-value *count*

no sdlc poll-limit-value *count*

Syntax Description

count	Number of times the Cisco IOS software can poll one secondary station before proceeding to the next station. The valid range is from 1 through 10. The default is 1.

Defaults

1 time

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

As is typical for the primary station of an Synchronous Data Link Control (SDLC) connection, if a secondary station sends its full possible window of input to the primary router or access server, the Cisco IOS software immediately will re-poll the same secondary for more data in an attempt to capture the complete transaction at one time. The **sdlc poll-limit-value** command indicates how many times this can happen before the next station in the poll loop must be polled.

Increasing the value allows for smoother transaction processing but can delay polling of other stations or giving output to other stations.

Examples

The following example specifies that the router can be polled two times before the next station in the poll list must be polled:

```
! enter a global command, if you have not already
interface serial 4
 no ip address
! use stun encapsulation
encapsulation stun
! establish stun group 4 on interface serial 4
 stun group 4
 stun sdlc-role primary
```

```
! poll the router up to two times before polling the next station
 sdlc poll-limit-value 2
```

Related Commands

Command	Description
sdlc poll-pause-timer	Controls how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc poll-pause-timer

To control how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface, use the **sdlc poll-pause-timer** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc poll-pause-timer *milliseconds*

no sdlc poll-pause-timer *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) that the software waits before sending the poll frame to a single serial interface. This is a number in the range from 1 to 10000. The default is 10 ms.

Defaults

10 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

As is typical for the primary station of a Synchronous Data Link Control (SDLC) connection, the software generates polls periodically to each of the secondary stations to solicit their input. After polling each station on a single serial interface, the software will pause before beginning to poll the next station.

Because the secondaries cannot send data until they are polled, increasing this timer value can increase response time to the users. However, making this value too small can flood the serial link with unneeded polls and require the secondary stations to spend wasted CPU time processing them.

Examples

In the following example, the software pauses 2000 ms before sending a series of poll frames through serial interface 4:

```
! enter a global command, if you have not already
interface serial 4
no ip address
! use STUN encapsulation
 encapsulation stun
! establish stun group 4 on interface serial 4
 stun group 4
!
 stun sdlc-role primary
```

```
! wait 2000 milliseconds before sending each series of poll frames
 sdlc poll-pause-timer 2000
```

Related Commands

Command	Description
sdlc poll-limit-value	Controls how many times a single secondary station can be polled for input before the next station must be polled.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc poll-wait-timeout

To specify the interval the Cisco IOS software will wait for polls from a primary node before timing out that connection when the router has been configured for local acknowledgment and some form of Synchronous Data Link Control (SDLC) communication (SDLLC or serial tunnel [STUN], for example), use the **sdlc poll-wait-timeout** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc poll-wait-timeout *milliseconds*

no sdlc poll-wait-timeout *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software will wait for a poll from the primary station before timing out the connection to the primary station. The minimum is 10 ms and the maximum is 64000 ms. The default is 10000 ms.

Defaults

10000 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be used on an interface that has been configured as a secondary node, but is not to be used on an interface that has been configured as a primary node.

In a locally acknowledged multidrop environment, the polls the primary node sends to the router can be delayed because the primary node is busy polling other secondary nodes. In such situations, this command can be used to extend the timeout, thus reducing the likelihood the Cisco IOS software times out the connection to the primary node.

Examples

The following example specifies that the local software will wait an interval of 63,000 ms for a poll from a primary station before timing out:

```
! sample stun peer-name global command
stun peer-name 10.136.134.86
! sample protocol-group command
stun protocol-group 4 sdlc
!
interface serial 0
! sample ip address command
```

```
 no ip address
! sample encapsulation stun command
 encapsulation stun
! place interface serial0 in previously defined STUN group 4
 stun group 4
! must enter the next command to use the sdlc poll-wait-timeout command
 stun sdlc-role secondary
! set timeout period for polls from primary station to 63000 milliseconds.
 sdlc poll-wait-timeout 63000
! list the addresses of the sdlc stations on the link
 sdlc address C1
 sdlc address C2
! provide stun route command
 stun route address C2 tcp 10.136.134.58
 stun route address C1 tcp 10.136.134.58
```

Related Commands

Command	Description
sdlc poll-limit-value	Controls how many times a single secondary station can be polled for input before the next station must be polled.
sdlc poll-pause-timer	Controls how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface.

sdlc qllc-prtnr

To establish correspondence between a Synchronous Data Link Control (SDLC) and Qualified Logical Link Control (QLLC) connection, use the **sdlc qllc-prtnr** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

sdlc qllc-prtnr *virtual-mac-address sdlc-address*

no sdlc qllc-prtnr *virtual-mac-address sdlc-address*

Syntax Description

virtual-mac-address	The virtual MAC address in the form *h.h.h.*
sdlc-address	SDLC address in hexadecimal. The valid range is from 1 to FE.

Defaults

No correspondence is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example establishes the correspondence between an SDLC and QLLC connection:

```
sdlc qllc-prtnr 4000.0122.0001 c1
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc role

To establish the router to be either a primary or secondary Synchronous Data Link Control (SDLC) station, use the **sdlc role** command in interface configuration mode. To cancel the designation, use the **no** form of this command.

sdlc role {**none** | **primary** | **secondary** | **prim-xid-poll**}

no sdlc role {**none** | **primary** | **secondary** | **prim-xid-poll**}

Syntax Description

none	Establishes the router as either a primary or secondary station, depending on the end stations.
primary	Establishes the router as a primary station.
secondary	Establishes the router as a secondary station.
prim-xid-poll	Establishes the router as a primary station when the end station is configured as a secondary NT2.1.

Defaults

No default role is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the role is **none**, the router can be either primary or secondary, depending on the end stations. The SDLC end station must be configured as negotiable or primary NT2.1. When the end stations are configured as physical unit type 2 (physical unit [PU] 2), you can set the role of the interface to **primary** or **secondary**. When the end station is configured as secondary NT2.1, you must set the role of the interface to **prim-xid-poll**.

To configure an SDLC multidrop line (downstream), configure the SDLC role as follows:

- **primary** if all SDLC devices are type PU 2.0 or mixed PU 2.0 and 2.1
- **prim-xid-poll** if all devices are type PU 2.1

Examples

The following example configures the router as a primary SDLC station:

```
interface serial 2/6
 no ip address
 encapsulation sdlc
 fras map sdlc c1 serial 2/0 frame-relay 32 4 4
 sdlc role primary
 sdlc address c1
 sdlc xid c1 01700001
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.

sdlc saps

To configure Synchronous Data Link Control (SDLC)-to-Logical Link Control (LLC) sessions with respect to the source service access point (SSAP) and destination service access point (DSAP) on the LLC, use the **sdlc saps** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

sdlc saps *address ssap dsap*

no sdlc saps *address ssap dsap*

Syntax Description

address	Address of the SDLC station that will communicate with the router. Valid range is from 1 to FF.
ssap	SSAP of the partner. Valid range is from 1 to FF. The default is 04.
dsap	DSAP of the partner. Valid range is from 1 to FF. The default is 04.

Defaults

The default value for both the *ssap* and *dsap* arguments is 04.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures SDLC address 01, SSAP 08, and DSAP 08.

```
sdlc saps 01 08 08
```

sdlc sdlc-largest-frame

To indicate the largest information frame (I-frame) size that can be sent or received by the designated Synchronous Data Link Control (SDLC) station, use the **sdlc sdlc-largest-frame** command in interface configuration mode. To return to the default value, use the **no** form of this command.

sdlc sdlc-largest-frame *address size*

no sdlc sdlc-largest-frame *address size*

Syntax Description

address	Address of the SDLC station that will communicate with the router.
size	Largest frame size that can be sent or received. The default is 265 bytes.

Defaults

The default size for the largest I-frame is 265 bytes.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the Cisco IOS software can send or receive a frame as large as 265 bytes (the default) from the SDLC station at address C6. Any frames larger will be fragmented by the software.

```
interface serial 4
 sdlc sdlc-largest-frame c6 265
```

sdlc simultaneous

To enable an interface configured as a primary Synchronous Data Link Control (SDLC) station to operate in two-way simultaneous mode, use the **sdlc simultaneous** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc simultaneous [**full-datamode** | **half-datamode**]

no sdlc simultaneous [**full-datamode** | **half-datamode**]

Syntax Description

full-datamode	(Optional) Enables the primary station to send data to and receive data from the polled secondary station.
half-datamode	(Optional) Prohibits the primary station from sending data to the polled secondary station.

Defaults

Two-way simultaneous mode is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, the SDLC driver supports alternative mode. This means that in a multidrop environment, the primary station cannot send data to another secondary station until it receives a response (F bit) from the secondary station with which it is communicating.

In contrast, two-way simultaneous mode enables the interface configured as a primary SDLC station to send data to a second secondary station, even when it is receiving data from another secondary station. This capability improves utilization of a full-duplex serial line.

Examples

The following example enables all primary stations to send and receive data at the same time:

```
sdlc simultaneous full-datamode
```

The following example enables all secondary stations to send or receive data at the same time:

```
sdlc simultaneous half-datamode
```

Related Commands

Command	Description
encapsulation sdlc-primary	Configures the router as the primary SDLC station if you plan to configure the SDLLC media translation feature.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc slow-poll

To enable the slow-poll capability of the router as a primary Synchronous Data Link Control (SDLC) station, use the **sdlc slow-poll** command in interface configuration mode. To disable slow-poll capability, use the **no** form of this command.

sdlc slow-poll *seconds*

no sdlc slow-poll

Syntax Description

seconds	Amount of time in seconds. The default is 10 seconds.

Defaults

10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can use this command to improve the performance of a multidropped SDLC configuration when one or more of the secondary stations are inactive.

When slow-poll is enabled, if the router acting as a primary station detects that a secondary SDLC station is not responding, it polls that secondary SDLC station less frequently. The router spends less time waiting for the inactive secondary station to respond, thereby minimizing the performance degradation on the active secondary SDLC stations on the multidropped line.

Examples

The following example enables the slow-poll capability:

```
interface serial 0
 sdlc slow-poll
```

Related Commands

Command	Description
sdlc poll-limit-value	Controls how many times a single secondary station can be polled for input before the next station must be polled.

Command	Description
sdlc poll-pause-timer	Controls how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc snrm-timer

To specify a Set Normal Response (SNRM) timer that is different from the T1 response time, set the Synchronous Data Link Control (SDLC) SNRM timer using the **sdlc snrm-timer** command in interface configuration mode. To deactivate, use the **no** form of this command.

sdlc snrm-timer *number*

no sdlc snrm-timer *number*

Syntax Description

number	Specifies the time to wait for a reply to a SNRM frame in milliseconds, and is enabled only if the station role is primary. range is from 1 to 64000 ms, and default is the **no** form of the command.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the SNRM timer only if you want to have a unique timeout period to wait for a reply to an SNRM.

The **sdlc snrm-timer** command is used to specify the time to wait for a reply to an SNRM frame in milliseconds. This command is enabled only if the station role is primary.

Examples

The following configuration defines serial interface 0 as the primary SDLC station with two SDLC secondary stations, C1 and C2, attached to it through a modem-sharing device. SDLC simultaneous half-datamode is enabled, and the time to wait for a reply to a SNRM frame is 2500 ms.

```
interface serial 0
 encapsulation sdlc
 sdlc role primary
 sdlc address c1
 sdlc address c2
 sdlc simultaneous half-datamode
 sdlc snrm-timer 2500
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
sdlc n2	Sets the number of times the Cisco IOS software will retry an operation that has timed out.
sdlc role primary	Establishes the router as a primary SDLC station.
sdlc simultaneous	Enables an interface configured as a primary SDLC station to operate in two-way simultaneous mode.
sdlc t1	Controls the amount of time the Cisco IOS software waits for a reply.

sdlc t1

To control the amount of time the Cisco IOS software waits for an acknowledgment to a frame or sequence of frames, use the **sdlc t1** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc t1 *milliseconds*

no sdlc t1 *milliseconds*

Syntax Description

milliseconds	Number of milliseconds that the software waits. The minimum is 1 ms and the maximum is 64000 ms. The default is 3000 ms.

Defaults

3000 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an Synchronous Data Link Control (SDLC) station sends a frame, it waits for an acknowledgment from the receiver that the frame has been received. The sending station cannot wait indefinitely for a response. When the frame is sent, a timer is started. To be consistent with the original specification of SDLC, this timer is called the T1 timer and is controlled by this parameter. If this timer reaches its limit before the acknowledgment is received, the software will try again and resend the frame.

Examples

In the following example, the software waits up to 4000 ms for a reply to a frame or sequence of frames:

```
! enter a global command, if you have not already
interface tokenring 0
 sdlc t1 4000
```

Related Commands

Command	Description
sdlc n2	Determines the number of times that the Cisco IOS software resends a frame before terminating the SDLC session.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc test serial

To determine the status of end stations, use the **sdlc test serial** command in user EXEC or privileged EXEC mode. To halt the sending of the test frames, use the **sdlc test serial** command with the **stop** keyword.

sdlc test serial *number address* [*iterations* | **continuous** | **stop** | **string** *string*]

Syntax Description

number	Serial interface on which the test frame is to be sent out.
address	Synchronous Data Link Control (SDLC) address (in hexadecimal) of the end station to receive the test frame.
iterations	(Optional) Number of test frames to be sent. The valid range is from 1 to 25 frames. The default is 10 frames.
continuous	(Optional) Sends frames continuously until the **sdlc test serial** command is issued with the **stop** keyword.
stop	(Optional) Halts the sending of test frames.
string *string*	(Optional) Specifies a string of characters as data within the test frame. If this option is not specified, the default test string is ABCDEFGHIJKLMNOPQRSTUVWXYZ.

Defaults

The **sdlc test serial** command is not active.
The default number of test frames sent is 10.
The default test string is ABCDEFGHIJKLMNOPQRSTUVWXYZ.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The command will precheck for correct interface and SDLC address. The results of the test frames sent can be displayed after the frames have been sent or an **sdlc test serial** command with the **stop** keyword has been issued.

There is not a **no** form for this command.

Examples

The following are variations of the **sdlc test serial** command, followed by the response for each:

```
Router# sdlc test serial 0 c1

SDLC Test for address C1 completed
Frames sent=10 Frames received=10

Router# sdlc test serial 0 c1 255

SDLC Test for address C1 completed
Frames sent=255 Frames received=255

Router# sdlc test serial 0 C1 stop

SDLC Test for address C1 completed
Frames sent=44 Frames received=44

Router# sdlc test serial 0 c1 string Thestuffofdreams

SDLC Test for address C1 completed
Frames sent=10 Frames received=10
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc virtual-multidrop

To allow Synchronous Data Link Control (SDLC) broadcast address FF to be replicated for each of the serial tunnel (STUN) peers, so that each of the end stations receives the broadcast frame, use the **sdlc virtual-multidrop** command in interface configuration mode. To disable the SDLC broadcast feature, use the **no** form of this command.

sdlc virtual-multidrop

no sdlc virtual-multidrop

Syntax Description

This command has no arguments or keywords.

Defaults

SDLC broadcast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example allows each STUN peer to receive a broadcast frame:

```
sdlc virtual-multidrop
```

Related Commands

Command	Description
stun route address tcp	Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for STUN.

sdlc vmac

To configure a MAC address for the serial interface, use the **sdlc vmac** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

sdlc vmac *mac-address*

no sdlc vmac *mac-address*

Syntax Description

mac-address	48-bit MAC address of the Token Ring host.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command must be configured if you will configure data-link switching plus (DLSw+). The last byte of the address must be 00.

Examples

The following example specifies a MAC address for the serial interface:

```
sdlc vmac 1234.3174.0000
```

Related Commands

Command	Description
encapsulation sdlc	Configures an Synchronous Data Link Control (SDLC) interface.
sdlc dlsw	Attaches SDLC addresses to DLSw+.

sdlc xid

To specify an exchange identification (XID) value appropriate for the designated Synchronous Data Link Control (SDLC) station associated with this serial interface, use the **sdlc xid** command in interface configuration mode. To disable XID processing for this address, use the **no** form of this command.

sdlc xid *address xid*

no sdlc xid *address xid*

Syntax Description

address	Address of the SDLC station associated with this interface.
xid	XID the Cisco IOS software will use to respond to XID requests the router receives. This value must be 4 bytes (8 digits) in length and is specified with hexadecimal digits.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

XID requests and responses are usually exchanged before sessions are started. Be sure that the XID value configured in the Cisco IOS software matches the IDBLK and IDNUM parameters configured on the host. The XID response to an XID request will contain the information you configured in the **sdlc xid** command. The host will check the XID response it receives with the IDBLK and IDNUM parameters (that are configured in the virtual telecommunications access method [VTAM]). If they match, the host will initiate a session with the router. If they do not match, the host will not initiate a session.

Examples

The following example specifies an XID value of 01720002 at address C2:

```
interface serial 0
 sdlc xid c2 01720002
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.

sdlc xid-pause-timer

To control the frequency of exchange identification (XID) retries between a router and an upstream virtual telecommunications access method (VTAM), use the **sdlc xid-pause-timer** command in interface configuration mode. To restore the default timer value, use the **no** form of this command.

sdlc xid-pause-timer *time*

no sdlc xid-pause-timer *time*

Syntax Description

time	Length of time the router is to wait, in seconds, before sending the next retry XID. The valid range is from 10 to 300 seconds. The default is 10 seconds.

Defaults

The default XID pause timer value is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a router attempts to send an XID upstream to VTAM, and the switched major node is down, the router continues to send retry XIDs at 10-second intervals. If many other routers are also attempting to send retry XIDs to VTAM, the resulting XID flood can cause problems. The **sdlc xid-pause-timer** command enables you to control the interval between router XID retries.

Examples

The following example specifies an XID pause timer value of 60 seconds:

```
interface serial 0
 sdlc xid-pause-timer 60
```

sdllc partner

To enable device-initiated connections for SDLC Logical Link Control. Cisco (SDLLC), use the **sdllc partner** command in interface configuration mode. This command must be specified for the serial interface that links to the serial line device. To cancel the original instruction, use the **no** form of this command.

sdllc partner *mac-address sdlc-address*

no sdllc partner *mac-address sdlc-address*

Syntax Description

mac-address	MAC address of the Token Ring host.
sdlc-address	Synchronous Data Link Control (SDLC) address of the serial device that will communicate with the Token Ring host.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Both the MAC address of the Token Ring host and the SDLC serial line address must be configured to initiate connections with the Token Ring host.

The Token Ring host and the serial device communicate with each other through the Cisco IOS software. Although the device is said to initiate connections, the software actually initiates connections with the Token Ring host on behalf of the serial device. As part of Cisco's SDLLC implementation, the serial device "thinks" that it is communicating with a host also on a serial line. It is actually the software that does all the frame and protocol conversions between serial and Token Ring devices.

There are two conditions under which the Cisco IOS software will attempt to initiate a connection to a host on behalf of a serial device:

- When the serial device attached to the router is powered on. In this case, the router attached to the serial line detects a change in interface signals and initiates a connection with the Token Ring hosts by exchanging explorer and exchange identification (XID) packets.
- When a serial interface previously shut down is brought back online. When the **no shutdown** command is issued, the software will detect a change in the serial line state from down to up and initiate a session with the Token Ring host by exchanging explorer and XID packets.

The Cisco IOS software will continue trying once a minute to initiate a connection whenever one of these two conditions is met, until the host responds to its requests. When you no longer want the software to initiate connections with a host, use the **no sdllc partner** command.

Note For device-initiated sessions, the host will check the IDBLK and IDNUM parameters of the serial device it receives in the XID packet against the information configured on the host. If the information in the XID packet does not match with what is configured on the host, the host will drop the session. Therefore, for device-initiated connections, always specify the correct IDBLK and IDNUM parameters on the router serial interfaces with the **sdllc xid** command.

Examples

In the following example, a serial device at SDLC address C2 wants to initiate a connection with a Token Ring host at MAC address 4000.0122.0001. The router initiates the connection on behalf of a serial device:

```
! sample global command
source-bridge ring-group 100
!
interface serial 0
! router initiates connections with Token Ring host at MAC address
! 4000.0122.0001 on behalf of serial device c2
sdllc partner 4000.0122.0001 c2
```

Related Commands

Command	Description
sdllc xid	Specifies an XID value appropriate for the designated SDLC station associated with this serial interface.

sdllc ring-largest-frame

To indicate the largest I-frame size that can be sent to or received from the Logical Link Control, type 2 (LLC2) primary station, use the **sdllc ring-largest-frame** command in interface configuration mode. To return to the default, use the **no** form of this command.

sdllc ring-largest-frame *bytes*

no sdllc ring-largest-frame *bytes*

Syntax Description

bytes	Frame size in bytes. Values are 516, 1500, 2052, 4472, 8144, 11407, and 17800. The default is 516 bytes.

Defaults

516 bytes

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Values for the *bytes* argument match those for the **lf** *size* of the various **source-bridge remote-peer** commands. You must ensure that your remote peer connection can support this largest frame size. Values for the *bytes* argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800.

Faster screen updates to 3278-style terminals often can be obtained by allowing the Token Ring front-end processor (FEP) to send as large a frame as possible and by allowing the Cisco IOS software to segment the frame into multiple Synchronous Data Link Control (SDLC) I-frames.

Examples

In the following example, the software can send or receive a frame as large as 11407 bytes from the Logical Link Control, type 2 (LLC2) primary station. Any frames larger will be fragmented by the software.

```
! sample global command
source-bridge ring-group 100
!
interface serial 3
! largest frame sent or received on serial 3 is 11407 bytes
sdllc ring-largest-frame 11407
```

Related Commands

Command	Description
source-bridge remote-peer interface	Specifies a point-to-point direct encapsulation connection.
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

sdllc sap

To associate a service access point (SAP) value other than the default SAP value with a serial interface configured for SDLC Logical Link Control. Cisco (SDLLC), use the **sdllc sap** command in interface configuration mode. To return this SAP value to its default state, use the **no** form of this command.

sdllc sap *sdlc-address ssap dsap*

no sdllc sap *sdlc-address ssap dsap*

Syntax Description

sdlc-address	MAC address associated with the remote Synchronous Data Link Control (SDLC) device.
ssap	Source SAP value. It must be in the range from 1 to 254. The default is 4.
dsap	Destination SAP value. It must be in the range from 1 to 254. The default is 4.

Defaults

The default source SAP value for IBM Systems Network Architecture (SNA) devices is 4.
The default destination SAP value for IBM SNA devices is 4.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You use the **sdllc sap** command in conjunction with the **sdllc traddr** command in interface configuration modes. A SAP can be viewed as a port through which a higher-layer application can communicate with its counterpart (peer) operating on another system. Although the standard SAP value for IBM SNA devices is 4, and NetBIOS devices is xF0, other values are allowed.

Examples

In the following example, source SAP and destination SAP values of 2 are specified for the remote SDLC device at the SDLC address C1 02 02:

```
interface serial 0
 sdllc sap c1 02 02
```

Related Commands

Command	Description
sdllc traddr	Enables SDLLC media translation on a serial interface. The address specified is a MAC address to be assigned to the serial station.

sdllc sdlc-largest-frame

To indicate the largest information frame (I-frame) size that can be sent or received by the designated Synchronous Data Link Control (SDLC) station, use the **sdllc sdlc-largest-frame** command in interface configuration mode. To return to the default value, use the **no** form of this command.

sdllc sdlc-largest-frame *address value*

no sdllc sdlc-largest-frame *address value*

Syntax Description

address	Address of the SDLC station that will communicate with the Token Ring host.
value	Largest frame size that can be sent or received by this SDLC station. The default is 265 bytes.

Defaults

265 bytes

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Most SDLC devices are limited to frames of 265 bytes. I-frames received from the Token Ring station that are larger than this size will be properly fragmented.

Examples

In the following example, the Cisco IOS software can send or receive a frame as large as 265 bytes (the default) from the SDLC station at address C6. Any frames larger will be fragmented by the software.

```
! sample global command
source-bridge ring-group 100
!
interface serial 4
! largest frame sent or received on serial 4 is 265 bytes
 sdllc sdlc-largest-frame c6 265
```

sdllc traddr

To enable SDLC Logical Link Control. Cisco (SDLLC) media translation on a serial interface, use the **sdllc traddr** command in interface configuration mode. To disable SDLLC media translation on the interface, use the **no** form of this command.

sdllc traddr *mac-address vrn bn trn*

no sdllc traddr *mac-address vrn bn trn*

Syntax Description

mac-address	MAC address to be assigned to the serial interface.
vrn	SDLLC virtual ring number.
bn	SDLLC bridge number.
trn	SDLLC target ring number.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The address specified is a MAC address to be assigned to the serial station.

Every control unit hooked off the serial line requires a virtual Token Ring address (VTRA). This usually is assigned by the system administrator as a locally administered MAC address (unique across the network).

When you enable SDLLC media translation by specifying the **sdllc traddr** command on a serial interface, you must specify a VTRA for each serial station attached to the serial line. The last two hexadecimal digits (that is, the last byte) of the VTRA *must* be 00. The Cisco IOS software uses this byte to represent the Synchronous Data Link Control (SDLC) address of a station on the serial link.

Note Addresses in the range from *xxxx.xxxx.xx*00 to *xxxx.xxxx.xx*FF are reserved for use by the Cisco IOS software. You must adhere to this addressing requirement. If you do not follow this addressing requirement, there may be a conflict between the VTRA and the addresses reserved by the software for the Synchronous Data Link Control (SDLC) link.

The *vrn*, *bn*, and *trn* arguments represent the SDLLC virtual ring number, bridge number, and target ring number, respectively, that you assign to the interface. In design, the serial interface appears to be a ring, *vrn*, on a source-route bridged network, and ties in through the bridge, *bn*, to the virtual ring group, *trn*. This provides access to other, real rings through remote source-route bridging **source-bridge remote-peer** commands. Note that SDLLC can be configured on a router containing no Token Ring interface cards.

The **sdllc traddr** command automatically turns on the Logical Link Control, type 2 (LLC2) process with default values. To change any of the LLC2 parameters, specify their values on the serial interface that is being enabled for SDLLC. This is done on the serial interface, even though LLC2 does not run on the serial interface, but on the SDLLC virtual ring associated with the serial interface. LLC2 commands can be configured after specifying the **sdllc traddr** command.

Examples

In the following example, SDLLC media translation is enabled off the serial 0 interface to a serial station at MAC address 0110.2222.3300. The SDLLC virtual ring number is 8, the bridge number is 1, and the target ring number is 100.

```
! global command to apply commands to the ring group
source-bridge ring-group 100
! remote peer at IP address 10.108.1.1 belongs to ring group 100 and uses
! tcp as the transport
source-bridge remote-peer 100 tcp 10.108.1.1
source-bridge remote-peer 100 tcp 10.108.2.2
!
interface serial 0
 encapsulation sdlc-primary
! establish address of SDLC station off serial-0 as c1
 sdlc address c1
! enable SDLLC media translation to serial station 0110.2222.3300
! on virtual ring 8, bridge 1, to target ring 100
 sdllc traddr 0110.2222.3300 8 1 100
```

Related Commands

Command	Description
sdllc sap	Associates a SAP value other than the default SAP value with a serial interface configured for SDLLC.
source-bridge remote-peer interface	Specifies a point-to-point direct encapsulation connection.
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

sdllc xid

To specify an exchange identification (XID) value appropriate for the designated Synchronous Data Link Control (SDLC) station associated with this serial interface, use the **sdllc xid** command in interface configuration mode. To disable XID processing for this address, use the **no** form of this command.

sdllc xid *address xid*

no sdllc xid *address xid*

Syntax Description

address	Address of the SDLC station associated with this interface.
xid	XID the Cisco IOS software will use to respond to XID requests received on the Token Ring Logical Link Control, type 2 (LLC2) side of the connection. This value must be 4 bytes (8 digits) in length and is specified with hexadecimal digits.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Exchange identification (XID) requests and responses are usually exchanged before sessions are started. Be sure that the XID value configured on the router matches the IDBLK and IDNUM parameters configured on the host. The XID response to an XID request from the Token Ring host will contain the information you configured in the **sdllc xid** command. The host will check the XID response it receives with the IDBLK and IDNUM parameters (that are configured in virtual telecommunications access method (VTAM)). If they match, the Token Ring host will initiate a session with the router. If they do not match, the host will not initiate a session.

Examples

The following example specifies an XID value of 01720002 at address C2:

```
! sample global command
source-bridge ring-group 100
!
interface serial 0
! sdllc exchange identification value of 01720002 at address c2
 sdllc xid c2 01720002
```

Related Commands

Command	Description
sdllc partner	Enables device-initiated connections for SDLLC. Must be specified for the serial interface that links to the serial line device.

sec-profile

To specify a security profile to be associated with a listen point, use the **sec-profile** command in TN3270 listen-point configuration mode. To remove this specification, use the **no** form of this command.

sec-profile *profilename*

no sec-profile *profilename*

Syntax Description

profilename	Name originally specified in the **profile** command. It consists of a string of alphanumeric characters that specify the security profile name to be associated with a listen point. The valid character range is from 1 to 24.

Defaults

No default behavior or values

Command Modes

TN3270 listen-point configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is not entered or if the **no** form of the command is entered, the security profile reverts to the profile configured in the **default-profile** command. If no default profile is specified, the listen point accepts only nonsecure connections

This command has no retroactive effect.

Examples

The following example specifies LAM as the security profile name for all new clients connecting to listen point 10.10.10.1 until the **sec-profile LAM1** command is configured. Once the **sec-profile LAM1** command is configured, all new client connections to 10.10.10.1 will use LAM1 as the profile name.

```
tn3270-server
 security
 profile LAM ssl
  keylen 128
  servercert slot0:lam
  certificate reload
 profile LAM1 ssl
  keylen 40
  servercert slot0:lam1
  certificate reload
 listen-point 10.10.10.1
 sec-profile LAM
 pu DIRECT 012ABCDE tok 0 04
Sec-profile LAM1
```

security (TN3270)

To enable security on the TN3270 server, use the **security** command in TN3270 server configuration mode. To turn off security on the TN3270 server, use the **no** form of this command.

security

no security

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to have security enabled.

Command Modes

TN3270 server configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **no** form of this command is configured, any listen points that contain a security profile definition are reconfigured and are no longer secure. Sessions already established on the listen point will continue to run in the same mode (secure or nonsecure) as originally configured. If sessions are active on a listen point, a message will be sent to the console stating that the listen point has sessions running with an outdated security specification. A shutdown/restart sequence must be performed on the listen point if the user wants the sessions on the listen point to use the new specification.

Entering the **security** command moves the user into security configuration mode. Entering the **no** form of this command moves the user to a TN3270 server configuration mode.

This command has no retroactive effect.

Examples

In the following example, security is enabled on the TN3270 server:

```
tn3270-server
 security
  profile secure-1 ss1
```

servercert

To specify the location of the TN3270 server's security certificate in the router's Flash memory, use the **servercert** command in profile configuration mode.

servercert *location*

Syntax Description

location	Hexadecimal string of up to 63 characters specifying the location of the server's certificate in the Flash memory.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The certificate is in X.509 format, signed by a certification authority (CA). The certificate must be created offline. It cannot be created using the Cisco IOS software. Use third-party software or a Windows-based utility. The certificate should be in privacy enhanced mail (PEM) or Base 64 format. The output from the certificate generation contains two parts: the certificate and the private key. Concatenate these two files to create a single certificate file in PEM or Base 64 format.

Store the concatenated file in Flash memory using TFIP and the location entered using the **servercert** *location* command. If the file does not exist in the Flash memory when the command is entered, an error message is displayed indicating that the file does not exist. The first time this command is configured the certificate is automatically loaded from the specified location. Subsequent changes to the location file do not cause the certificate to be read automatically into system's memory. The **certificate reload** command must be entered to read the certificate into memory. If the user exits from the profile configuration mode without configuring the **servercert** command, a warning message is displayed. The warning message indicates that it is mandatory to configure a certificate using the **servercert** command.

Examples

The following example specifies that slot0:lam is the location of the security certificate:

```
tn3270-server
 security
 profile LAM ssl
  keylen 512
  servercert slot0:lam
  certificate reload
```

Related Commands

Command	Description
profile	Specifies a name and a security protocol for a security profile and enters profile configuration mode.

show access-expression

To display the defined input and output access list expressions, use the **show access-expression** command in privileged EXEC mode.

show access-expression [**begin** | **include** | **exclude**]

Syntax Description

begin	(Optional) Begin with the access list expression that matches.
include	(Optional) Include access list expressions that match.
exclude	(Optional) Exclude access list expressions that match.

Defaults

Displays all input and output access list expressions.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show access-expression** command:

```
Router# show access-expression
Router# Interface TokenRing0/0:
        Input:(dmac(701) | ~lsap(202))
```

See the **access-expression** command for a description of the access expressions.

Related Commands

Command	Description
access-expression	Defines an access expression.

show alps ascu

To display the status of the Airline Product Set (ALPS) agent-set control unit (ASCU), use the **show alps ascu** command in user EXEC or privileged EXEC mode.

show alps ascu [*interface* [*id*]] [**detailed**]

Syntax Description

interface	(Optional) Combined interface and ASCU interchange address (IA). • If the interface and ASCU are specified, the status for the ASCU on that interface is displayed. • If the interface is specified, then all ASCUs defined on that interface are displayed. • If the interface and ASCU are not specified, then all ASCUs defined are displayed.
id	(Optional) id number of the interface.
detailed	(Optional) Displays detailed output.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(5)T	The output of this command was modified.
12.1(2)T	The output for the **detailed** version of this command was modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2 SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 The *interface* and *id* arguments are not supported in this release.

Examples

The following is sample output from the **show alps ascu** command:

```
Router# show alps ascu

interface  dlc id a1 a2 circuit        pkt_tx      pkt_rx      state
----------------------------------------------------------------------
Serial1/2  ALC 5F 41 42 MATIP-ALC      0           0           DOWN
Serial1/3  UTS 21 23 4A MATIP          0           0           DOWN
Serial1/6  ALC 5F 41 45 MATIP-ALC      0           0           DOWN
Serial1/6  ALC 6F 41 44 MATIP-ALC      0           0           DOWN
Total number of ASCUs: 4
Total number of up ASCUs: 0
```

The following is sample output from the **show alps ascu detailed** command for ASCUs 4F and 6F on serial interface 1/6:

```
Router# show alps ascu detailed

ascu 4F on i/f Serial1/6, dlc = ALC, state = UP
  default-circuit = MATIP-ALC, a1 = 41, a2 = 45
  max_msg_len = 962, retry_option = none, alias = 6F
  err_disp_terminal = 114, err_disp_line = 102
  pkt_tx = 0, byte_tx = 0, pkt_rx = 0, byte_rx = 0
  bad_CCC = 0, garbledMsgs = 0, T1Timeouts = 0

ascu 6F on i/f Serial1/6, dlc = ALC, state = DOWN
  default-circuit = MATIP-ALC, a1 = 41, a2 = 44
  max_msg_len = 962, retry_option = none
  err_disp_terminal = 114, err_disp_line = 102
  pkt_tx = 0, byte_tx = 0, pkt_rx = 0, byte_rx = 0
  bad_CCC = 0, garbledMsgs = 0, T1Timeouts = 14
```

Table 17 describes the significant fields in the display.

Table 17 show alps ascu Field Descriptions

Field	Description
dlc	Data link control.
state	Status of connection; UP, DOWN, or DISABLED.
default-circuit	Name of the default circuit.
a1	Logical ASCU identification information for A1.
a2	Logical ASCU identification information for A2.
max_msg_len	Maximum input message length. Protocol level count that includes all protocol overhead plus data. The valid range is from 1 to 3840 bytes. The default is 962 bytes. Anything over the maximum is discarded and the interface giant counter is incremented. This does not apply to the GarbledMsg for the ASCU.
retry_option	Retry option. When a message with a bad cycle check character (CCC) is received from an ASCU, a retry option can be configured using the **alps retry-option** command. The retry option configures the customer premises equipment (CPE) to send a message to the ASCU. The following retry options are available: • resend—Indicator LED signals the operator at the ASCU to resend data. • reenter—Service messages signal the operator at the ASCU to reenter data. The default retry option is no retry.
alias	Parent ASCU interchange address to which this nonpolling automatic level control (ALC) ASCU is aliased.
err_disp_terminal	Terminal address to which error service messages are sent.
err_disp_line	Screen line number where error service messages are sent.
pkt_tx	Packets sent.
byte_tx	Bytes sent.
pkt_rx	Packets received.
byte_rx	Bytes received.

Table 17 show alps ascu Field Descriptions (continued)

Field	Description
bad_CCC	Number of bad CCCs. Bad CCCs occurs due to the following reasons: • The proper control characters were received. • The characters did not exceed the maximum length. • The CCC calculation fails.
garbledMsgs	Number of garbled messages. Garbled messages are a result of a range of different errors, including the following: • An unexpected character is received. • The maximum interface buffer size is exceeded. • The maximum message length is exceeded.
T1Timeouts	Number of response timeouts.

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.

show alps circuits

To display the status of the Airline Product Set (ALPS) circuits, use the **show alps circuits** command in user EXEC or privileged EXEC mode.

show alps circuits [**peer** *ip-address*] [**name** *name*] [**detailed**]

Syntax Description

peer *ip-address*	(Optional) Displays the status of the circuits connected to the specified peer.
name *name*	(Optional) Displays the status of the specified circuit.
detailed	(Optional) Displays the detailed output.

Command Default

If a circuit name is specified, then the status of that circuit will be displayed; otherwise, the status of all circuits will be displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(5)T	The output was modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2 SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show alps circuits** command:

```
Router# show alps circuits

name         pri_peer        curr_peer       dlc   state  pkt_tx     pkt_rx
--------------------------------------------------------------------------------
CKT1         172.18.60.201   0.0.0.0         NONE  DISC   0          0
CKT2         172.18.60.201   0.0.0.0         NONE  DISC   0          0
MATIP        10.100.1.2      0.0.0.0         UTS   DISC   0          0
MATIP-ALC    10.100.1.2      0.0.0.0         ALC   INOP   0          0
Total number of circuits: 4
Total number of connected circuits: 0
```

The following is sample output from the **show alps circuits name detailed** command:

```
Router# show alps circuit name matip-alc detailed

MATIP-ALC: dlc = ALC, conn_type = PERM, state = INOP, uptime = 00:00:00
  down reason = noReason
  pri_peer = 10.100.1.2, sec_peer = 0.0.0.0
  curr_peer = 0.0.0.0,
  local_hld = 4D02, remote_hld = 7F7F
  emtox: hostlink = 255, x121 = 1234
  lifetime_tmr = 4, idle_tmr = 60, retry_tmr = 30
  pkt_tx = 0, byte_tx = 0, pkt_rx = 0, byte_rx = 0
  src_corr = 0, dst_corr = 0
  drops_q_overflow = 0, drops_ckt_disabled = 0
  drops_lifetime_tmr = 0, drops_invalid_ascu = 0
  ascus: (41,42)U, (41,44)U, (41,45)U
Total number of ASCUs: 3
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.

show alps peers

To display the status of the Airline Product Set (ALPS) partner peers, use the **show alps peers** command in user EXEC or privileged EXEC mode.

show alps peers [**ipaddress** *address*] [**detailed**] [**name** *name*]

Syntax Description

ipaddress *address*	(Optional) Displays the status of the specified agent-set control unit (ASCU).
detailed	(Optional) Displays the detailed output.
name *name*	(Optional) Displays the circuit name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(5)T	The output was modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2 SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 The **name** keyword *name* argument are not supported in this release

Usage Guidelines

If an IP address is specified, then only the status of that peer will be displayed; otherwise, the status of all peers will be displayed.

Examples

The following is sample output from the **show alps peers detailed** command:

```
Router# show alps peers detailed

TCP:10.227.50.106, conn_id = MATIP_A_CKT-2
   protocol = MATIP_A, fport = 350, lport = 11592
   type = DYN, create = ADMIN, state = OPENED, uptime = 00:00:53
   down reason = unknown
   pkt_tx = 1071, byte_tx = 37264, pkt_rx = 1066, byte_rx = 36010
   Drops:giants = 0, q_overflow = 0, peer_down = 0, ver_mismatch = 0
```

Related Commands

Command	Description
alps primary-peer	Specifies the primary TCP peer and, optionally, a backup TCP peer for this ALPS circuit.
alps remote-peer	Specifies the partner IP address.

show bridge

To display classes of entries in the bridge forwarding database, use the **show bridge** command in privileged EXEC mode.

show bridge [*bridge-group*] [*interface*] [*address* [*mask*]] [**verbose**]

Syntax Description

bridge-group	(Optional) Number that specifies a particular spanning tree.
interface	(Optional) Specific interface, such as Ethernet 0.
address	(Optional) 48-bit canonical (Ethernet ordered) MAC address. This may be entered with an optional mask of bits to be ignored in the address, which is specified with the *mask* argument.
mask	(Optional) Bits to be ignored in the address. You must specify the *address* argument if you want to specify a mask.
verbose	(Optional) Displays additional detail, including any Frame Relay data-link connection identifier (DLCI) associated with a station address.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.0	The **verbose** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **verbose** keyword first appeared in Cisco IOS Release 11.0.

The following are possible variations of the **show bridge** command:

```
show bridge ethernet 0
show bridge 0000.0c00.0000 0000.00FF.FFFF
show bridge 0000.0c00.0e1a
show bridge
show bridge verbose
```

In the sample output, the first command would display all entries for hosts reachable via Ethernet interface 0, the second command would display all entries with the vendor code of 0000.0c00.0000, and the third command would display the entry for address 0000.0c00.0e1a. In the fourth command, all entries in the forwarding database would be displayed. The fifth command provides additional detail. In all five lines, the bridge group number has been omitted.

Examples

The following is sample output from the **show bridge** command. The second display is output from the **show bridge** command with the **verbose** argument.

```
Router# show bridge

Total of 300 station blocks, 280 free
Codes: P - permanent, S - self

Bridge Group 32:Bridge Group 32:

    Address       Action   Interface       Age   RX count   TX count
0180.c200.0000   receive       -            S           0          0
ffff.ffff.ffff   receive       -            S           0          0
0900.2b01.0001   receive       -            S           0          0
0300.0c00.0001   receive       -            S           0          0
0000.0c05.1000   forward   Ethernet0/1      4           1          0
0000.0c04.4b5b   receive       -            S           0          0
0000.0c04.4b5e   receive       -            S           0          0
0000.0c04.4b5d   receive       -            S           0          0
0000.0c04.4b5c   receive       -            S           0          0
0000.0c05.4a62   forward   Ethernet0/1      4           1          0
aa00.0400.2108   forward   Ethernet0/1      0          42          0
0000.0c12.b888   forward   Ethernet0/2      4           1          0
0000.0c12.b886   forward   Ethernet0/1      4           1          0
aa00.0400.4d09   forward   Ethernet0/1      4           1          0
0000.0c06.fb9a   forward   Ethernet0/1      4           1          0
0000.0c04.b039   forward   Ethernet0/1      4           1          0

Router# show bridge verbose

Total of 300 station blocks, 287 free
Codes: P - permanent, S - self

BG Hash      Address      Action Interface     DLCI   Age RX count   TX count
32 00/0   0180.c200.0000 receive      -           -     S           0          0
32 00/1   ffff.ffff.ffff receive      -           -     S           0          0
32 01/0   0900.2b01.0001 receive      -           -     S           0          0
32 01/1   0300.0c00.0001 receive      -           -     S           0          0
32 10/0   0000.0c04.4b5b receive      -           -     S           0          0
32 15/0   0000.0c04.4b5e receive      -           -     S           0          0
32 16/0   0000.0c04.4b5d receive      -           -     S           0          0
32 17/0   0000.0c04.4b5c receive      -           -     S           0          0
32 29/0   aa00.0400.2108 forward  Ethernet0/1    -     0          48          0
32 30/0   0000.0c12.b888 forward  Ethernet0/2    -     0           1          0
32 A4/0   0800.2002.ff5b forward  Ethernet0/1    -     0           6          0
32 E2/0   aa00.0400.e90b forward  Ethernet0/1    -     0          65          0
32 F2/0   0000.0c04.b042 forward  Ethernet0/2    -     3           2          0
```

Table 18 describes the significant fields shown in the display.

Table 18 show bridge Field Descriptions

Field	Description
Total of 300 station blocks	Total number of forwarding database elements in the system. The memory to hold bridge entries is allocated in blocks of memory sufficient to hold 300 individual entries. When the number of free entries falls below 25, another block of memory sufficient to hold another 300 entries is allocated. Therefore, the size of the bridge forwarding database is limited to the amount of free memory in the router.
295 free	Number in the free list of forwarding database elements in the system. The total number of forwarding elements is expanded dynamically, as needed.
BG	Bridging group to which the address belongs.
Hash	Hash key/relative position in the keyed list.
Address	Canonical (Ethernet ordered) MAC address.
Action	Action to be taken when that address is looked up; choices are to discard or forward the datagram.
Interface	Interface, if any, on which that address was seen.
Age	Number of minutes since a frame was received from or sent to that address. The letter "P" indicates a permanent entry. The letter "S" indicates the system as recorded by the router. On the modular systems, this is typically the broadcast address and the router's own hardware address; on the IGS, this field will also include certain multicast addresses.
RX count	Number of frames received from that address.
TX count	Number of frames forwarded to that address.

show bridge circuit-group

To display the interfaces configured in each circuit group and show whether they are currently participating in load distribution, use the **show bridge circuit-group** command in user EXEC or privileged EXEC mode.

show bridge [*bridge-group*] **circuit-group** [*circuit-group*] [*src-mac-address*] [*dst-mac-address*]

Syntax Description

bridge-group	(Optional) Number that specifies a particular bridge group.
circuit-group	(Optional) Number that specifies a particular circuit group.
src-mac-address	(Optional) 48-bit canonical (Ethernet ordered) source MAC address.
dst-mac-address	(Optional) 48-bit canonical (Ethernet ordered) destination MAC address.

Command Modes

User EXEC
Prvileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from various **show bridge circuit-group** command strings:

```
Router# show bridge circuit-group

Bridge group 1 Circuit group 1:
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding
Bridge group 1 Circuit group 2:
    Interface Serial2 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 1

Bridge group 1 Circuit group 1:
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 2

Bridge group 1 Circuit group 2:
    Interface Serial2 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 1 0000.6502.23EA 0000.1234.4567

Output circuit group interface is Serial3

Router# show bridge 1 circuit-group 1 0000.6502.23EA
```

```
%Destination MAC address required

Router# show bridge 1 circuit-group 1

Bridge group 1 Circuit group 1:
    Transmission pause interval is 250ms
    Output interface selection is source-based
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding
    Interface Serial2 is unavailable

Router# show bridge 1 circuit-group 1 0000.6502.23EA 0000.1234.4567

%Please enter source MAC address only
```

Table 19 describes the significant fields shown in the display.

Table 19 show bridge circuit-group Field Descriptions

Field	Description
inserted	Indicates whether this interface is included or not included in circuit-group operation. If the interface is administratively down, or if line protocol is not up, the interface is not included in the circuit-group operation.
learning	Indicates whether this interface is in Spanning Tree Protocol (IEEE or Digital) learning or not learning state.
forwarding	Indicates whether this port is in Spanning Tree Protocol (IEEE or Digital) forwarding or not forwarding state.

show bridge group

To display the status of each bridge group, use the **show bridge group** command in privileged EXEC mode.

show bridge group [**verbose**]

Syntax Description

verbose	(Optional) Displays detailed information.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show bridge group** command:

```
Router# show bridge group

Bridge Group 1 is running the DEC compatible Spanning Tree Protocol

   Port 7 (ATM0.1 LANE Ethernet) of bridge group 1 is down
   Port 4 (TokenRing0) of bridge group 1 is forwarding
```

"Forwarding" and "down" indicate the port state as determined by the spanning-tree algorithm or via configuration.

The following examples are for bridge group 30 and bridge group 40 of a PA-12E/2FE port adapter in slot 3:

```
Router# show bridge group

Bridge Group 30 is running the IEEE compatible Spanning Tree Protocol
   Port 19 (Fast Ethernet3/0) of bridge group 30 is forwarding
   Port 20 (Fast Ethernet3/1) of bridge group 30 is forwarding
   Port 21 (Ethernet3/2) of bridge group 30 is forwarding
   Port 22 (Ethernet3/3) of bridge group 30 is forwarding
   Port 23 (Ethernet3/4) of bridge group 30 is forwarding
   Port 24 (Ethernet3/5) of bridge group 30 is forwarding
   Port 25 (Ethernet3/6) of bridge group 30 is forwarding

Bridge Group 40 is running the IEEE compatible Spanning Tree Protocol

   Port 26 (Ethernet3/7) of bridge group 40 is down
   Port 27 (Ethernet3/8) of bridge group 40 is down
   Port 28 (Ethernet3/9) of bridge group 40 is down
   Port 29 (Ethernet3/10) of bridge group 40 is down
   Port 30 (Ethernet3/11) of bridge group 40 is down
   Port 31 (Ethernet3/12) of bridge group 40 is down
   Port 32 (Ethernet3/13) of bridge group 40 is down
```

show bridge multicast

To display transparent bridging multicast state information, use the **show bridge multicast** command in user EXEC or privileged EXEC mode.

show bridge [*bridge-group*] **multicast** [**router-ports** | **groups**] [*group-address*]

Syntax Description

bridge-group	(Optional) Bridge group number specified in the **bridge protocol** command.
router-ports	(Optional) Display information for multicast router ports.
groups	(Optional) Display information for multicast groups.
group-address	(Optional) Multicast IP address associated with a specific multicast group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show bridge multicast** command:

```
Router# show bridge multicast

 Multicast router ports for bridge group 1:

  2 multicast router ports
   Fddi2/0         R
   Ethernet0/4     R

 Multicast groups for bridge group 1:

  235.145.145.223            RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0

  235.5.5.5                  RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0

  235.4.4.4                  RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0
```

Table 20 describes the significant fields shown in the display.

Table 20 show bridge multicast Field Descriptions

Field	Description
Multicast router ports for…	List of the multicast router ports by bridge group. Within the bridge group cluster, the display lists the number of multicast router ports and then lists the ports by interface.
Multicast groups for…	List of the multicast groups by bridge group. Within each multicast group, identified by a unique address, the display lists each port by interface name and indicates whether that port is a group member ("G"), a multicast router port ("R"), or both. The receive (RX) and transmit (TX) counts show the number of multicast packets that have been constrained to the multicast group by the bridge.

show bridge vlan

To display virtual LAN subinterfaces, use the **show bridge vlan** command in privileged EXEC mode.

show bridge vlan

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show bridge vlan** command:

```
Router# show bridge vlan

Bridge Group: 50

Virtual LAN Trunking Interface(s):  vLAN Protocol:     vLAN ID:  State

Fddi2/0.1000                        IEEE 802.10        1000      forwarding
Fast Ethernet4/0.500                 Inter Switch Link  500       listening

Virtual LAN Native Interface(s):    State

Ethernet0/1                         forwarding
Serial1/1                           down
```

Table 21 describes the fields shown in the display.

Table 21 show bridge vlan Field Descriptions

Field	Description
Bridge Group	Bridge group to which these interfaces belong.
Virtual LAN Trunking Interface(s)	VLAN interface.
vLAN Protocol)	IEEE 802.10 or Cisco Inter-Switch Link (ISL) encapsulation.
vLAN ID	VLAN identifier that maintains VLAN identities between switches.

Table 21 show bridge vlan Field Descriptions (continued)

Field	Description
State	Spanning-tree port state of the interface.
Virtual LAN Native Interface(s):	Interfaces whose transparently bridged traffic will be propagated only to other LAN segments within the same virtual LAN.

show bsc

To display statistics about the interfaces on which Bisync is configured, use the **show bsc** command in privileged EXEC mode.

show bsc [**group** *bstun-group-number*] [**address** *address-list*]

Syntax Description

group *bstun-group-number*	(Optional) block serial tunnel (BSTUN) group number. Valid numbers are decimal integers in the range from 1 to 255.
address *address-list*	(Optional) List of poll addresses.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show bsc** command:

```
Router# show bsc

BSC pass-through on Serial4:
HDX enforcement state: IDLE.
Frame sequencing state: IDLE.
Total Tx Counts: 0 frames(total). 0 frames(data). 0 bytes.
Total Rx Counts: 0 frames(total). 0 frames(data). 0 bytes.

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

        Poll address: C3. Select address: E3 *CURRENT-CU*
        State is Active.
        Tx Counts: 1136 frames(total). 0 frames(data). 1136 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

Total Tx Counts: 2273 frames(total). 0 frames(data). 2273 bytes.
Total Rx Counts: 2284 frames(total). 0 frames(data). 11420 bytes.
```

The following is sample output from the **show bsc** command specifying BSTUN group 50:

```
Router# show bsc group 50

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
        Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.

        Poll address: C3. Select address: E3 *CURRENT-CU*
        State is Active.
        Tx Counts: 1214 frames(total). 0 frames(data). 1214 bytes.
        Rx Counts: 1220 frames(total). 0 frames(data). 6100 bytes.

Total Tx Counts: 2431 frames(total). 0 frames(data). 2431 bytes.
Total Rx Counts: 2442 frames(total). 0 frames(data). 12200 bytes.
```

The following is sample output from the **show bsc** command specifying BSTUN group 50 and poll address C2:

```
Router# show bsc group 50 address C2

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
        Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.

Total Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
Total Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.
```

The following is sample output from the **show bsc** command specifying poll address C2:

```
Router# show bsc address C2

BSC pass-through on Serial4:
HDX enforcement state: IDLE.
Frame sequencing state: IDLE.
Total Tx Counts: 0 frames(total). 0 frames(data). 0 bytes.
Total Rx Counts: 0 frames(total). 0 frames(data). 0 bytes.

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

Total Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
Total Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.
```

Table 22 describes the fields shown in the display.

Table 22 show bsc Field Descriptions

Field	Description
BSC *x* on *interface y*	Indicates whether the router is configured for pass-through or local acknowledgment on the indicated interface.
Output queue depth	Packets queued on this interface. This field is displayed only when the value is not zero.
Frame builder state	Current frame building state. This field is displayed only when the state is not IDLE.
HDX enforcement state	Current half-duplex send enforcement state. The values are: • IDLE—Waiting for communication activity. • PND_COMP—Waiting for router to send. • PND_RCV—Waiting for attached device to respond to data sent.
Frame sequencing state	Frame sequencing state to protect against network latencies. When the router is configured as the primary end of the link, the values are: • IDLE—Waiting for a poll. • SEC—In a session with a device. When the router is configured as the secondary end of the link, the values are: • IDLE—Waiting for a poll. • PRI—In a session with a device. When the router is configured for point-to-point contention, the values are: • IDLE—Waiting for a poll. • PEND—Waiting for the first data frame. • PRI—Connected device is acting as a primary device. • SEC—Connected device is acting as a secondary device.
Total Tx Counts	Total transmit frame count for the indicated interface.
Total Rx Count	Total receive frame count for the indicated interface.

Table 22 show bsc Field Descriptions (continued)

Field	Description
Primary state is …	The current state when the router is configured as the primary end of the link. The possible values are: • TCU_Down—Waiting for the line to become active. • TCU_EOFile—A valid block ending in ETX has been received. • TCU_Idle—Waiting for work or notification of completion of the sending of end of transmission (EOT). • TCU_InFile—A valid block ending in ETB has been received. • TCU_Polled—A general poll has been issued. • TCU_Selected—A select has been issued. • TCU_SpecPolled—A specific poll has been sent. • TCU_TtdDelay—An ETB block was acknowledged, but the next block to be sent has not yet been received. • TCU_TtdSent—A TTD has been sent because no data was received by the time the timeout for sending Ttd expired. • TCU_TxEOFile—A block of data ending in ETX has been sent. • TCU_TxInFile—A block of data ending in ETB has been sent. • TCU_TxRetry—Trying to send a frame again.
Secondary state is …	The current state when the router is configured as the secondary end of the link. The possible values are: • CU_DevBusy—A select has been refused with WACK or RVI. • CU_Down—Waiting for the line to become active. • CU_EOFile—A valid block ending in ETX has been received. • CU_Idle—Waiting for a poll or select action. • CU_InFile—A valid block ending in ETB has been received. • CU_Selected—A select has been acknowledged. • CU_TtdDelay—An ETB block was acknowledged, but the next block to be sent has not yet been received. • CU_TtdSent—A TTD has been sent because no data was received by the time the timeout for sending Ttd expired. • CU_TxEOFile—A block of data ending in ETX has been sent. • CU_TxInFile—A block of data ending in ETB has been sent. • CU_TxRetry—Trying to send a frame again. • CU_TxSpecPollData—A data frame (typically S/S) has been used to answer a specific poll. • CU_TxStatus—Host has polled for device-specific status.
Poll address	Address used when the host wants to get device information.
Select address	Address used when the host wants to send data to the device.

Table 22 show bsc Field Descriptions (continued)

Field	Description
State is …	Current initialization state of this control unit. The values are: • Active—The remote device is active. • Inactive—The remote device is dead. • Initializing—No response from remote device yet.
Tx Counts	Transmit frame count for this control unit.
Rx Counts	Receive frame count for this control unit.
Total Tx Counts	Total transmit frame count for the indicated interface.
Total Rx Counts	Total receive frame count for the indicated interface.

show bstun

To display the current status of serial tunnel (STUN) connections, use the **show bstun** command in privileged EXEC mode.

show bstun [**group** *bstun-group-number*] [**address** *address-list*]

Syntax Description

group *bstun-group-number*	(Optional) Block Serial Tunneling (BSTUN) group number. Valid numbers are decimal integers in the range from 1 to 255.
address *address-list*	(Optional) List of poll addresses.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(4)T	This command was modified for the Bisync-to-IP Conversion for Automated Teller Machines feature. The display was modified to include Bisync-to-IP (BIP) as a transport protocol, and to show both the foreign and local port numbers.
12.3(2)T	This command was modified for the Asynchronous Point of Sale-to-IP Conversion (APIP) feature to include APIP as a transport protocol.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show bstun** command with no options:

```
Router# show bstun

This peer: 10.26.54.111
 *Serial0/0 (group 201 [bsc-local-ack])
route  transport  address         dlci  lsap     state     rx_pkts   tx_pkts   drops
C1     TCP       10.26.54.2                      closed    0         0         0
C2     TCP       10.26.54.2                      closed    0         0         0
C3     TCP       10.26.54.2                      closed    0         0         0
```

The following is sample output from the **show bstun** command using the new BIP configuration:

```
Router# show bstun

This peer: 10.26.54.111
 *Serial0/0 (group 201 [bsc-local-ack])
route  transport  address       fport  lport     state     rx_pkts   tx_pkts   drops
C1     BIP       10.26.54.2     2002   1963      closed    0         0         0
C2     BIP       10.26.54.2     2001   1963      closed    0         0         0
C3     BIP       10.26.54.2     2000   1963      closed    0         0         0
```

```
Router# show bstun

 Serial1/7  (group 10 [apos])
route  transport  address       fport  lport     state     rx_pkts    tx_pkts    drops
all     APIP      10.26.54.2    10550  0         closed    0          0          0
```

Table 23 describes the significant fields shown in the output.

Table 23 show bstun Field Descriptions

Field	Description
This peer	Lists the peer name or address. The interface name (as defined by the **description** command), its block serial tunnel (BSTUN) group number, and the protocol associated with the group are shown on the next header line.
route	Bisync control unit address or all.
transport	Description of link, either a serial interface using serial transport (indicated by IF followed by interface name), a TCP connection to a remote router (TCP followed by IP address), a BIP connection to a host, or APIP connection to a host (APIP followed by an IP address).
address	The IP address or serial interface that packets are being forwarded to.
fport	The foreign port number.
lport	The local port number.
state	State of the link. The following are possible values for the state of the link: • open: A connection is active. • open pending: Indicates the router will be attempting to connect to the remote device. • open wait: An active open message has been sent to the remote device, and the router is waiting for a response. • direct: A direct link to another line is active. • dead: The connection has been aborted. • closed: A normal close operation has disconnected the connection.
open	A connection is active.
open pending	Indicates the router will be attempting to connect to the remote device.
open wait	An active open message has been sent to the remote device, and the router is waiting for a response.
direct	A direct link to another line is active.
dead	The connection has been aborted.
closed	A normal close operation has disconnected the connection.
rx_pkts	Number of received packets.
tx_pkts	Number of sent packets.
drops	Number of packets that had to be dropped for whatever reason.

show controllers channel

To display Channel Port Adapter (CPA)-specific information, including the loaded microcode, use the **show controllers channel** command in user EXEC or privileged EXEC mode.

show controllers channel [*slot*/*port*]

Syntax Description

slot	(Optional) Slot number.
port	(Optional) Interface number.

Command Modes

User EXEC
Prvileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show controllers channel** command:

```
Router# show controllers channel 5/0

ECPA 5, hardware version 1.0, microcode version 26.0
    Mailbox commands: 0 forevers, 0 max elapsed usecs
    Microcode loaded from flash slot0:xcpa26-0_kernel_xcpa
    Loaded:seg_eca         Rev. 0    Compiled by cip-release on 01-Apr-98
    EPROM version 1.0, VPLD version 1.1
    ECA0: hw version 255, microcode version C50602D1
    Load metrics:
      Memory    sram 2964552/4096K, dram 11552952/16M
      CPU       1m   0%, 5m   0%, 60m   0%
      DMA       1m   0%, 5m   0%, 60m   0%
      ECA0      1m   0%, 5m   0%, 60m   0%
 Interface Channel5/0
 Hardware is Escon Channel
  HW Registers control status=0x0001EC07  LED control=0x00045DD5
  HW Poll Register 4B05D4E0:[00000001]
  Free buffer queues
    queue=0 max_entries=128 size=600 head=39 ring=4B095F00
    queue=1 max_entries=32 size=4520 head=31 ring=4B095E40
    queue=2 max_entries=64 size=4520 head=63 ring=4B096140
  Tx Queues
    queue=0 head=0 tail=0 tx_cnt=0 tx_pakcnt=0
    max_entries=128 type=1 poll_index=0 ring=4B0963C0
    fspak buffers swapped out=0
    queue=1 head=31 tail=31 tx_cnt=0 tx_pakcnt=0
    max_entries=32 type=2 poll_index=1 ring=4B096280
    fspak buffers swapped out=0
```

```
Rx Queues
  max_entries=221 poll_index=3 head=57 ring=4B096800
  max packets per interrupt count = 0
```

show controllers token (IBM)

To display information about memory management, error counters, and the board itself, use the **show controllers token** command in privileged EXEC mode.

show controllers token

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Depending on the board being used, the output from the **show controllers token** command can vary. The **show controllers token** command also displays proprietary information. Thus, the information that the **show controllers token** command displays is of primary use to Cisco Systems technical personnel. Information that is useful to users can be obtained with the **show interfaces tokenring** command, described later.

Examples

The following is sample output from the **show controllers token** command of a CSC-IR or CSC-2R card:

```
Router# show controllers token

TR Unit 0 is board 0 - ring 0

 state 3, dev blk: 0x1D2EBC, mailbox: 0x2100010, sca: 0x2010000
   current address: 0000.3080.6f40, burned in address: 0000.3080.6f40
   current TX ptr: 0xBA8, current RX ptr: 0x800

   Last Ring Status: none

 Stats: soft:0/0, hard:0/0, sig loss:0/0
        tx beacon: 0/0, wire fault 0/0, recovery: 0/0
        only station: 0/0, remote removal: 0/0
   Bridge: local 3330, bnum 1, target 3583
     max_hops 7, target idb: 0x0, not local
   Interface failures: 0 -- Bkgnd Ints: 0
   TX shorts 0, TX giants 0

   Monitor state: (active)
     flags 0xC0, state 0x0, test 0x0, code 0x0, reason 0x0
 f/w ver: 1.0, chip f/w: '000000.ME31100', [bridge capable]
```

```
     SMT form of this command s: 1.01 kernel, 4.02 fastmac
     ring mode: F00, internal enables: SRB REM RPS CRS/NetMgr
     internal functional: 0000011A (0000011A), group: 00000000 (00000000)
     if_state: 1, ints: 0/0, ghosts: 0/0, bad_states: 0/0
     t2m fifo purges: 0/0
     t2m fifo current: 0, t2m fifo max: 0/0, proto_errs: 0/0
     ring: 3330, bridge num: 1, target: 3583, max hops: 7

Packet counts:
       receive total: 298/6197, small: 298/6197, large 0/0
               runts: 0/0, giants: 0/0
               local: 298/6197, bridged: 0/0, promis: 0/0
             bad rif: 0/0, multiframe: 0/0
       ring num mismatch 0/0, spanning violations 0
       transmit total: 1/25, small: 1/25, large 0/0
                runts: 0/0, giants: 0/0, errors 0/0
bad fs: 0/0, bad ac: 0
congested: 0/0, not present: 0/0
     Unexpected interrupts: 0/0, last unexp. int: 0

     Internal controller counts:
    line errors:  0/0, internal errors: 0/0
    burst errors: 0/0, ari/fci errors:  0/0
    abort errors: 0/0, lost frame: 0/0
    copy errors:  0/0, rcvr congestion: 0/0
    token errors: 0/0, frequency errors: 0/0
    dma bus errors: -/-, dma parity errors: -/-
     Internal controller smt state:
    Adapter MAC:     0000.3080.6f40, Physical drop:     00000000
    NAUN Address:    0000.a6e0.11a6, NAUN drop:         00000000
    Last source:     0000.a6e0.11a6, Last poll:         0000.3080.6f40
    Last MVID:       0006,           Last attn code:    0006
    Txmit priority:  0006,           Auth Class:        7FFF
    Monitor Error:   0000,           Interface Errors:  FFFF
    Correlator:      0000,           Soft Error Timer:  00C8
    Local Ring:      0000,           Ring Status:       0000
    Beacon rcv type: 0000,           Beacon txmit type: 0000
    Beacon type:     0000,           Beacon NAUN:       0000.a6e0.11a6
```

Table 24, Part 1 describes the fields shown in the first line of sample output.

Table 24, Part 1   show controllers token Field Descriptions

Field	Description
TR Unit 0	Unit number assigned to the Token Ring interface associated with this output.
is board 0	Board number assigned to the Token Ring controller board associated with this interface.
ring 0	Number of the Token Ring associated with this board.

In the following line, state 3 indicates the state of the board. The rest of this output line displays memory mapping that is of primary use to Cisco engineers.

```
state 3, dev blk: 0x1D2EBC, mailbox: 0x2100010, sca: 0x2010000
```

The following line also appears in **show interface token** output as the address and burned-in address (bia), respectively:

```
current address: 0000.3080.6f40, burned in address: 0000.3080.6f40
```

The following line displays buffer management pointers that change by board:

```
current TX ptr: 0xBA8, current RX ptr: 0x800
```

The following line indicates the ring status from the controller chipset. This information is used by LAN Network Manager:

```
Last Ring Status: none
```

The following line displays Token Ring statistics. See the Token Ring specification for more information:

```
Stats: soft:0/0, hard:0/0, sig loss:0/0
        tx beacon: 0/0, wire fault 0/0, recovery: 0/0
        only station: 0/0, remote removal: 0/0
```

The following line indicates that Token Ring communication has been enabled on the interface. If this line of output appears, the message "Source Route Bridge capable" should appear in the **show interfaces tokenring** display.

```
Bridge: local 3330, bnum 1, target 3583
```

Table 24, Part 2 describes the fields shown in the following line of sample output:

```
max_hops 7, target idb: 0x0, not local
```

Table 24, Part 2 show controllers token Field Descriptions

Field	Description
max_hops 7	Maximum number of bridges.
target idb: 0x0	Destination interface definition.
not local	Interface has been defined as a remote bridge.

The following line is specific to the hardware:

```
Interface failures: 0 -- Bkgnd Ints: 0
```

In the following line, transmit (TX) shorts are the number of packets the interface sends that are discarded because they are smaller than the medium's minimum packet size. TX giants are the number of packets the interface sends that are discarded because they exceed the medium's maximum packet size.

```
TX shorts 0, TX giants 0
```

The following line indicates the state of the controller. Possible values are active, failure, inactive, and reset.

```
Monitor state: (active)
```

The following line displays detailed information relating to the monitor state shown in the previous line of output. This information relates to the firmware on the controller. This information is relevant to Cisco engineers only if the monitor state is something other than active.

```
flags 0xC0, state 0x0, test 0x0, code 0x0, reason 0x0
```

Table 24, Part 3 describes the fields in the following line of output:

```
f/w ver: 1.0 expr 0, chip f/w: '000000.ME31100', [bridge capable]
```

Table 24, Part 3 show controllers token Field Descriptions

Field	Description
f/w ver: 1.0	Version of Cisco firmware on the board.
chip f/w: '000000.ME31100'	Firmware on the chipset.
[bridge capable]	Interface has not been configured for bridging, but it has that capability.

The following line displays the version numbers for the kernel and the accelerator microcode of the Madge firmware on the board; this firmware is the Logical Link Control (LLC) interface to the chipset:

```
SMT form of this command s: 1.01 kernel, 4.02 fastmac
```

The following line displays LAN Network Manager information that relates to ring status:

```
ring mode: F00, internal enables: SRB REM RPS CRS/NetMgr
```

The following line corresponds to the functional address and the group address shown in **show interfaces tokenring** output:

```
internal functional: 0000011A (0000011A), group: 00000000 (00000000)
```

The following line displays interface board state information that is proprietary:

```
if_state: 1, ints: 0/0, ghosts: 0/0, bad_states: 0/0
```

The following lines display information that is proprietary. Our engineers use this information for debugging purposes:

```
t2m fifo purges: 0/0
t2m fifo current: 0, t2m fifo max: 0/0, proto_errs: 0/0
```

Each of the fields in the following line maps to a field in the **show source bridge** display, as follows: ring maps to srn; bridge num maps to bn; target maps to trn; and max hops maps to max:

```
ring: 3330, bridge num: 1, target: 3583, max hops: 7
```

In the following lines of output, the number preceding the slash (/) indicates the count since the value was last displayed; the number following the slash (/) indicates the count since the system was last booted:

```
Packet counts:
       receive total: 298/6197, small: 298/6197, large 0/0
```

In the following line, the number preceding the slash (/) indicates the count since the value was last displayed; the number following the slash (/) indicates the count since the system was last booted. The runts and giants values that appear here correspond to the runts and giants values that appear in **show interfaces tokenring** output:

```
runts: 0/0, giants: 0/0
```

The following lines are receiver-specific information that Cisco engineers can use for debugging purposes:

```
local: 298/6197, bridged: 0/0, promis: 0/0
bad rif: 0/0, multiframe: 0/0
ring num mismatch 0/0, spanning violations 0
transmit total: 1/25, small: 1/25, large 0/0
runts: 0/0, giants: 0/0, errors 0/0
```

The following lines include very specific statistics that are not relevant in most cases, but exist for historical purposes. In particular, the internal errors, burst errors, ari/fci, abort errors, copy errors, frequency errors, dma bus errors, and dma parity errors fields are not relevant.

```
Internal controller counts:
 line errors: 0/0, internal errors: 0/0
 burst errors: 0/0, ari/fci errors: 0/0
 abort errors: 0/0, lost frame: 0/0
 copy errors: 0/0, rcvr congestion: 0/0
 token errors: 0/0, frequency errors: 0/0
 dma bus errors: -/-, dma parity errors: -/-
```

The following lines are low-level Token Ring interface statistics relating to the state and status of the Token Ring with respect to all other Token Rings on the line:

```
Internal controller smt state:
 Adapter MAC:     0000.3080.6f40, Physical drop:     00000000
 NAUN Address:    0000.a6e0.11a6, NAUN drop:         00000000
 Last source:     0000.a6e0.11a6, Last poll:         0000.3080.6f40
 Last MVID:       0006,           Last attn code:    0006
 Txmit priority:  0006,           Auth Class:        7FFF
 Monitor Error:   0000,           Interface Errors:  FFFF
 Correlator:      0000,           Soft Error Timer:  00C8
 Local Ring:      0000,           Ring Status:       0000
 Beacon rcv type: 0000,           Beacon txmit type: 0000
```

show dlsw capabilities

To display the configuration of a specific peer or all peers, use the **show dlsw capabilities** command in privileged EXEC mode.

show dlsw capabilities [**interface** *type number* | **ip-address** *ip-address* | **local**]

Syntax Description

interface *type number*	(Optional) Specifies the interface type and number for which the data-link switching plus (DLSw+) capabilities are to be displayed.
ip-address *ip-address*	(Optional) Specifies a peer by its IP address.
local	(Optional) Specifies the local DLSw+ peer.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw capabilities** command:

```
Router# show dlsw capabilities

DLSw: Capabilities for peer 10.1.1.6(2065)
   vendor id (OUI)         : '00C' (cisco)
   version number          : 1
   release number          : 0
   init pacing window      : 20
   unsupported saps        : none
   num of tcp sessions     : 1
   loop prevent support    : no
   icanreach mac-exclusive : no
   icanreach netbios-excl. : no
   reachable mac addresses : none
   reachable netbios names : none
   cisco version number    : 1
   peer group number       : 0
   border peer capable     : no
   peer cost               : 3
   biu-segment configured  : no
   UDP Unicast support     : yes
   local-ack configured    : yes
   priority configured     : no
   configured ip address   : 1.1.1.6
   peer type                : conf
   version string           :
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-JSV-M), Version 11.3(4), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Tue 16-Jun-98 04:29 by phanguye
```

Table 25 describes the fields shown in the display.

Table 25 show dlsw capabilities Field Descriptions

Field	Description
vendor id (OUI)	Vendor ID.
version number	RFC 1795 version of the Sequenced Packet Protocol (SSP) protocol.
release number	RFC 1795 release of the SSP protocol
init pacing window	Initial pacing window.
unsupported saps	Unsupported service access point (SAP)s.
num of tcp sessions	Number of TCP sessions.
loop prevent support	No loop prevent support.
icanreach mac-exclusive	Configured MAC addresses that the router can reach.
icanreach netbios-excl.	Configured NetBIOS names that the router can reach.
reachable mac addresses	Reachable MAC addresses.
reachable netbios name	Reachable NetBIOS names.
cisco version number	Cisco version number.
peer group number	Peer group member number.
border peer capable	Border peer capability.
peer cost	Peer cost.
biu-segment configured	Basic information unit (BIU) segment configured.
UDP Unicast support	User Datagram Protocol (UDP) unicast support.
local-ack configured	Local acknowledgment capable.
priority configured	Priority capability.
configured ip address	Configured IP address.
peer type	Peer type can be peer-on-demand or promiscuous.
version string	Cisco IOS software version information.

show dlsw circuits

To display the state of all circuits involving this MAC address as a source and destination, use the **show dlsw circuits** command in privileged EXEC mode.

show dlsw circuits [**detail**] [**mac-address** *address* | **sap-value** *value* | **circuit id**]

Syntax Description

detail	(Optional) Display circuit state information in expanded format.
mac-address *address*	(Optional) Specifies the MAC address to be used in the circuit search.
sap-value *value*	(Optional) Specifies the service access point (SAP) to be used in the circuit search.
circuit id	(Optional) Specifies the circuit ID of the circuit index.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw circuits** command:

```
Router# show dlsw circuits

Index           local addr(lsap)    remote addr(dsap)  state          uptime
4060086272      4000.0000.0056(F0)  4001.0000.0049(F0) CONNECTED      00:00:13
Total number of circuits connected: 1
```

The following is sample output from the **show dlsw circuits** command with the **detail** argument:

```
Router# show dlsw circuits detail

Index   local addr(lsap)    remote addr(dsap)   state uptime
194 0800.5a9b.b3b2(F0)  800.5ac1.302d(F0)  CONNECTED 00:00:13
        PCEP: 995AA4     UCEP: A52274
        Port: To0/0      peer 172.18.15.166(2065)
        Flow-Control-Tx SQ CW:20, Permitted:28; Rx CW:22, Granted:25 Op:
IWO
        Congestion: LOW(02), Flow Op: Half: 12/5 Reset 1/0
        RIF = 0680.0011.0640
```

Table 26 describes the fields shown in the display.

Table 26 show dlsw circuits Field Descriptions

Field	Description
Index	Number the software uses to reference an individual circuit.
local addr(lsap)	MAC address and SAP value used by end station closest to this data-link switching plus (DLSw+) peer.
remote addr(dsap)	MAC address and SAP value used by end station that is across the peer connection (remote).
state	Indicates whether circuit has completed establishment.
uptime	Length of time a circuit has been connected.
Total number of circuits connected	Number of total connected circuits. If a circuit has not completed connection, it will not show a value.
PCEP, UCEP	Internal correlators used as labels for communication internal to the router between DLSw+ and Logical Link Control, type 2 (LLC2), Synchronous Data Link Control (SDLC), or Qualified Logical Link Control (QLLC).
Port	Local port over which this circuit has been established or DLSw interface to the bridge group.
Flow Control (Tx and Rx)	Reports DSLw+ flow control windows as described in Section 8 of RFC 1795.
SQ	Two flags indicating congestion toward the remote peer. These flags are displayed only when the circuit is congested.
S	Data flow from the local station has been stopped. This results in LLC2 or SDLC sending Receiver Not Ready (RNR) frames.
Q	Data frames are being queued for transport to the remote peer.
CW	Current pacing window. See RFC 1795.
Permitted	Packet counter for tx. See RFC 1795.
Granted	Packet counter for rx. See RFC 1795.
Op	Next flow indicator (FCI) that will be sent to the remote peer. See RFC 1795.
Congestion	Data flow indicator from router to station is congested. Values are Low, Medium, High, and Max.
Flow Op	Amount of Reset Window Operator and Half Window Operator being sent or received. See RFC 1795.
RIF	Routing Information Field used over the local port for data traversing this circuit (if appropriate).

show dlsw circuits history

To display the details of the last status of all DLSW circuits either currently active or not active, use the **show dlsw circuits history** command in privileged EXEC mode.

show dlsw circuits history [**detail**] [**mac-address** *address* | **sap-value** *value* | **circuit id**]

Syntax Description

detail	(Optional) Displays details for all remote circuits in the connected state.
mac-address *address*	(Optional) Specifies the MAC address to be used for all remote circuits.
sap-value *value*	(Optional) Specifies the service access point (SAP) to be used for all remote circuits.
circuit id	(Optional) Specifies the circuit ID of a specific remote circuit.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show dlsw circuits history** command keeps the history for the last 32 circuits. For every circuit, the command stores a maximum of 16 entries.

Examples

The following is sample output from the **show dlsw circuits history** command:

```
Router# show dlsw circuits history

Circuit history kept for last 32 circuits using 4096 bytes:
Index           local addr(lsap)    remote addr(dsap)  remote peer
1761607680      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198
3657433089      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198 Ckt Active
```

The following is sample output from the **show dlsw circuits history** command with the **detail** keyword:

```
Router# show dlsw circuits history detail

Circuit history kept for last 32 circuits, using 4096 bytes
Index           local addr(lsap)    remote addr(dsap)  remote peer
1761607680      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198
        Created at   : 08:19:14.440 EDT Wed Sep 21 2005
        Connected at : 08:19:14.476 EDT Wed Sep 21 2005
        Destroyed at : 08:20:21.159 EDT Wed Sep 21 2005
        Local Corr   : 1761607680   Remote Corr: 1962934272
        Bytes:             633/731        Info-frames:           7/7
        XID-frames:          4/5          UInfo-frames:          0/0
        Flags: Remote created, Local connected
        Last events:
         Current State        Event             Add. Info  Next State
        ------------------------------------------------------------------
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN halt-noack       0x0      HALT_NOACK_PEND
        HALT_NOACK_PEND      DLC DiscCnf          0x0      CLOSE_PEND
        CLOSE_PEND           DLC DiscInd          0x0      CLOSE_PEND
        CLOSE_PEND           DLC CloseStnCnf      0x0      DISCONNECTED

3657433089      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198 Ckt Active
        Created at   : 08:20:51.146 EDT Wed Sep 21 2005
        Connected at : 08:20:51.182 EDT Wed Sep 21 2005
        Local Corr   : 3657433089   Remote Corr: 3137339393
        Bytes:            633/731        Info-frames:           7/7
        XID-frames:         4/5          UInfo-frames:          0/0
        Flags: Remote created, Local connected
        Last events:
        Current State        Event             Add. Info  Next State
        ------------------------------------------------------------------
        CONNECT_PENDING      WAN contacted        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC ConnectCnf       0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            WAN infoframe        0x0      CONNECTED
        CONNECTED            DLC DataInd          0x0      CONNECTED
```

The following is sample output from the **show dlsw circuits history** command for specific circuits only:

```
Router# show dlsw circuits history mac-address 0000.6666.4242

Circuit history kept for last 32 circuits, using 4096 bytes
Index           local addr(lsap)    remote addr(dsap)  remote peer
1761607680      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198
3657433089      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198 Ckt Active
Router# show dlsw circuits history detail mac-address 4000.1000.2000
Circuit history kept for last 32 circuits, using 4096 bytes
Index           local addr(lsap)    remote addr(dsap)  remote peer
1761607680      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198
3657433089      0000.6666.4242(04)  4000.1000.2000(04) 172.18.62.198 Ckt Active
```

Table 27 show dlsw circuits history Field Descriptions

Field	Description
Index	Number the software uses to reference an individual circuit.
local addr(lsap)	MAC address and SAP value used by the end station that is closest to this data-link switching plus (DLSw+) peer.
remote addr(dsap)	MAC address and SAP value used by the end station that is across the peer connection (remote).
Ckt Active	Indicates a circuit that is Active.
remote peer	IP address of the peer that is used by the individual circuit.
Ckt Active	Indicates a circuit that is Active.
Local Corr	Circuit ID of the local router.
Remote Corr	Circuit ID of the peer.
Bytes	Bytes that are transmitted and bytes that are received.
Info-frames	Transmitted frames/received frames. Info-frames carry the actual information that you want to transmit or received.
XID-frames	Transmitted XID's/received XID's. XIDs are exchange ids.
Uinfo-frames	Unnumbered information frames that use the Logical Link Control 1(llc1) mode with no guaranteed delivery and no retransmission of the information frame.
Flags	Flags that are created can be either local or remote: • local = This router has started the circuit. • remote = Partner DLSw peer has started the circuit. Connected can be either local or remote: • local = This router has received the Set Asynchronous Balanced Mode Extended (SABME) from the end system. The router transmits a UA back in response. • remote = This router has received a DLSw contacted primitive from the DLSw partner and is sending out a SABME to the end system, receiving a UA back in response.
Current State	Current state of the finite state machine.
Next State	The state to which the transition occurs is based on the event.
CONNECTED	The DLSw+ circuit is fully established and connected end to end.
HALT_NOACK_PEND	Indicates a state for which the DLSw peer is lost and the local router is awaits the Disc.Cnf or Close_Stn.Cnf signal.
CLOSE_PEND	DLSw is awaiting Close_Stn.Cnf with a disc confirmation from the end station and also from the DLSw partner.
DISCONNECTED	A state where no DLSw circuit exists.
LOCAL_RESOLVE	DLSw is awaiting the Req_Opn_Stn_confirm signal.
REMOTE_RESOLVE	Successful circuit end point (CEP) creation, which receives a Canureach_Ex.
CKT_ESTABLISHED	The two end stations are exchanging Exchange Ids (XID).

Table 27 show dlsw circuits history Field Descriptions (continued)

Field	Description
CKT_PENDING	DLSw is awaiting CONTACTED, having received a SABME and sending a CONTACT to the partner. The partner must send out the SABME, get the UA and respond with CONTACTED
CONTACT_PENDING	DLSw is awaiting DLC_CONTACTED, having received the CONTACT from the partner.
CKT_RESTART	The data link switch (DLS) that originated the reset is awaiting the restart of the data link and the DL_RESTARTED response to a RESTART_DL_message.
RESTART_PENDING	The remote DLS is awaiting the DLC_DL_HALTED indication following the DLC_HALT_DL request.
DISC_PENDING	DLSw is awaiting Ssp dl_Halted.
HALT_PENDING	DLSw is awaiting Disc.dnf.
HALT_NOACK_PEND	Indicates a state in which the DLSw peer is lost and the local router is awaits the Disc.Cnf or Close_Stn.Cnf signal.
CLOSE_PEND	DLSw is awaiting Close_Stn.Cnf having received a Disc.Cnf from the end station and also from the DLSw partner.
Event	An incident or occurrence corresponding to a state.
ADM Stop	A clear DLSw circuit or the DLSw peer goes down.
ADM RingStop	DLSw configuration gets removed.
ADM WANFailure	The peer is down. See RFC1795.
WAN contact	The WAN connection is fully established. See RFC1795.
WAN contacted	A UA received in response to a SABME. See RFC1795.
WAN infoframe	An infoframe (data containing a valid payload) is received on the WAN.See RFC1795.
DLC DataInd	An infoframe is received from the local media. See RFC1795.
DLC ConnectCnf	A UA is going out on the local interface. See RFC1795.

Related Commands

Command	Description
show dlsw circuits	Displays the state of all circuits involving a common MAC address as a source and destination.

show dlsw fastcache

To display the fast cache for Fast Sequenced Transport (FST) and direct-encapsulated peers, use the **show dlsw fastcache** command in privileged EXEC mode.

show dlsw fastcache

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw fastcache** command with an FST peer:

```
Router# show dlsw fastcache

    peer              local-mac      remote-mac   l/r sap rif
FST 10.2.32.1       0800.5a8f.881c 0800.5a8f.8822 04/04 0680.02D5.1360
```

The following is sample output from the **show dlsw fastcache** command:

```
Router# show dlsw fastcache

    peer              local-mac      remote-mac   l/r sap rif

IF Se1  0800.5a8f.881c  0800.5a8f.8822 F0/F0 0680.02D5.1360
```

Table 28 describes the fields shown in the display.

Table 28 show dlsw fastcache Field Descriptions

Field	Description
peer	Peer in which the router is connected. Could represent either an IP address or interface.
local-mac	Local MAC address.
remote-mac	Remote MAC address.
l/r sap	Local or remote service access point (SAP) value.
rif	Routing Information Field (RIF) value.

show dlsw local-circuit

To display the state of all locally-switched DLSw+ circuits, use the **show dlsw local-circuit** privileged EXEC command.

show dlsw local-circuit [**mac-address** *address* | **sap-value** *value* | *circuit-id*]

Syntax Description

mac-address *address*	(Optional) Specifies the MAC address to be used in the circuit search.
sap-value *value*	(Optional) Specifies the SAP to be used in the circuit search.
circuit-id	(Optional) Specifies the circuit ID of the circuit index. The valid range is 0 to 4294967295.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw local-circuit** command:

```
Router# show dlsw local-circuit

~ key         mac-addr    sap    state         port       rif
34886696   4000.1111.22c1 04  CONNECTED      Se2/0      --no rif--
~                 PCEP: 2145198  UCEP: 2145428
~          4000.3745.0001 04  CONNECTED      DL0         --no rif--
~                 PCEP: 2176C90  UCEP: 2145428
```

Table 29 describes significant fields shown in the display

Table 29 show dlsw local-circuit Field Descriptions

Field	Description
mac-addr	MAC address of the remote peer connection.
SAP	SAP value used by the remote peer.
state	Indicates whether circuit has completed establishment.
Port	Local port over which this circuit has been established or DLSw interface to the bridge group.

Table 29 show dlsw local-circuit Field Descriptions (continued)

Field	Description
RIF	Routing Information Field used over the local port for data traversing this circuit (if appropriate).
PCEP, UCEP	Internal correlators used as labels for communication internal to the router between DLSw+ and LLC2, SDLC, or QLLC.

show dlsw peers

To display data-link switching plus (DLSw) peer information, use the **show dlsw peers** command in privileged EXEC mode.

show dlsw peers [**interface** *type number* | **ip-address** *ip-address* | **ssp-dlx** [**interface** *type number* | **ip-address** *ip-address*] | **udp**]

Syntax Description

interface *type number*	(Optional) Specifies a remote peer by a direct interface.
ip-address *ip-address*	(Optional) Specifies a remote peer by its IP address.
ssp-dlx	(Optional) Details Sequenced Packet Protocol (SSP) and Data Link Exchange (DLX) primitive frames received and sent by a TCP or Logical Link Control, type 2 (LLC2) peer.
udp	(Optional) Displays User Datagram Protocol (UDP) frame forwarding statistics for specified peers.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	The **ssp-dlx** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw peers** command:

```
Router# show dlsw peers udp

Peers:   tot-Q'd    total-rx  total-tx    tot-retx  tot-drop curr-Q'd TCP uptime
1.1.1.      0                                               23
0                                            0                                     0
                   0                         0      00:01:02
Total number of connected peers: 2
Total number of connections:     8
```

The following is sample output from the **show dlsw peers** command with a TCP connection:

```
Router# show dlsw peers

Peers:                state     pkts_rx   pkts_tx  type  drops ckts TCP   uptime
 TCP 10.1.91.1
     High priority   CONNECT         43        40  conf      0    1   0 00:01:02
```

```
   Medium priority   CONNECT          0        0  conf      0    -   0 00:01:02
   Normal priority   CONNECT          4       41  conf      0    -   5 00:01:02
      Low priority   CONNECT          1        0  conf      0    -   0 00:01:02
 TCP 10.1.93.1
     High priority   CONNECT          3        3  conf      0    0   0 00:00:58
   Medium priority   CONNECT          0        0  conf      0    -   0 00:00:58
   Normal priority   CONNECT          0        0  conf      0    -   0 00:00:58
      Low priority   CONNECT          0       39  conf      0    -   0 00:00:58
Total number of connected peers: 2
Total number of connections:     8
```

The following is sample output from the **show dlsw peers** command with a Direct Frame Relay connection:

```
Router # show dlsw peers

Peers:                state    pkts_rx pkts_tx  type  drops ckts TCP    uptime
IF         SE1 16
        connect                 53                                               2597
        conf                                       0
-                  -            00:04:09
Total number of connected peers: 2
Total number of connections:     8
```

The following is sample output from the **show dlsw peers** command with a Direct Frame Relay with local acknowledgment (LLC2) connection:

```
Router # show dlsw peers

Peers:                state     pkts_rx pkts_tx  type  drops ckts TCP    uptime
LLC2 SE116                                     connect
1179                                                108                 conf
0   1               -                  -                                        00:04:09
Total number of connected peers: 2
Total number of connections:     8
```

The following is sample output from the **show dlsw peers ssp-dlx** command:

```
Router # show dlsw peers ssp-dlx

Peer:10.1.1.6                               received transmitted
    CUR_ex Can U Reach Explorers                   5           2
    CUR_cs Can U Reach Circuit Start               2           5
    ICR_ex I Can Reach Explorers                   4           5
    ICR_cs I Can Reach Circuit Start               4           1
    ACK Reach Acknowledgement                      1           4
    XID Frame                                     22          20
    CONQ Contact Remote Station                    4           0
    CONR Remote Station Contacted                  0           4
    INFO Information (I) Frame                    39          39
    HLTQ Halt Data Link                            0           1
    HLTR Data Link Halted                          1           0
    HLTN Halt Data Link (no ack)                   1           2
    CAPX Capabilities Exchange                     2           2
    Total SSP Primitives                          85          85

    DLX Peer Test Request                        122         146
    DLX Peer Test Response                       146         122
    DLX Border to Border Message                  53           9
    --> SSP:CUR Can U Reach                      53           2
    --> SSP:DATA Data Frames                      0           7

    Last SSP Received: INFO
    Last SSP Sent: ICR

Total number of connected peers:1
Total number of connections:    1
```

Table 30 describes the significant fields shown in the display.

Table 30 show dlsw peers Field Descriptions

Field	Description
Peers	Information related to the remote peer, including encapsulation type, IP address (if using Fast Sequenced Transport [FST] or TCP)and interface number (if using direct encapsulation).
tot-Q'd	Number of UDP packets that have been queued because of TCP congestion.
total-rx	Number UDP packets received from the peer.
total-tx	Number of UDP packets sent to the peer.
tot-retx	Number of reachability resends (for example, DLSw+ retries NQ_ex and CUR_ex) when originally sent via UDP.
tot-drop	Number of queued UDP packets that were dropped because of persistent TCP congestion.
curr-Q'd	Number of current UDP packets queued because of TCP congestion.
TCP	Number of packets on the TCP output queue.
state	State of the peer: • CONNECT—normal working peer. • DISCONN—peer is not connected. • CAP_EXG—capabilities exchange mode. Waiting for capabilities response. • WAIT_RD—TCP write pipe (local port 2065) is open and peer is waiting for remote peer to open the read port (local port 2067). This field applies only to TCP peers. • WAN_BUSY—TCP outbound queue is full. This field applies only to TCP peers.
pkts_rx	Number of received packets.
pkts_tx	Number of sent packets.
type	Type of remote peer: • conf—configured • prom—promiscuous • pod—peer on demand

Table 30 show dlsw peers Field Descriptions (continued)

Field	Description
drops	Number of drops done by this peer. Reasons for the counter to increment: • WAN interface not up for a direct peer. • DLS tries to send a packet before the peer is fully connected (waiting for TCP event or capabilities event). • Outbound TCP queue full. • FST sequence number count mismatch. • Cannot get buffer to “slow switch” FST packet. • CiscoBus controller failure on high end (cannot move packet from receive buffer to send buffer, or vice versa). • Destination IP address of FST packet does not match local peer ID. • WAN interface not up for an FST peer. • No source-route bridging (SRB) route cache command configured. • Madge ring buffer is full on low-end systems (WAN feeding LAN too fast).
ckts	Number of active circuits through this peer. This field applies only to TCP and LLC2 transport peer types.
uptime	How long the connection has been established to this peer.
total number of connected peers	Total number of connected peers.
total number of connections	Total number of active circuit connections.

show dlsw reachability

To display data-link switching plus (DLSw+) reachability information, use the **show dlsw reachability** command in privileged EXEC mode.

show dlsw reachability [**group** [*value*] | **local** | **remote** | **mac-address** [*address*] | **netbios-names** [*name*]]

Syntax Description

group	(Optional) Displays contents of group reachability cache only.
value	(Optional) Specifies the group number for the reachability check. Only displays group cache entries for the specified group. The valid range is from 1 to 255.
local	(Optional) Displays contents of local reachability cache only.
remote	(Optional) Displays contents of remote reachability cache only.
mac-address	(Optional) Displays DLSw reachability for MAC addresses only.
address	(Optional) Specifies the MAC address for which to search in the reachability cache.
netbios-names	(Optional) Displays DLSw reachability for NetBIOS names only.
name	(Optional) Specifies the NetBIOS name for which to search in the reachability cache.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If none of the group, local, or remote options is specified, then the caches will be displayed in the following order: local, remote, and group.

Examples

The following is sample output from the **show dlsw reachability group** command:

```
Router# show dlsw reachability group

DLSw Group MAC address reachability cache list
Mac Addr Group
0000.3072.1070     10
DLSW Group NetBIOS Name reachability cache list
```

```
NetBIOS Name    Group
```

The following is sample output from the **show dlsw reachability** command:

```
Router# show dlsw reachability

DLSw MAC address reachability cache list
Mac Addr        status     Loc.    peer/port          rif
0000.f641.91e8  SEARCHING  LOCAL
0006.7c9a.7a48  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
0800.5a4b.1cbc  SEARCHING  LOCAL
0800.5a54.ee59  SEARCHING  LOCAL
0800.5a8f.9c3f  FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
4000.0000.0050  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
4000.0000.0306  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
4000.0000.0307  SEARCHING  LOCAL
4000.0000.0308  SEARCHING  LOCAL
4000.1234.56c1  FOUND      LOCAL   Serial3/7      --no rif--
4000.1234.56c2  FOUND      LOCAL   Serial3/7      --no rif--
4000.3000.0100  FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
4000.4000.ff40  SEARCHING  LOCAL
4000.7470.00e7  SEARCHING  LOCAL
4000.ac0b.0001  FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
4001.0000.0064  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
4001.3745.1088  FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
4100.0131.1030  FOUND      LOCAL   TokenRing0/0
10B0.FFF1.4041.0041.3E71.A041.0DE5.0640

DLSw NetBIOS Name reachability cache list
NetBIOS Name    status     Loc.    peer/port          rif
APPNCLT2        FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
```

The following is sample output from the **show dlsw reachability** command with the **mac-address** keyword:

```
Router# show dlsw reachability mac-address 4000.00000306

DLSw MAC address reachability cache list
Mac Addr        status     Loc.    peer/port          rif
4000.0000.0306  FOUND      LOCAL   TokenRing0/0   0CB0.0011.3E71.A041.0DE5.0640
```

The following is sample output from the **show dlsw reachability** command with the **netbios-names** keyword:

```
Router# show dlsw reachability netbios-names

DLSw NetBIOS Name reachability cache list
NetBIOS Name    status     Loc.    peer/port          rif
APPNCLT2        FOUND      LOCAL   TokenRing0/0   08B0.A041.0DE5.0640
```

Table 31 describes the significant fields shown in the display.

Table 31 show dlsw reachability Field Descriptions

Field	Description
Mac Addr	MAC address of station being sought (destination MAC address of canureach_ex packet).
NetBIOS Name	NetBIOS name of station being sought (destination MAC address of NQ_ex packet).

Table 31 show dlsw reachability Field Descriptions (continued)

Field	Description
status	Result of station search. The status can be one of the following: • FOUND—Station has recently sent a broadcast or responded to a broadcast. • SEARCHING—Router has sent a broadcast to this station and is waiting for a response. • NOT_FOUND—Negative caching is on, and the station has not responded to queries. • UNCONFIRMED—Station is configured, but DLSw has not verified it. • VERIFY—Cache information is being verified because cache is going stale, or the user configuration is being verified.
Loc.	Location of station. LOCAL indicates that the station is on the local network. REMOTE indicates that the station is on the remote network.
peer/port	Peer/port number. If the Loc. field lists a REMOTE station, the peer/port field indicates the peer through which the remote station is reachable. If the Loc. field lists a LOCAL station, the peer/port field indicates the port through which the local station is reachable. For ports, the port number and slot number are given. Pxxx-Syyy denotes port xxx slot yyy. If the station is reachable through a bridge group, that is shown by TBridge-xxx.
rif	Displays the Routing Information Field (RIF) in the cache. This column applies only to LOCAL stations. If the station was reached through a medium that does not support RIFs (such as Synchronous Data Link Control [SDLC] or Ethernet) then "--no rif--" is shown.

show dlsw statistics

To display the number of frames that have been processed in the local, remote, and group cache, use the **show dlsw statistics** command in privileged EXEC mode.

show dlsw statistics [**border-peers**]

Syntax Description

border-peers	(Optional) Displays the number of frames processed in the local, remote, and group caches.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw statistics** command. The output displays the number of frames processed in the local, remote, and group cache.

```
Router# show dlsw statistics border-peers

100 Border Peer Frames processed
10 Border frames found Local
20 Border frames found Remote
17 Border frames found Group Cache
```

show dlsw transparent cache

To display the master circuit cache for each transparent bridged domain, use the **show dlsw transparent cache** command in privileged EXEC mode.

show dlsw transparent cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Issue the **show dlsw transparent cache** command on the master router of the transparent bridged domain.

Examples

The following is sample output from the **show dlsw transparent cache** command:

```
Router# show dlsw transparent cache

Interface Ethernet0/1
 Circuit Cache
local addr(lsap)    remote addr(dsap)  state          Owner
0000.3028.92b6(08)  0007.0db1.238c(08) POSITIVE        SELF
0000.3028.92b6(08)  0008.dec3.609e(12) NEGATIVE        0009.fa50.0b1c
Total number of circuits in the Cache:2
```

show dlsw transparent map

To display MAC address mappings on the local router and any mappings for which the local router is acting as backup for a neighbor peer, use the **show dlsw transparent map** command in privileged EXEC mode.

show dlsw transparent map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Issue the **show dlsw transparent map** command to ensure that the local MAC address is the address created in the **dlsw transparent map** command. The command should be issued on all the routers configured for the Ethernet Redundancy feature to ensure the local MAC addresses match.

Examples

The following is sample output from the **show dlsw transparent map** command on two routers configured for the Ethernet Redundancy feature:

```
Router6# show dlsw transparent map

Interface Ethernet6/2
      LOCAL Mac          REMOTE MAC      BACKUP
      ---------          ----------      ------
    0008.dec3.0080     0008.dec3.609e    0007.7fb0.1080     STATIC
    0008.dec3.0040     0008.dec3.609e    0007.7fb0.1080     DYNAMIC(Passive)

Router7# show dlsw transparent map

Interface Ethernet0/1
      LOCAL Mac          REMOTE MAC      BACKUP
      ---------          ----------      ------
    0008.dec3.0080     0008.dec3.609e    0006.3a0a.1a55     DYNAMIC(Passive)
    0008.dec3.0040     0008.dec3.609e    0006.3a0a.1a55     STATIC
```

The output from Router 6 and Router 7 shows the created MAC addresses are 0008.dec3.0080 and 0008.dec3.0040.

show dlsw transparent neighbor

To display data-link switching plus (DLSw) neighbors in a transparent bridged domain, use the **show dlsw transparent neighbor** command in privileged EXEC mode.

show dlsw transparent neighbor

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dlsw transparent neighbor** command:

```
Router# show dlsw transparent neighbor

Interface ATM0.1
0006.e278.6c0e  SELF                      Master
0009.fa50.0b1c  Rcvd Master-Accepted      VALID
```

The output shows that Router 7 is the master router whose MAC address is 0006.e278.6c0e. The other router, with a MAC address of 0009.fa50.0b1c, is a slave router on the common domain. The master router received a packet from the slave and notes the router is VALID.

show drip

To display the status of the duplicate ring protocol (DRiP) database for a router or an Route Switch Module (RSM), use the **show drip** command in privileged EXEC mode.

show drip

Syntax Descriptions

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show drip** command:

```
Router# show drip

DRIP Database for Mgmt Domain Fast Ethernet4/0
--------------------------------------------------
Mac Address 0010-A6AE-B440
Vlan     100    Status    30 : l-active, l-config,

Mac Address 0010-2F72-C800
Vlan      20    Status    0C : r-active, r-config,
Vlan    1003    Status    0C : r-active, r-config,

Statistics:
Advertisements received            126
Advertisements processed           1
Advertisements transmitted         131
Last revision transmitted          0x84
Last changed revision transmitted  0x2
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
interface vlan	Configures a Token Ring or Ethernet interface on the RSM.
show vlans	Displays virtual LAN subinterfaces.

show dspu

To display the status of the downstream physical unit (DSPU) feature, use the **show dspu** command in privileged EXEC mode.

show dspu [**pool** *pool-name* | **pu** {*host-name* | *pu-name*}] [**all**]

Syntax Description

pool *pool-name*	(Optional) Name of a pool of logical unit (LU)s (as defined by the **dspu pool** command).
pu	(Optional) Name of defined physical unit (PU) (as defined by either the **dspu pu** or the **dspu host** command).
host-name	Name of a host defined in a **dspu host** command.
pu-name	Name of a PU defined in a **dspu pu** command.
all	(Optional) Displays a detailed status.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dspu** command. It shows a summary of the DSPU status.

```
Router# show dspu

dspu host HOST_NAMEA interface PU STATUS ssssssss
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
dspu host HOST_NAMEB interface PU STATUS ssssssss
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
dspu pu PU_NAMEE interface PU STATUS ssssssss
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
dspu pu PU_NAMEF interface PU STATUS ssssssss
```

```
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
```

The following is sample output from the **show dspu** command with the **pu** keyword:

```
Router# show dspu pu putest

dspu pu PUTEST interface PU STATUS ssssssss
RMAC remote_mac RSAP remote_sap LSAP local_sap
XID xid RETRIES retry_count RETRY_TIMEOUT retry_timeout
WINDOW window_size MAXIFRAME max_iframe
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
```

The following is sample output from the **show dspu** command with the **all** keyword:

```
Router# show dspu pu putest all

dspu pu PUTEST interface PU STATUS ssssssss
RMAC remote_mac RSAP remote_sap LSAP local_sap
XID xid RETRIES retry_count RETRY_TIMEOUT retry_timeout
WINDOW window_size MAXIFRAME max_iframe
FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LU nnn PEER PU HOST_NAMEA PEER LU nnn STATUS tttttttt
       FRAMES RECEIVED nnnnnn FRAMES SENT nnnnnn
LU nnn PEER PU HOST_NAMEA PEER LU nnn STATUS tttttttt
       FRAMES RECEIVED nnnnnn, FRAMES SENT nnnnnn
LU nnn PEER PU HOST_NAMEB PEER LU nnn STATUS tttttttt
       FRAMES RECEIVED nnnnnn, FRAMES SENT nnnnnn
```

The following example shows a summary of the LUs in a pool:

```
Router# show dspu pool poolname

dspu pool poolname host HOST_NAMEA lu start-lu end-lu
```

The following example shows the details of all the LUs in a pool:

```
Router# show dspu pool poolname all

dspu pool poolname host HOST_NAMEA lu start-lu end-lu
DSPU POOL poolname INACTIVITY_TIMEOUT timeout-value
lu nnn host HOST_NAMEA peer lu nnn pu PU_NAMEF status tttttttt
lu nnn host HOST_NAMEA peer lu nnn pu PU_NAMEF status tttttttt
lu nnn host HOST_NAMEA peer lu nnn pu PU_NAMEF status tttttttt
```

show extended channel backup

To display information about the Common Link Access for Workstations (CLAW) and offload commands for each backup group configured on Cisco Mainframe Channel Connection (CMCC) channel interfaces, use the **show extended channel backup** command in privileged EXEC mode.

show extended channel *slot/port* **backup** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
backup	Displays all **claw** or **offload** commands associated with the backup group.
ip-address	(Optional) Displays information about all devices in the backup group defined by the *ip-address* argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel backup** command:

```
Router# show extended channel 0/1 backup

Mode     Path Device IP Address: 10.11.198.2
OFFLOAD  E200   50  CISCOVM  RISPIX   TCPIP    TCPIP    TCPIP    API
OFFLOAD  E300   50  CISCOVM  RISPIX   TCPIP    TCPIP    TCPIP    API
Last statistics 4 seconds old, next in 6 seconds
```

Related Commands

Command	Description
claw (backup)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.

show extended channel cmgr

To display information about the Cisco Multipath Channel (CMPC+) transmission group (TG) connection manager, use the **show extended channel cmgr** command in privileged EXEC mode.

show extended channel *slot*/*port* **cmgr** [*tg-name*]

Syntax Description

slot	Slot number.
port	Physical channel interface port number.
tg-name	(Optional) Name of the TG.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid on the Channel Interface Processor (CIP)'s virtual channel interface or the Channel Port Adapter (CPA)'s physical channel interface.

Examples

The following is sample output from the **show extended channel cmgr** command:

```
Router# show extended channel 3/2 cmgr

CMGR:MPCPTG2  Type=PTP
  Local Group Token:0500128933                    Remote Group Token :0500993355
  Local VC Token   :0500109002                    Local Conn. Token  :0500109003
  Remote VC Token  :0500201002                    Remote Conn. Token :0500201002
  VC Status        :Active                        Connection Status  :Active

CMGR:MPCPTG3   Type=PTP
  Local Group Token:050014573                    Remote Group Token :05008984300
  Local VC Token   :0500109044                   Local Conn. Token  :0500109066
  Remote VC Token  :0500201095                   Remote Conn. Token :0500201088
  VC Status        :Active                       Connection Status  :Active
```

Table 32 describes the significant fields shown in the display.

Table 32 show extended channel cmgr Field Descriptions

Field	Description
Local Group Token	Cisco Mainframe Channel Connection (CMCC)'s Multi-Path Channel plus (MPC+) group token for this TG.
Remote Group Token	Host's MPC+ group token for this TG.
Type	Connection manager type supported is point-to-point (PTP).
Local VC Token	CMCC adapter's token for the connection manager's virtual circuit.
Remote VC Token	Host's token for the connection manager's virtual circuit.
VC Status	Valid states for a VC are: • Reset—Awaiting a connection manager virtual circuit activate indication from the host. • Active—Connection manager virtual circuit active indication was received from the host and CMCC adapter has sent a virtual circuit active indication to the host. The virtual circuit is now ready to send receive connection requests.
Local Conn.Token	CMCC's token for the connection manager's connection.
Remote Conn.Token	Host's token for the connection manager's connection.
Connection Status	Valid states for a connection manager's connection are: • Reset—Awaiting a connection manager connection request from the host. • Active—Connection is active. The host has sent a connection request and the CMCC adapter has responded with a confirmation of the connection.

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.

show extended channel cmpc

To display information about each Cisco Multipath Channel (CMPC) or CMPC+ subchannel configured on the specified channel interface, use the **show extended channel cmpc** command in privileged EXEC mode.

show extended channel *slot***/***port* **cmpc** [*path* [*device*]]

Syntax Description

slot	Slot number.
port	Physical channel interface port number.
path	(Optional) Logical channel path.
device	(Optional) Two-digit hexadecimal value that specifies a device address of the CPMC or CMPC+ subchannel. If specified, only status for that CMPC or CMPC+ device is displayed. If not specified, status for all CMPC or CMPC+ devices for the specified path is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the Cisco Mainframe Channel Connection (CMCC) adapter physical interfaces.

Examples

The following is sample output on a Cisco 7500 router from the **show extended channel cmpc** command:

```
Router# show extended channel 3/0 cmpc c020

     Path Dv  TGName    Dir    Bfrs  Status
CMPC C020 46  MVS2ISRA  READ   10    Active
CMPC C020 47  MVS2ISRA  WRITE  16    Active
CMPC C020 4A  MVS2ISR1  READ   7     Active
CMPC C020 4B  MVS2ISR1  WRITE  16    Active
CMPC C020 4C  MVS2ISR2  READ   7     Active
CMPC C020 4D  MVS2ISR2  WRITE  16    Active
CMPC C020 4E  MVS2TN    READ   0     Inactive
CMPC C020 4F  MVS2TN    WRITE  0     Inactive
```

Table 33 describes the specified fields shown in the display.

Table 33 show extended channel cmpc Field Descriptions

Field	Description
Path	CMPC or CMPC+ channel path configured.
Dv	CMPC or CMPC+ subchannel device configured.
TGName	TG name configured for the CMPC or CMPC+ subchannel.
Dir	Identifies this CMPC or CMPC+ subchannel as READ or WRITE.
Bfrs	On the read subchannel, this is the number of 4 KB-size pages that virtual telecommunications access method (VTAM) has allocated for each Read. This will match the MAXBFRU value configured in the VTAM Transport Resource List (TRL) major node. On the write subchannel, this is the maximum number of 4-KB pages VTAM can write to the CMCC adapter for a single channel I/O. The value will always be 16 for the write subchannel because the Channel Interface Processor (CIP)always allows VTAM to write up to 64 KB per channel I/O.
Status	State of the CMPC or CMPC+ subchannel. Valid values are: • Shutdown—CMCC adapter interface for this CMPC or CMPC+ subchannel is shut down. In this state, the Bfrs value is not available and will be displayed as zeros. • Inactive—CMPC or CMPC+ subchannel is not active. • XID2 Pending—exchange identification (XID)2 handshaking in progress. • Active—XID2 exchange completed; CMPC or CMPC+ subchannel is active. • Active**+**—XID2 exchange is complete; subchannel is active in High-Performance Data Transfer (HPDT) mode.

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
tg (CMPC)	Defines LLC connection parameters for the CMPC transmission group.
tg (CMPC+)	Defines IP connection parameters for the CMPC+ transmission group.
show extended channel cmgr	Displays information about the MPC+ transmission group connection manager.

show extended channel connection-map llc2

To display the number of active Logical Link Control, type 2 (LLC2) connections for each service access point (SAP) and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP, use the **show extended channel connection-map llc2** command in privileged EXEC mode.

show extended channel *slot***/***port* **connection-map llc2**

Syntax Description

slot	Slot number.
port	Port number.
connection-map llc2	Displays a connection map of LLC2 connections.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel connection-map llc2** command is valid only on the virtual channel interfaces.

Examples

The following is sample output from the **show extended channel connection-map llc2** command:

```
Router# show extended channel 1/2 connection-map llc2

LAN Token  0 Adapter   0 4000.7000.0747
 Local SAP=08 LLC2 Connections=4   CSNA Port=1 Path=C200 Device=60
 Local SAP=0C LLC2 Connections=4   CSNA Port=1 Path=C200 Device=60
 Local SAP=10 LLC2 Connections=2   CSNA Port=1 Path=C200 Device=60
 Local SAP=14 LLC2 Connections=0   CSNA Port=1 Path=C200 Device=60

LAN Token  1 Adapter   1 4000.7000.0767
 Local SAP=08 LLC2 Connections=3   CSNA Port=1 Path=C200 Device=61
 Local SAP=0C LLC2 Connections=3   CSNA Port=1 Path=C200 Device=61
 Local SAP=10 LLC2 Connections=2   CSNA Port=1 Path=C200 Device=61
 Local SAP=14 LLC2 Connections=2   CSNA Port=1 Path=C200 Device=61

LAN Token  2 Adapter   2 4000.7000.0737
 No SAPs open on this interface

 Total : SAPs opened = 8      Connections active = 20
```

show extended channel csna

To display information about the cisco systems network architecture (CSNA) subchannels configured on the specified Cisco Mainframe Channel Connection (CMCC) interface, use the **show extended channel csna** command in privileged EXEC mode.

show extended channel *slot*/*port* **csna** [*path* [*device*]] [**admin** | **oper** | **stats**]

Syntax Description

slot	Slot number.
port	Port number.
path	(Optional) A hexadecimal value in the range from 0000 to FFFF. This specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch), one digit for the control unit address, and one digit for the channel logical address. If not specified, information is displayed for all CSNA subchannels configured on the selected interface.
device	(Optional) A hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host input/output configuration program (IOCP) file. If not specified, information is displayed for all CSNA subchannels configured with the specified path on the selected interface.
admin	(Optional) Displays configured values for CSNA channel devices. If neither **admin**, **oper**, nor **stats** is specified, **admin** is the default.
oper	(Optional) Displays operational values for CSNA channel devices.
stats	(Optional) Displays statistics for CSNA channel devices.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The information that is displayed by this command is generally useful for diagnostic tasks performed by technical support personnel only.

Examples

The following is sample output from the **show extended channel csna** command. Three examples are provided, one for each type of output as specified by the **admin**, **oper**, and **stats** keywords.

The following example displays the configured values for all CSNA devices on interface channel 1/0:

```
Router# show extended channel 1/0 csna admin

     Path Dv  maxpiu       time-delay   length-delay
```

```
CSNA C200 60  64000        100          64000
CSNA C200 61  64000        100          64000
CSNA C200 62  64000        100          64000
```

The following example displays operational data for all CSNA devices configured on interface channel 1/0. The channel interface must be up (no shut) for this information to be displayed.

```
Router# show extended channel 1/0 csna oper

     Path Dv Status       SlowDown  maxpiu       time-delay   length-delay
CSNA C200 60 setupComplet off       64000        100          64000
CSNA C200 61 setupComplet off       64000        100          64000
CSNA C200 62 setupComplet off       64000        100          64000
```

The following example displays CSNA statistics for subchannel path c200, device 60. The channel interface must be up (no shut) for this information to be displayed. If the maxpiu value is reconfigured while the CSNA subchannel is active (setupComplete) then the maxpiu value displayed by the **oper** keyword is the old, operational value.

```
Router# show extended channel 1/0 csna c200 60 stats

CSNA     C200 60
Blocks Transmitted =   38979079  Received =   38979075
Bytes  Transmitted =  79251477K  Received =      13554
Slow downs Sent =          0  Received =          0
Txd by maxpiu      : Blocks =          0   Bytes =         0
Txd by time-delay  : Blocks =        222   Bytes =     12522
Txd by length-delay: Blocks =          0   Bytes =         0
```

Table 34 describes the specified fields shown in the displays.

Table 34 show extended channel csna Field Descriptions

Field	Description
Path	Path from the CSNA configuration.
Dev	Device address from the CSNA configuration.
Status	State of the CSNA device. One of the following values: • closed—Subchannel is closed. • pendingOpen—An Open Subchannel command has been received from virtual telecommunications access method (VTAM). • open—Subchannel is open. • pendingSetup—VTAM has queried Channel Interface Processor (CIP) for all configured MAC adapters. • setupComplete—All internal MAC adapter information has been collected from the CIP. The CSNA subchannel is operational. • pendingClose—A Close Subchannel command has been received from VTAM. • unknown—Current state of the CSNA subchannel cannot be determined.

Table 34 show extended channel csna Field Descriptions (continued)

Field	Description
SlowDown	Status of flow control for the CSNA device. • off—Subchannel is normal (both CSNA and VTAM are able to send data. • sent— CSNA has put VTAM into a slow down state for this CSNA subchannel. • received—VTAM has put the CSNA subchannel into a slow down state. • both—Both VTAM and the CSNA subchannel are in a slow down state. • unknown—Current state of flow control on this CSNA subchannel cannot be determined.
maxpiu	Maximum size of a channel I/O block that the CSNA subchannel can send to the host. This value may differ from the configured maxpiu value if the value is reconfigured while the CSNA subchannel is active (setupComplete). CSNA blocks Systems Network Architecture (SNA) frames into channel I/O blocks which must not exceed the maxpiu value. A length-delay value less than the maxpiu value can cause the channel I/O blocks to be limited to the lower value. The maxpiu value may be reconfigured while the subchannel is operational but the new maxpiu value does not take effect until the subchannel is reinitialized (in other words, until the XCA major node is recycled). In this case, the maxpiu value displayed with the **admin** keyword will be the new, configured value while the maxpiu displayed by the **oper** keyword will be the old, operational value.
time-delay	CSNA blocks SNA frames destined for VTAM for time-delay milliseconds from the time the first SNA frame within a channel I/O block is blocked from sending. This can increase the overall throughput of CSNA by minimizing the number of channel I/O operations. However, blocking can induce response time latency of a transaction by up to the time-delay value. If time-delay=0, CSNA ignores length-delay and puts each frame into the channel I/O block for sending to the host. Even with a time-delay=0, CSNA may still block frames while waiting for a previous channel I/O to complete.
length-delay	CSNA blocks SNA frames destined for VTAM when the current block reaches the length-delay value in size (bytes). This will increase the chance of using larger block sizes for CSNA channel I/O. SNA frames are blocked up to either time-delay milliseconds or until the block reaches the length-delay size, at which time CSNA starts the channel I/O. The length-delay is ignored if larger than the maxpiu value. It can be used to force CSNA blocking to generate smaller I/O blocks than specified by maxpiu. In general, however, larger blocks result in better channel throughput and efficiency. A value of zero causes the length-delay value to be ignored; blocking is then controlled by the maxpiu and time-delay parameters.

Table 34 show extended channel csna Field Descriptions (continued)

Field	Description
Blocks Transmitted	Number of channel I/O blocks sent to VTAM from this CSNA subchannel. The Blocks Transmitted value may be higher than the total blocks for the Txd by maxpiu, Txd by time-delay, and Txd by length-delay counters. This is due to NULL blocks (8 bytes each with no data) that CSNA sends. The channel program used for link-state advertisement (LSA) traffic consists of a write/read CCW chain. When VTAM has data for CSNA it sends it with the write CCW. When the chained read CCW is executed CSNA will respond with any pending inbound data. If CSNA has no pending inbound data the read CCW is satisfied with an 8-byte header indicating no data.
Blocks Received	Number of channel I/O blocks received from VTAM by this CSNA subchannel.
Slow downs Sent	Number of times CSNA put VTAM into a slowdown (flow control) for this subchannel device.
Slow downs Received	Number of times VTAM put CSNA into a slowdown (flow control) for this subchannel.
Txd by maxpiu Blocks/Bytes	Number of channel I/O blocks and bytes sent to VTAM by this CSNA subchannel because the size of the channel I/O block reached the maxpiu value configured for this subchannel.
Txd by time-delay Blocks/Bytes	Number of channel I/O blocks and bytes sent to VTAM by this CSNA subchannel because the blocking time delay configured for this subchannel expired.
Txd by length-delay Blocks/Bytes	Number of channel I/O blocks and bytes sent to VTAM by this CSNA subchannel because the blocking length delay configured for this subchannel was reached.

Related Commands

Command	Description
csna	Configures SNA support on a CMCC physical channel interface and specifies the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe.

show extended channel icmp-stack

To display information about the Internet Control Message Protocol (ICMP) stack running on the Cisco Mainframe Channel Connection (CMCC) channel interfaces, use the **show extended channel icmp-stack** command in user EXEC or privileged EXEC mode.

show extended channel *slot***/***port* **icmp-stack** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn3270-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The Alias addresses field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel icmp-stack** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show extended channel icmp-stack** command:

```
Router# show extended channel 0/1 icmp-stack

ICMP Statistics for IP Address 10.11.198.2
  InMsgs          : 3           InErrors        : 0           InDestUnreachs: 0
  InTimeExcds     : 0           InParmProbs     : 0           InSrcQuenchs  : 0
  InRedirects     : 0           InEchos         : 3           OutEchoReps   : 3
  OutTimestamps   : 0           OutTimestampReps: 0           OutAddrMasks  : 0
  OutAddrMaskReps: 0
ICMP Statistics for IP Address 10.11.198.3
  InMsgs          : 1           InErrors        : 0           InDestUnreachs: 0
  InTimeExcds     : 0           InParmProbs     : 0           InSrcQuenchs  : 0
  InRedirects     : 0           InEchos         : 1           OutEchoReps   : 1
  OutTimestamps   : 0           OutTimestampReps: 0           OutAddrMasks  : 0
  OutAddrMaskReps: 0
```

The following is sample output from the **show extended channel icmp-stack** for an offload device at real IP address 10.10.21.3 and alias IP address 10.2.33.88:

```
Router# show extended channel 3/1 icmp-stack

ICMP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  InMsgs          : 0           InErrors        : 0          InDestUnreachs: 0
  InTimeExcds     : 0           InParmProbs     : 0          InSrcQuenchs  : 0
  InRedirects     : 0           InEchos         : 0          OutEchoReps   : 0
  OutTimestamps   : 0           OutTimestampReps: 0          OutAddrMasks  : 0
  OutAddrMaskReps: 0
```

Table 35 describes the specified fields shown in the display.

Table 35 show extended channel icmp-stack Field Descriptions

Field	Description
Alias addresses	Virtual IP addresses assigned to the real IP address of an offload device.
InMsgs	Total number of Internet Control Message Protocol (ICMP) messages that the entity received. Note that this counter includes all those counted by icmpInErrors.
InErrors	Number of ICMP messages that the entity received but determined as having ICMP-specific errors (for example, bad ICMP checksums, bad length).
InDestUnreachs	Number of ICMP Destination Unreachable messages received.
InTimeExcds	Number of ICMP Time Exceeded messages received.
InParmPrbs	Number of ICMP Parameter Problem messages received.
InSrcQuenchs	Number of ICMP Source Quench messages received.
InRedirects	Number of ICMP Redirect messages received.
InEchos	Number of ICMP Echo (request) messages received.
OutEchoReps	Number of ICMP Echo Reply messages sent.
OutTimestamps	Number of ICMP Timestamp (request) messages sent.
OutTimestampReps	Number of ICMP Timestamp Reply messages sent.
OutAddrMasks	Number of ICMP Address Mask Request messages sent.
OutAddrMaskReps	Number of ICMP Address Mask Reply messages sent.

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.

show extended channel ip-stack

To display information about the IP stack running on Cisco Mainframe Channel Connection (CMCC) channel interfaces, use the **show extended channel ip-stack** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **ip-stack** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn327-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The Alias addresses field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel ip-stack** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show extended channel ip-stack** command:

```
Router# show extended channel 0/1 ip-stack

IP Statistics for IP Address 10.11.198.2
  Forwarding     : no          DefaultTTL     : 64          InReceives   : 165
  InHdrErrors    : 0           InAddrErrors   : 0           ForwDatagrams: 0
  InUnknownProtos: 0           InDiscards     : 0           InDelivers   : 165
  OutRequests    : 157         OutDiscards    : 0           OutNoRoutes  : 0
  ReasmTimeout   : 60          ReasmReqds     : 0           ReasmOKs     : 0
  ReasmFails     : 0           FragOKs        : 0           FragFails    : 0
  FragCreates    : 0           RoutingDiscards: 0
IP Statistics for IP Address 10.11.198.3
  Forwarding     : no          DefaultTTL     : 64          InReceives   : 77
  InHdrErrors    : 0           InAddrErrors   : 0           ForwDatagrams: 0
  InUnknownProtos: 0           InDiscards     : 0           InDelivers   : 77
  OutRequests    : 78          OutDiscards    : 0           OutNoRoutes  : 0
  ReasmTimeout   : 60          ReasmReqds     : 0           ReasmOKs     : 0
  ReasmFails     : 0           FragOKs        : 0           FragFails    : 0
  FragCreates    : 0           RoutingDiscards: 0
```

The following is sample output from the **show extended channel ip-stack** for an offload device at real IP address 10.10.21.3 and alias IP address 10.2.33.88:

```
Router# show extended channel 3/1 ip-stack

IP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  Forwarding      : no          DefaultTTL      : 64          InReceives    : 16
  InHdrErrors     : 0           InAddrErrors    : 0           ForwDatagrams: 0
  InUnknownProtos: 0            InDiscards      : 0           InDelivers    : 16
  OutRequests     : 7           OutDiscards     : 0           OutNoRoutes   : 0
  ReasmTimeout    : 60          ReasmReqds      : 0           ReasmOKs      : 0
  ReasmFails      : 0           FragOKs         : 0           FragFails     : 0
  FragCreates     : 0           RoutingDiscards: 0
```

The following is sample output from the **show extended channel ip-stack** when you specify the alias IP address for an offload device at real IP address 10.10.21.3:

```
Router# show extended channel 3/1 ip-stack 10.2.33.88

IP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  Forwarding      : no          DefaultTTL      : 64          InReceives    : 16
  InHdrErrors     : 0           InAddrErrors    : 0           ForwDatagrams: 0
  InUnknownProtos: 0            InDiscards      : 0           InDelivers    : 16
  OutRequests     : 7           OutDiscards     : 0           OutNoRoutes   : 0
  ReasmTimeout    : 60          ReasmReqds      : 0           ReasmOKs      : 0
  ReasmFails      : 0           FragOKs         : 0           FragFails     : 0
  FragCreates     : 0           RoutingDiscards: 0
```

Table 36 describes the specified fields shown in the display.

Table 36 show extended channel ip-stack Field Descriptions

Field	Description
Alias addresses	Virtual IP addresses assigned to the real IP address of an offload device.
Forwarding	Indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host). Note that for some managed nodes this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a "badValue" response if a management station attempts to change this object to an inappropriate value.
DefaultTTL	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity whenever a TTL value is not supplied by the transport layer protocol.
InReceives	Total number of input datagrams received from interfaces, including those received in error, for this IP address instance.
InHdrErrors	Number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.

Table 36 show extended channel ip-stack Field Descriptions (continued)

Field	Description
InAddrErrors	Number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
ForwDatagrams	Number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP Gateways, this counter will include only those packets that were source-routed through this entity, and the source-route option processing was successful.
InUnknownProtos	Number of locally-addressed datagrams received but discarded because of an unknown or unsupported protocol.
InDiscards	Number of input IP datagrams for which no problems were encountered to prevent their continued processing, but that were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.
InDelivers	Total number of input datagrams delivered to IP user protocols (including Internet Control Message Protocol (ICMP)).
OutRequests	Total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for sending. Note that this counter does not include any datagrams counted in ipForwDatagrams.
OutDiscards	Number of output IP datagrams for which no problem was encountered to prevent sending them to their destination, but that were discarded (for example, for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
OutNoRoutes	Number of IP datagrams discarded because no route could be found to send them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this no-route criterion. Note that this includes any datagrams that a host cannot route because all of its default gateways are down.
ReasmTimeout	Maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
ReasmReqds	Number of IP fragments received that needed to be reassembled at this entity.
ReasmOKs	Number of IP datagrams reassembled.
ReasmFails	Number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, and so on). Note that this is not necessarily a count of discarded IP fragments because some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
FragOKs	Number of IP datagrams that have been fragmented at this entity.
FragFails	Number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their Don't Fragment flag was set.

Table 36 show extended channel ip-stack Field Descriptions (continued)

Field	Description
FragCreates	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
RoutingDiscards	Number of routing entries that were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free buffer space for other routing entries.

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.

show extended channel lan

To display the internal LANs and adapters configured on a Cisco Mainframe Channel Connection (CMCC) adapter, use the **show extended channel lan** command in user EXEC or privileged EXEC mode.

show extended channel *slot***/***port* **lan** [*tokenring* [*lan-id* [*adapno*]]]

Syntax Description

slot	Slot number.
port	Port number.
tokenring	(Optional) Specify the CMCC internal LAN type to be displayed.
lan-id	(Optional) Specify the CMCC internal LAN number to be displayed.
adapno	(Optional) Specify the CMCC internal adapter number on the selected internal LAN to be displayed.

Defaults

Display all internal LANs and adapters on the selected channel interface.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel lan** command:

```
Router# show extended channel 3/2 lan

Lan TokenRing 0
        Adapno Mac Address    Name     Vcnum
             0 4000.1111.1112            544
            20 4000.1111.2200            564
            30 4000.3030.0101            574
Lan TokenRing 1
        source-bridge 207 1 2002
        Adapno Mac Address    Name     Vcnum
             1 4000.2222.2222            545
Lan TokenRing 2
        source-bridge 50 1 1500
        Adapno Mac Address    Name     Vcnum
             2 4000.3333.2222            546
Lan TokenRing 5
        source-bridge 112 1 3000
        Adapno Mac Address    Name     Vcnum
             5 4000.1234.5656            549
Lan TokenRing 9
        source-bridge 111 1 3000
        Adapno Mac Address    Name     Vcnum
             9 4000.9999.1111            553
Lan TokenRing 10
        source-bridge 110 1 3000
        Adapno Mac Address    Name     Vcnum
            10 4000.aaaa.1111            554
Lan TokenRing 20
        source-bridge 20 1 2002
        Adapno Mac Address    Name     Vcnum
            21 4000.2020.2020            565
```

Related Commands

Command	Description
adapter	Configures internal adapters.
lan	Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode.

show extended channel llc2

To display information about the Logical Link Control, type 2 (LLC2) sessions running on the Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show extended channel llc2** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **llc2** [**admin** | **oper** | **stats**] [*lmac* [*lsap* [*rmac* [*rsap*]]]]

Syntax Description

slot	Slot number.
port	Port number.
admin	(Optional) Displys Shows configured values. This is the default.
oper	(Optional) Displays operational values for: • Internal adapters • Service access point (SAP)s opened on the internal adapters • LLC2 connections on the internal adapters
stats	(Optional) Displays statistics for: • Internal adapters • SAPs opened on the internal adapters • LLC connections on the internal adapters
lmac	(Optional) Local MAC address.
lsap	(Optional) Local SAP address, in the range from 0 to 256.
rmac	(Optional) Remote MAC address.
rsap	(Optional) Remote SAP address, in the range from 0 to 256.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel llc2** command is valid on virtual channel interfaces.

To specify LLC information for internal adapters, perform the following asks:

- Specify a value for the *lmac* argument to get information for a specific internal adapter.
- Omit the *lmac* argument to display information for all internal adapters on the specified channel interface.

To display LLC information for SAPs opened on an internal adapter, perform the following tasks:

- Specify values for the *lmac* and *lsap* arguments to display information for a particular SAP.
- Specify a value for the *lmac* argument and "*' to display information for all SAPs opened on the specified channel adapter.

To display information for LLC2 connections on a channel interface, perform the following tasks:

- Specify values for the *lmac*, *lsap*, *rmac*, and *rsap* arguments to display information for a particular active LLC2 connection.
- Specify values for the *lmac*, *lsap*, and *rmac* arguments to display information for all LLC2 connections active between the specified remote MAC address and the specified local SAP opened on the specified internal adapter.
- Specify values for the *lmac* and *lsap* arguments and "*" to display information for all LLC2 connections active on the specified local SAP and the specified internal adapter and any remote MAC address the connections are active with.
- Specify a value for the *lmac* argument, "*" for the local SAP, and a value for the *rmac* argument to display information for all LLC2 connections active between the specified internal adapter and the remote MAC address.
- Specify a value for the *lmac* argument, "*" for the local SAP, and "*"' for the remote MAC address to display information for all active LLC2 connections on the specified internal adapter.

Examples

The following is sample output from the **show extended channel llc2** command. Three examples are provided, one for each type of output as specified by the **admin**, **oper**, and **stats** keywords.

The following sample displays the configured values for all LLC2 connections on channel 2/2:

```
Router# show extended channel 2/2 llc2 admin

     Lan Token adapter   0 0004.0004.0004
  t1-time    = 1000  tpf-time  = 1000  trej-time = 3200  tbusy-tim = 9600
  idle-time =60000  local-win =    7  recv-wind =    7  N2        =    8
  N1        = 1033  ack-delay =  100  ack-max   =    3  nw        =    0
```

Table 37 describes the specified fields shown in the display.

Table 37 show extended channel llc2 admin Field Descriptions—All LLC2 Connections

Field	Description
t1-time	Length of time in milliseconds the CMCC LLC2 link station waits for an acknowledgment to a sent I-frame before polling the remote LLC2 station.
tpf-time	Length of time in milliseconds the CMCC LLC2 link station waits for a final response to a poll before resending the original poll frame.
trej-time	Length of time in milliseconds the CMCC LLC2 link station waits for a correct frame after sending a reject command to a remote LLC2 station.
tbusy-time	Length of time in milliseconds the CMCC LLC2 link station waits before repolling a busy LLC2 station.
idle-time	Frequency of polls during periods of idle traffic.
local-win	Maximum number of I-frames that the CMCC LLC2 link station connection can send to the remote LLC2 station without receiving an acknowledgment.

Table 37 show extended channel llc2 admin Field Descriptions—All LLC2 Connections

Field	Description
recv-wind	Maximum number of I-frames that the CMCC LLC2 link station connection can receive without receiving an acknowledgment.
N2	Number of times the CMCC LLC2 link station connection will resend an unacknowledged I-frame.
N1	Maximum size of LLC frames supported by the CMCC LLC2 link station. The maximum size LLC frame supported on the CMCC is controlled by other factors including the largest interface MTU between the CMCC and the remote network device, and configured values at virtual telecommunications access method (VTAM) and at the end station.
ack-delay	Maximum amount of time the CMCC LLC2 link station allows received I-frames to remain unacknowledged. The CMCC LLC2 connection will acknowledge received I-frames within the ack-delay time.
ack-max	Maximum number of I-frames the Channel Interface Processor (CIP) LLC2 link station receives before sending an acknowledgment.
Nw	Working send window size. When I-frames sent by the CMCC are rejected by the remote LLC2 station, the CMCC LLC2 connection reduces its working send window size to 1. Then, for every subsequent I-frame sent by the CMCC LLC2 connection that is positively acknowledged by the remote LLC2 station, the CMCC LLC2 connection increases its working send window by the Nw value until the working send window reaches the configured local-window value.

The following sample displays the operational values for all LLC2 connections on channel 2/2:

```
Router# show extended channel 5/2 llc oper

  LAN Token  0 Adapter   0 4000.1010.2020
      Open SAPs=1
      Max SAPs Opened=1
```

Open SAPS is the number of SAPs opened on this internal MAC adapter. *Max SAPs Opened* is the number of SAPs concurrently opened on this internal MAC adapter since the last reset of the channel adapter of channel interface.

The following sample displays operational information for the specified SAP opened on a CMCC internal adapter:

```
Router# show extended channel 5/2 llc stats

LAN Token  0 Adapter   0 4000.1010.2020
      PDUsIn     =     223339    PDUsOut     =       9564
      OctetsIn   =    6949875    OctetsOut   =     307448
      TESTCmdsIn =     213293    TESTRspsOut =          2
      LocalBusies=          0    UnknownSAPs =          0
```

Table 38 describes the specified fields shown in the display. These statistics are available on the adapter because when LLC2 connections are deactivated, users can no longer retrieve the information per LLC2 connection.

Table 38 show extended channel llc2 stats Field Descriptions—All LLC2 Connections

Field	Description
PDUsIn	Protocol data units received by the internal adapter.
PDUsOut	Protocol data Units sent by the internal adapter.
OctetsIn	PDU bytes received by the internal adapter.
OctetsOut	PDU bytes sent by the internal adapter.
TESTCmdsIn	Number of TEST commands received destined for this MAC address.
TESTRspsOut	Number of TEST responses sent by this MAC address responding to TEST commands received.
Local Busies	Number of times LLC2 connection stations on this adapter entered a busy state, sent Receiver Not Ready (RNR)s to the remote LLC2 station.
UnknownSAPs	Number of frames received that are destined for a SAP that does not exist on this adapter.

The following sample displays operational information for the specified SAP opened on the internal adapter, 4000.1010.2020, configured on channel interface 5/2:

```
Router# show extended channel 5/2 llc2 oper 4000.1010.2020 04

  LAN Token  0 Adapter   0 4000.1010.2020
    Local SAP=04
      Open Connections=2
      Max Connections Opened=2
```

Table 39 describes the specified fields shown in the display.

Table 39 show extended channel llc2 oper Field Descriptions for Specified Interface

Field	Description
Open Connections	Number of LLC2 connections active on the SAP.
Max Connections	Highest number of LLC2 connections concurrently active on that SAP since the SAP has been active.

The following sample displays statistics for the specified SAP on the internal adapter, 4000.1010.2020 configured on channel interface 5/2:

```
Router# show extended channel 5/2 llc2 stats 4000.1010.2020 04

  LAN Token  0 Adapter   0 4000.1010.2020
    Local SAP=04
      TESTRspsIn     =          0  TESTCmdsOut    =          0
      XIDCmdsIn      =         14  XIDCmdsOut     =         16
      XIDRspsIn      =          4  XIDRspsOut     =          0
      UIFramesIn     =          0  UIFramesOut    =          0
      UIOctetsIn     =          0  UIOctetsOut    =          0
      ConnectOk      =          2  ConnectFail    =          0
      DiscNorm       =          0  DiscByTmr      =          0
      DiscByFRMRSent =          0  DiscByFRMRRcvd =          0
      DMsInABM       =           0  SABMEsInABM     =           0
```

Table 40 describes the specified fields shown in the display. All statistics for SAPs are based on the time the SAP was last opened.

Table 40 show extended channel llc2 stats Field Descriptions for Specified Interface

Field	Description
TESTRspsIn	Number of TEST responses received on this SAP for TEST commands sent by VTAM (connect out).
TESTCmdsOut	Number of TEST commands sent by this SAP to explore for a remote MAC address (VTAM connect out).
XIDCmdsIN	Number of exchange identification (XID) commands received by this SAP from a remote link station.
XIDCmdsOut	Number of XID commands sent by this SAP to a remote link station.
XIDRspsIN	Number of XID responses received by this SAP from a remote link station.
XIDRspsOut	Number of XID responses sent by this SAP to a remote link station.
UIFramesIn	Number of Unnumbered I-frames received by this SAP from a remote link station.
UIFramesOut	Number of Unnumbered I-frames sent by this SAP to a remote link station.
UIOctetsIn	Number of Unnumbered I-frame bytes received by this SAP from a remote link station.
UIOctetsOut	Number of Unnumbered I-frame bytes sent by this SAP to a remote link station.
ConnectOk	Number of successful LLC2 connection attempts on this SAP.
ConnectFail	Number of LLC2 connections that failed.
DiscNorm	Number of normal LLC2 connection disconnections.
DisByTmr	Number of LLC2 connections disconnected due to the CMCC LLC2 link station not getting responses to polls from the remote LLC2 station, typically due to the remote station being powered off or a severe network failure or congestion. The CMCC LLC2 stack generates an event each time it detects this condition. The event can be configured to generate a NetView alert, SNMP trap, and a router console message.
DiscByFRMRSent	Number of times a CMCC LLC2 connection disconnected after detecting a protocol violation and sending a FRNR to the remote LLC2 station. The CMCC LLC2 link station generates an event each time it detects this condition. The event can be configured to generate a NetView alert, an SNMP trap, and a router console message.
DiscByFRMRRcvd	Number of times the CMCC LLC2 connection disconnected after the remote LLC2 station detected a protocol violation and sent an FRMR to the CMCC LLC2 link station. The CMCC LLC2 stack generates an event each time it detects this condition. The event can be configured to generate a NetView alert, an SNMP trap, and a router console message.

Table 40 show extended channel llc2 stats Field Descriptions for Specified Interface

Field	Description
DMsInABM	Number of times the CMCC LLC2 link station went into disconnect mode after receiving a disconnect mode (DM). The CMCC LLC2 stack generates an event each time it detects this condition. The event can be configured to generate a NetView alert, an SNMP trap, and a router console message.
SABMEDsInABM	Number of times the CMCC LLC2 link station went into disconnect mode after receiving a Set Asynchronous Balanced Mode Extended (SABME) from the LLC2 station. The CMCC LLC2 stack generates an event each time it detects this condition. The event can be configured to generate a NetView alert, an SNMP trap, and a router console message.

The following sample displays operation information for the specified CMCC link station:

```
Router# show extended channel 5/2 llc2 oper 4000.1010.2020 04 4000.1234.1030 18

  LAN Token  0 Adapter   0 4000.1010.2020
    Local SAP=04 Remote MAC=4000.1234.1030 Remote SAP=18 State=normal
      t1-time   = 1000  tpf-time  = 1000  trej-time = 3200  tbusy-tim = 9600
      idle-time =60000  local-win =    7  recv-wind =    7  N2        =    8
        N1-Send   = 4105  N1-Rcv    = 4105  ack-delay =  100  ack-max   =    3
Nw        =    0  Ww        =    7
      Last Ww Cause = neverInvoked
      Connection Time: 17:50:11
      Last modified: never
```

Table 41 explains parameters in use by the LLC2 connection. These parameters are the ones configured on the internal adapter 4000.0000.0001 at the time the LLC2 connection was established. If the LLC2 parameters on the internal adapter are changed while this connection is active, the connection will not reflect the changes to the adapter.

Table 41 show extended channel llc2 Field Descriptions for Internal LAN Adapter

Field	Description
State	• ADM (Asynchronous Disconnect Mode) • setup • conn • normal • busy • reject • await • awaitBusy

Table 41 show extended channel llc2 Field Descriptions for Internal LAN Adapter (continued)

Field	Description
State (continued)	• awaitReject • discConn • reset • error • pendDiscRsp The descriptions for each state can be found in Section 7.8.3, IOS 8802-2: 1989, ANSI/IEEE Std 802.2 - 1989.
t1-time	Length of time in milliseconds the CMCC LLC2 link station waits for an acknowledgment to a sent I-frame before polling the remote LLC2 station.
tpf-time	Length of time in milliseconds the CMCC LLC2 link station waits for a final response to a poll before resending the original poll frame.
trej-time	Length of time in milliseconds the CMCC LLC2 link station waits for a correct frame after sending a reject command to a remote LLC2 station.
tbusy-tim	Length of time in milliseconds the CMCC LLC2 link station waits before repolling a busy LLC2 station.
idle-time	Frequency of polls during periods of idle traffic.
local-win	Maximum number of I-frames that the CMCC LLC2 link station can send to the remote LLC2 station without receiving an acknowledgment.
recv-wind	Maximum number of I-frames that a CMCC LLC2 link station can receive without receiving an acknowledgment.
N2	Number of times a CMCC LLC2 link station will resend an unacknowledged I-frame.
N1-Send	Largest frame size this CMCC LLC2 link station is allowed to send.
N1-Rcv	Largest frame size this CMCC LLC2 link station can receive.
ack-delay	Maximum length of time in milliseconds the CMCC LLC2 link station allows received I-frames to remain unacknowledged. The Channel Interface Processor (CIP)LLC2 connection will acknowledge received I-frames within the ack-delay time.
ack-max	Maximum number of I-frames a CMCC LLC2 link station receives before sending an acknowledgment.
Nw	Working send window size. When I-frames sent by a CMCC LLC2 link station are rejected by the remote LLC2 station, the CMCC LLC2 link station reduces its working send window size to 1. Then, for every subsequent I-frame sent by the CMCC LLC2 connection that is positively acknowledged by the remote LLC2 station, the CMCC LLC2 link station increases its working send window by the Nw value until the working send window reaches the configured local-window value.
Ww	Current working window size for this LLC2 link station. This is the current number of unacknowledged I-frames that this LLC2 link station will send.

Table 41 show extended channel llc2 Field Descriptions for Internal LAN Adapter (continued)

Field	Description
Last Ww Cause	Last event that caused the working window to change values. Valid values are: • neverInvoked—This LLC2 station has not detected a condition to change the working window from the initial value at activation time. • lostData—The current working window value was changed due to loss of data by the remote LLC2 link station. • macLayerCongestion—The current working window value was changed due to the remote end station sending this LLC2 link station a Receiver Not Ready (RNR) frame.
Connection Time	Length of time this LLC2 connection has been active.
Last modified	Length of time since one of the LLC2 parameters for this connection was last modified.

The following sample displays statistics for the CMCC LLC2 link station connection between LMAC 4000.1010.2020 LSAP 04 and RMAC 4000.1234.1030 RSAP 18:

```
Router# show extended channel 5/2 llc2 stats 4000.1010.2020 04 4000.1234.1030 18

  LAN Token  0 Adapter   0 4000.1010.2020
    Local SAP=04 Remote MAC=4000.1234.1030 Remote SAP=18
      LocalBusies     =          0  RemoteBusies    =          0
      IFramesIn       =          1  IFramesOut      =          1
      IOctetsIn       =         19  IOctetsOut      =         21
      SFramesIn       =          0  SFramesOut      =          0
      REJsIn          =          0  REJsOut         =          0
      RetransmitsOut  =          0  WwCountChanges  =          0
```

Table 42 describes the specified fields shown in the display.

Table 42 show extended channel llc2 stats Field Descriptions

Field	Description
LocalBusies	Number of times the CMCC LLC2 link station entered the busy state. This state occurs for a CMCC LLC2 link station when there are *x* I-frames received from the remote LLC2 station on the CMCC queued to be sent over the channel to VTAM; Where *x* is two times the recv-wind value. The CMCC LLC2 link station will also enter into busy state whenever it receives a flow control command from VTAM.
RemoteBusies	Number of times the remote LLC2 link station entered into busy state.
IFramesIn	Number of LLC2 information frames received by the CMCC LLC2 link station from the remote link station.
IFramesOut	Number of LLC2 information frames sent by the CMCC link station to the remote link station.
IOctetsIn	Number of LLC2 information frame bytes received by the CMCC LLC2 link station from the remote link station.
IOctetsOut	Number of LLC2 information frame bytes sent by the CMCC link station to the remote link station.

Table 42 show extended channel llc2 stats Field Descriptions (continued)

Field	Description
SFramesIn	Number of LLC2 supervisory frames received by the CMCC link station from the remote link station. These include RRs, RNRs, and REJs.
SFramesOut	Number of LLC2 supervisory frames sent by the CMCC link station to the remote link station. These include RRs, RNRs and REJs.
REJsIn	Number of LLC2 REJ frames received by the CMCC link station from the remote link station. This field indicates the number of times the remote link station detected dropped I-frames sent from the CMCC LLC2 station.
REJsOut	Number of LLC2 REJ frames sent by the CMCC link station to the remote link station. This indicates the number of times the CMCC link station detected dropped I-frames sent by the remote link station.
RetransmitsOut	Number of I-frames the CMCC link station was required to resend.
WwCountChanges	Number of times the CMCC LLC2 link station changed its working send window (local-win). See the Nw field description in Table 40 for a description of when the LLC2 link stations working send window is changed.

Related Commands

Command	Description
adapter	Configures internal adapters.

show extended channel max-llc2-sessions

To display information about the number of Logical Link Control, type 2 (LLC2) sessions supported on the Cisco Mainframe Channel Connection (CMCC) adapter, use the **show extended channel max-llc2-sessions** command in privileged EXEC mode.

show extended channel *slot*/*port* **max-llc2-sessions**

Syntax Description

slot	Slot number.
port	Port number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel max-llc2-sessions** command:

```
Router# show extended channel 1/2 max-llc2-sessions

Administrative max-llc2-sessions = 1000
Operational max-llc2_sessions = 1000
Highest concurrent LLC2 sessions = 30
LLC2 session allocation failures = 0
```

Table 43 describes the specified fields shown in the display.

Table 43 show extended channel max-llc2-sessions Field Descriptions

Field	Description
Administrative max-llc2-sessions	Maximum number of LLC2 sessions configured.
Operational max-llc2-sessions	Maximum number of LLC2 sessions configured on the CMCC adapter. This value differs from the value for the administrative max-llc2-sessions if the maximum number of LLC2 sessions is decreased by configuring a new value while the CMCC adapter's virtual interface is up. If the CMCC adapter's virtual interface is reset **shut** and **no shut** command, both the administrative and operational max-llc2-sessions numbers will match.

Table 43 show extended channel max-llc2-sessions Field Descriptions (continued)

Field	Description
Highest concurrent LLC2 sessions	Highest number of LLC2 sessions active concurrently since the CMCC adapter LLC2 was started. When the CMCC adapter llc2 is initiated, the following message displays: `%CIP1-6-MSG: %MSG802-6-LLC_START: Starting LLC-2 with a session capacity of 1000`
LLC2 session allocation failures	Number of times network devices tried to establish an LLC2 connection with the CMCC adapter and failed because the operational max-llc2-sessions limit was reached when the connection was attempted.

Related Commands

Command	Description
adapter	Configures internal adapters.
show extended channel connection-map llc2	Displays the number of active LLC2 connections for each service access point (SAP) and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.

show extended channel packing names

To display Common Link Access for Workstations (CLAW) packing names and their connection state, use the **show extended channel packing names** command in user EXEC or privileged EXEC mode.

show extended channel *slot***/***port* **packing names** [*path* [*device-address*]]

Syntax Description

slot	Slot number.
port	Port number.
path	(Optional) Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default value for channel logical address and control unit logical address is 0.
device-address	(Optional) Hexadecimal value in the range from 00 to FE. This is the unit address associated with the control unit number and path as specified in the host IOCP file. The device address must have an even numbered value.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel packing names** command:

```
Router# show extended channel 3/0 packing names

Path: C010  Devices: F2,F3 CLAW Link: 1

    Sublink            Link Names
       0                 CONTROL
       1               IP        IP
       2               CKSUM     CKSUM

Path: C030  Devices: F6,F7 CLAW Link: N

    Sublink            Link Names
  DISCONNECTED           CONTROL
  DISCONNECTED         IP        IP
  DISCONNECTED         CKSUM     CKSUM
```

Table 44 describes the specified fields shown in the display.

Table 44 show extended channel packing names Field Descriptions

Field	Description
Path	Path from the CLAW configuration. It indicates which port on the switch is used by the channel side of the configuration.
Devices	Device address for each device. One CLAW connection requires two devices. You need only specify the even numbered address.
CLAW Link	Established CLAW link number used for all CLAW packing messages. A number value indicates that a CONTROL sublink is connected. "N" indicates that a control sublink is disconnected.
Sublink	DISCONNECTED indicates that a sublink connection for a particular link name is not established. 0 indicates that the CONTROL sublink is established. 1 to 15 indicates the negotiated sublink number for each application pair.
Link Names	Name used to represent the type of traffic that flows over a particular sublink: • CONTROL indicates the sublink used to transport CLAW packing control messages. • IP indicates the sublink used to send IP datagrams whose TCP checksum is handled by the host. CKSUM indicates the sublink used to send IP datagrams that use the CMCC checksum assist feature.

Related Commands

Command	Description
claw (primary) (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (primary) (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

show extended channel packing stats

To display Common Link Access for Workstations (CLAW) packing statistics, use the **show extended channel packing stats** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **packing stats** [*path* [*device-address*]]

Syntax Description

slot	Slot number.
port	Port number.
path	(Optional) Hexadecimal value in the range from 0000 to FFFF. This specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch): one digit for the control unit address, and one digit for the channel logical address. If not specified, the control unit address and channel logical address default to 0.
device-address	(Optional) Hexadecimal value in the range from 00 to FE. This value is the unit address associated with the control unit number and path as specified in the host input/output configuration program (IOCP) file. For CLAW and offload support, the device address must have an even numbered value.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel packing stats** command:

```
Router# show extended channel 3/0 packing stats

Path: C010 Devs: F2,F3 CLAW Link: 1  Read Blks: 4584      Wrt Blks: 15054
                  Packets              Bytes                Drops
Linkname       Read      Write      Read    Write       Read      Write   Err C
CONTROL           4          2       128       64          0          0     0 Y
IP                5          5       500      500          0          0     0 Y
CKSUM          4694      93584    187854 53889648          0          0     0 Y
  Total:       4703      93591    188482 53890212          0          0     0

Path: C030 Devs: F6,F7 CLAW Link: N  Read Blks: UNKNOWN   Wrt Blks: UNKNOWN
                  Packets              Bytes                Drops
Linkname       Read      Write      Read    Write       Read      Write   Err C
CONTROL           0          0         0        0          0          0     0 N
IP                0          0         0        0          0          0     0 N
CKSUM             0          0         0        0          0          0     0 N
  Total:          0          0         0        0          0          0     0
```

Table 45 describes the specified fields shown in the display

.

Table 45 show extended channel packing stats Field Descriptions

Field	Description
Path	Path from the CLAW, offload, or Cisco Systems Network Architecture (CSNA) configuration.
Devs	Device address for each device. One CLAW connection requires two devices. You need only specify the even numbered address.
CLAW Link	Established CLAW link number used for all CLAW packing messages. A number value indicates that a CONTROL sublink is connected. “N” indicates that a control sublink is disconnected.
Read Blks	Number of CLAW channel blocks read.
Write Blks	Number of CLAW channel blocks written.
Linkname	Name used to represent the type of traffic that flows over a particular sublink. • CONTROL indicates the sublink used to transport CLAW packing control messages. • IP indicates the sublink used to send IP datagrams whose TCP checksum is handled by the host. CKSUM indicates the sublink used to send IP datagrams that use the CMCC checksum assist feature.
Packets Read Write	Total number of packets read and written for each sublink.
Bytes Read Write	Total number of bytes read and written for each sublink.
Drops Read Write	Total number of dropped read and write packets for each sublink.
Err	Number of errors. Each error produces an error message at the router console.
C	Connection state of a sublink. “Y” indicates connected. “N” indicates not connected.
Total	Total for each of the recorded statistics.

Related Commands

Command	Description
claw (primary) (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (primary) (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

show extended channel statistics

To display statistical information about subchannels on the physical interface of a Cisco Mainframe Channel Connection (CMCC) adapter, use the **show extended channel statistics** command in user EXEC or privileged EXEC mode. This command displays information that is specific to the interface channel devices. The information is generally useful only for diagnostic tasks performed by technical support personnel.

show extended channel *slot*/*port* **statistics** [*path* [*device-address*]] [**connected**]

Syntax Description

slot	Slot number.
port	Port number.
path	(Optional) Hexadecimal value in the range from 0x0000 to 0xFFFF. This value specifies the data path and consists of two digits for the physical connection (either on the host or on the ESCON Director switch): one digit for the control unit address, and one digit for the channel logical address.
device-address	(Optional) Hexadecimal value in the range from 0x00 to 0xFE. This value is the unit address associated with the control unit number and path as specified in the host input/output configuration program (IOCP) file. For Common Link Access for Workstations (CLAW) and offload support, the device address must have an even numbered value.
connected	(Optional) For each backup group, displays information only about the active subchannel or the first subchannel defined in the group if none are active.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel statistics** command from a CMCC adapter configured with Common Link Access for Workstations (CLAW), offload, cisco systems network architecture (CSNA), and Cisco Multipath Channel (CMPC):

```
Router# show extended channel 0/1 statistics E010

Path: E010  -- ESTABLISHED
                  Command             Selective     System    Device         CU
Dev   Connects    Retries    Cancels      Reset      Reset    Errors       Busy
 D0       4459       4459          0          0          0         0          0
 D1       4950          0          0          0          0         0          0
 D2       2529       2526          0          0          0          0          0
 D3       2600          0          0          0          0          0          0
 D9       2211          0          0          0          0          0          0
 DA       4048       2024          0          0          0          0          0
                 Blocks               Bytes              Dropped Blk    Memd
Dev-Lnk      Read      Write      Read     Write       Read      Write  wait Con
 D0-00          0          0         0         0          0          0     0   Y
 D0-01       5017          0   1215457         0          0          0     0   Y
Total:       5017          0   1215457         0          0          0     0
 D1-00          0          0         0         0          0          0     0   Y
 D1-01          0       5039         0   1247307          0          0     0   Y
Total:          0       5039         0   1247307          0          0     0
 D2-00          0          0         0         0          0          0     0   Y
 D2-01          0          0         0         0          0          0     0   Y
 D2-02       2671          0    661621         0          0          0     0   Y
Total:       2671          0    661621         0          0          0     0
 D3-00          0          0         0         0          0          0     0   Y
 D3-01          0          0         0         0          0          0     0   Y
 D3-02          0       2680         0    653285          0          0     0   Y
Total:          0       2680         0    653285          0          0     0
 D9-00          0       2214         0    223418          0          0     0   Y
 DA-00       2024          0    124587         0          0          0     0   Y
Path E010
Total:       9712       9933   2001665   2124010          0          0     0
  Last statistics 5 seconds old, next in 5 seconds
```

The following is sample output from the **show extended channel statistics** command from a CMCC adapter configured with CLAW, offload, cisco systems network architecture (CSNA), and CMPC+:

```
Router# show extended channel 0/1 statistics

Path:C020  -- ESTABLISHED
                  Command             Selective     System     Device        CU
Dev   Connects    Retries    Cancels      Reset      Reset     Errors       Busy
 30          5          0          0          0          3          0          0
 31          5          0          0          0          3          0          0
 36         27         15          1          0          3          0          0
 37         29          6          1          0          3          0          0

                 Blocks               Bytes              Dropped Blk    Memd
Dev-Lnk      Read      Write      Read     Write       Read      Write  wait Con
 30-00          0          0         0         0          0          0     0   N
 31-00          0          0         0         0          0          0     0   N
 36-00         19          6     54236       789          0          0     0   Y
 37-00          9         17       801     63302          0          0     0   Y

Path C020
Total:         28         23     55037     64091          0          0     0

Path:C190  -- ESTABLISHED
                  Command             Selective     System     Device        CU
Dev   Connects    Retries    Cancels      Reset      Reset     Errors       Busy
 34         12          0          0          0          5          0          0
 35         12          0          0          0          5          0          0
 36        251        226          6          0          5          0          0
 37        258         14          8          0          5          0          0
 3E         12          0          0          0          5          0          0
 3F         12          0          0          0          5          0          0

                 Blocks               Bytes              Dropped Blk    Memd
Dev-Lnk      Read      Write      Read     Write       Read      Write  wait Con
 34-00          0          0         0         0          0          0     0   N
 35-00          0          0         0         0          0          0     0   N
 36-00        236         12   3604441      1578          0          0     0   Y
 37-00         18         236       1602    4217913          0          0     0   Y
 3E-00          0           0          0          0          0          0     0   N
 3F-00          0           0          0          0          0          0     0   N

Path C190
Total:       254        248   3606043   4219491          0          0     0

Adapter Card
Total:       282        271   3661080   4283582          0          0     0

  Last statistics 8 seconds old, next in 2 seconds
```

Table 46 describes the specified fields shown in the display.

Table 46 show extended channel statistics Field Descriptions

Field	Description
Path	Path from the CLAW, offload, CMPC, CMPC+, or CSNA configuration.
Dev	Address for each device. For CLAW and offload, there are two device addresses. In the configuration statement, you specify only the even numbered address. Both CSNA, CMPC, and CMPC+ have one device.
Connects	Number of times the channel started a channel program on the device.
Command Retries	Number of times the CMCC adapter either had no data to send to the channel (for the read subchannel) or the number of times the CMCC adapter had no buffers to hold data from the channel (for the write subchannel). Every command retry that is resumed results in a connect. A command retry can be ended via a cancel.
Cancels	Host requested any outstanding operation to be terminated. It is a measure of the number of times the host program was started.
Selective Reset	Resets only one device. On the virtual machine (VM), selective reset occurs when a device is attached and a CP Initial Program Load (IPL) command is issued.
System Reset	Number of times the system IPL command was issued. A system reset affects all devices on the given channel. The command is always issued when the ESCON Channel Adapter (ECA) is initialized, and when the channel is taken off line.
Device Errors	Errors detected by the ESCON or parallel interface because of problems on the link. This value should always be 0.
CU Busy	Number of times the adapter returned a control unit busy indication to the host. This indication occurs after a cancel or reset if the host requests an operation before the CMCC adapter has finished processing the cancel or reset.
Dev-Lnk	First number is the device address. The second number is the logical link. Link 0 is always used for CLAW control messages. For IP datagram mode, link 1 is for actual datagram traffic. For offload, link 2 is for application program interface (API) traffic. For CSNA, CMPC, and CMPC+, the Dev-Lnk is not relevant.
Blocks Read/Write	Count of channel blocks that are read and written from the mainframe.
Bytes Read/Write	Sum of the bytes in the blocks.

Table 46 show extended channel statistics Field Descriptions (continued)

Field	Description
Dropped Blk Read/Write	If the Route Processor sends data to the CMCC adapter faster than it can send it to the channel, then the block is dropped. High values mean the host is not running fast enough. A write drop occurs if the CMCC adapter fails to get a router processor buffer *x* times for a given block. See the Memd wait counter.
Memd wait	Number of times the CMCC adapter could not obtain a buffer.
Con	For link 0, a connection of Y means the system validation is complete. For all other links, Con means the connection request sequence is completed. For CSNA devices, a value of Y is displayed when the CSNA device status is complete. For all other states, the Con shows a value of N. **Note** If you halt the host or terminate virtual telecommunications access method (VTAM) using the Z NET, CANCEL command, VTAM does not halt the subchannels, and CON shows a value of Y until the subchannels time out (approximately 180 seconds).

The following is sample output from the CSNA path, using the **show extended channel statistics** command:

```
Router# show extended channel 0/1 statistics E200

Path: E200  -- ESTABLISHED
                  Command             Selective     System     Device        CU
Dev   Connects    Retries    Cancels      Reset      Reset     Errors       Busy
 D0     217440     108293          1          0          0          0          0
 D1      59530      19800          1          0          0          0          0
 D2       1065        252          2          0          0          0          0
 D3       1329         16          2          0          0          0          0
 D4       1066        251          2          0          0          0          0
 D5        887         29          2          0          0          0          0
 DA       1073         17          2          0          0          0        373
 DB        410        174          2          0          0          0          0
 DC       1154         14          2          0          0          0        459
 DD        254         17          2          0          0          0          0
                 Blocks               Bytes              Dropped Blk    Memd
Dev-Lnk      Read      Write      Read     Write       Read      Write  wait Con
 D0-00     109096     109095 237799616    880468          0          0     0   Y
 D1-00      19877      19875    160688 237876362          0          0     0   Y
 D2-00          9      12842       801  52554701          0          0     0   Y
 D3-00       1315          8  30378114      1052          0          0     0   Y
 D4-00          9      12842       801  52554701          0          0     0   Y
 D5-00        860          8  17003956      1052          0          0     0   Y
 DA-00        687          8  14617852      1052          0          0     0   Y
 DB-00          9       3578       801  14613989          0          0     0   Y
 DC-00        682          8  14513604      1052          0          0     0   Y
 DD-00          9       3594       801  14679517          0          0     0   Y
Path E200
Total:     132553     161858 314477034 373163946          0          0     0
  Last statistics 3 seconds old, next in 7 seconds
```

Related Commands

Command	Description
claw (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
csna	Configures Systems Network Architecture (SNA) support on a CMCC physical channel interface and specifies the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

show extended channel subchannel

To display information about the Cisco Mainframe Channel Connection (CMCC) adapter physical interfaces, use the **show extended channel subchannel** command in user EXEC or privileged EXEC mode. This command displays information that is specific to the interface channel connection. The information displayed is generally useful only for diagnostic tasks performed by technical support personnel.

show extended channel *slot*/*port* **subchannel** [**connected**]

Syntax Description

slot	Slot number.
port	Port number.
connected	(Optional) For each backup group, displays information about the active subchannel or the first subchannel defined in the group if none are active.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel subchannel connected** command used on a CMCC adapter configured for Common Link Access for Workstations (CLAW), offload, and cisco systems network architecture (CSNA):

```
Router# show extended channel 1/0 subchannel

Channel1/0:state up
  Flags:VALID ESCON LOADED ENABLED SIGNAL
  Link:E9, Buffers 0, CRC errors 1, Load count 1
  Link Incident Reports
    implicit 0, bit-error 0, link failed 1,
    NOS 0, sequence timeout 0, invalid sequence 0
  Neighbor Node - VALID
    Class:Switch          Type Number :009032        Tag:E9
    Model:002             Manufacturer:IBM
    Plant:02              Sequence    :000000010685
  Local Node - VALID
    Class:CTCA-standalone Type Number :C7200         Tag:10
    Model:6               Manufacturer:CSC
    Plant:A               Sequence    :8083599
                                                                  Last
   Mode    Path Device                                            Sense
```

```
 CLAW    E020 90 172.18.55.12  CISCOMVS TRAILMIX TCPIP  TCPIP    0000  Flags:RESET_EVENT
 CLAW    E020 91 172.18.55.12  CISCOMVS TRAILMIX TCPIP  TCPIP    0000  Flags:RESET_EVENT
 CSNA    E020 94 maxpiu 20470 time-delay  10 length-delay 20470  0000  Flags:RESET_EVENT
 OFFLOAD E140 90 172.18.55.11  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  TCPIP  API   Flags:CMD_RETRY
 OFFLOAD E140 91 172.18.55.11  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  TCPIP  API   Flags:CMD_RETRY
 CLAW    E150 90 172.18.55.13  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E150 91 172.18.55.13  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E150 96 172.18.55.22  CISCOMVS TRAILMIX TCPIP  TCPIP    0080
 CLAW    E150 97 172.18.55.22  CISCOMVS TRAILMIX TCPIP  TCPIP    0080
 CLAW    E160 90 172.18.55.14  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E160 91 172.18.55.14  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E170 90 172.18.55.15  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E170 91 172.18.55.15  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E180 90 172.18.55.20  VMV2R3   TRAILMIX TCPIP  TCPIP    0000  Flags:CMD_RETRY
 CLAW    E180 91 172.18.55.20  VMV2R3   TRAILMIX TCPIP  TCPIP    0000  Flags:CMD_RETRY
 CLAW    E180 92 172.18.55.21  TSOMAIN  TRAILMIX TCPIP  TCPIP    0000  Flags:CMD_RETRY
 CLAW    E180 93 172.18.55.21  TSOMAIN  TRAILMIX TCPIP  TCPIP    0000  Flags:CMD_RETRY
 CLAW    E190 90 172.18.55.17  CISCOMVS TRAILMIX TCPIP  TCPIP    0000  Flags:RESET_EVENT
 CLAW    E190 91 172.18.55.17  CISCOMVS TRAILMIX TCPIP  TCPIP    0000  Flags:RESET_EVENT
 CLAW    E1E0 90 172.18.55.18  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E1E0 91 172.18.55.18  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E1F0 90 172.18.55.19  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY
 CLAW    E1F0 91 172.18.55.19  CISCOMVS TRAILMIX TCPIP  TCPIP    0080  Flags:CMD_RETRY

Last statistics 6 seconds old, next in 4 seconds
```

Table 47 describes the specified fields shown in the display.

Table 47 show extended channel subchannel Field Descriptions

Field	Description
Channel1/0: state	State can be up, down, or administratively down.
Flags	• GO-OFF—CMCC adapter is trying to shut down the channel interface. This state should not persist for more than a few seconds. This flag is not applicable to the virtual channel interface. • INVALID—All displays for virtual channel interfaces should contain this flag. On physical channel interfaces, it indicates a problem with the CMCC adapter microcode. • LOADED—Channel firmware for the physical channel interface is loaded. The channel firmware is loaded only if the interface configuration contains at least one device configuration statement and is not shut down. This flag matches the state of the “loaded” LED. This flag is not applicable to the virtual channel interface. • LOVE—Note indicating an interface state change (up-down or down-up) is pending on this interface. This state should not persist for more than a few seconds. • OFFLINE—For an ESCON channel interface, this flag indicates that no mainframe has established an ESCON logical path corresponding to the paths specified in any device configuration statement (claw, offload, csna, or cmpc). For a parallel channel interface, this flag indicates that the x'0100' path is not defined in any device configuration statement or SIGNAL is not present.

Table 47 show extended channel subchannel Field Descriptions (continued)

Field	Description
Flags (continued)	• ONLINE—For an ESCON channel interface, this flag indicates that at least one mainframe has established an ESCON logical path corresponding to the paths specified in one of the device configuration statements (CLAW, offload, CSNA, CMPC, or CMPC+). For a parallel channel interface, this flag indicates that the x'0100' path is defined in at least one device configuration statement and SIGNAL is present. • RQC_PEND—CMCC adapter is attempting to send status to the channel on this interface. This state should not persist for more than a few seconds. This flag is not applicable to the virtual channel interface. • RESET_EVENT—Indicates that a reset event has been received. • SIGNAL—For an ESCON channel interface, this flag indicates that light is detected. For a parallel channel interface, this flag indicates that the "operational out" signal is detected. This flag matches the state of the "signal" LED. It will be set only if the LOADED flag is also set. This flag is not applicable to the virtual channel interface. • STAT_PEND—CMCC adapter has status to present for this device. The indication is cleared when the mainframe accepts the status.
Flags (continued)	• SUSPEND—Indicates that the CMCC device task has decided to suspend data transfer for a particular device. • VALID—A physical interface is installed. All displays for physical channel interfaces should contain this. This flag matches the state of the "present" LED.
Link: xx	Director port number to which the physical channel is connected. If the physical channel is directly connected, then this value is host dependent.
Buffers	Number of times the CMCC adapter has dropped a packet bound for the Route Processor because no packet switching buffer was available on the Route Processor.
CRC errors	Number of cyclic redundancy check (CRC) errors detected on the channel for ESCON. Number of parity errors detected on the channel for parallel.
Load count	For a CMCC physical channel interface, the number of times the channel adapter microcode has been loaded.

Table 47 show extended channel subchannel Field Descriptions (continued)

Field	Description
Link Incident Reports	Link incidents are errors on an ESCON channel. These errors are reported to the host operating system and are recorded here for additional information. • Implicit incidents—Recoverable error occurred in the ESCON Channel Adapter (ECA). • Bit errors—Bit error rate threshold was reached. The bit error rate threshold is 15 error bursts within 5 minutes. An error burst is defined as a time period of 1.5 +/– 0.5 seconds during which one or more code violations occurred. A code violation error is caused by an incorrect sequence of 10 bit characters. • Link failed—Loss of synchronization or light has occurred. • NOS—Channel or switch sent the Not Operational Sequence. • Sequence timeout—Connection recovery timeout has occurred or the router is waiting for the appropriate response while in the send offline sequence (OLS) state. • Invalid Sequence—Unconditional disconnect (UD) or unconditional disconnect response (UDR) is recognized in the wait for offline sequence state.
Neighbor node	Describes the channel or switch. Valid values are: • VALID—Information has been exchanged between the router and channel or switch. • Class—Switch or channel depending on whether the connection is a switched point-to-point connection or a point-to-point connection. • Type number—Model of switch or processor. • TAG—Physical location of the connector. • Model—A further classification of type. • Manufacturer—Identifies who made switch or processor. • Plant and sequence—Manufacturer-specific information to uniquely define this one device.

Related Commands

Command	Description
claw (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.

Command	Description
csna	Configures Systems Network Architecture (SNA) support on a CMCC physical channel interface and specifies the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

show extended channel tcp-connections

To display information about the TCP sockets on a channel interface, use the **show extended channel tcp-connections** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tcp-connections** [*loc-ip-addr* [*loc-port* [*rem-ip-addr* [*rem-port*]]]] [**detail** | **summary**]

Syntax Description

slot	Slot number.
port	Port number.
tcp-connections	Specifies TCP connections display.
loc-ip-addr	(Optional) Local IP address. IP address of the local connection endpoint. Restricts the output to those connections with a matching local IP address.
loc-port	(Optional) Local TCP port. This is the TCP port of the local connection endpoint. Restricts the output to those connections with a matching local TCP port. An asterisk (*) is a wildcard that matches every port.
rem-ip-addr	(Optional) Remote IP address. IP address of the remote connection endpoint. Restricts the output to those connections with a matching remote IP address.
rem-port	(Optional) Remote TCP port. TCP port of the remote connection endpoint. Restricts the output to those connections with a matching remote TCP port.
detail	(Optional) Prints detailed information about every matching connection.
summary	(Optional) This is the default. Prints a summary of all matching connections.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The stack address field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tcp-connections** command is valid on both physical and virtual channel interfaces. If no IP addresses or TCP ports are specified, all TCP connections are displayed in a summary for the specified interface.

The command displays detailed information about a large number of sessions that can take a long time. Consider restricting the output by IP address and TCP port to connections of interest.

Examples

The following is sample output from the **show extended channel tcp-connections detail** command:

```
Router# show extended channel 0/1 tcp-connections detail

Local IP Addr   Port  Remote IP Addr  Port   State        In Bytes   Out Bytes
10.11.198.2     21    0.0.0.0         0      listen              0           0
10.11.198.2     21    172.18.48.194   38668  establish          62         298
10.11.198.2     23    0.0.0.0         0      listen              0           0
10.11.198.2     23    172.18.48.194   38666  establish         124       11966
10.11.198.2     1025  0.0.0.0         0      listen              0           0
10.11.198.2     1025  172.18.48.194   38705  closeWait          24           1
10.11.198.3     7     0.0.0.0         0      listen              0           0
10.11.198.3     9     0.0.0.0         0      listen              0           0
10.11.198.3     19    0.0.0.0         0      listen              0           0
10.11.198.3     21    0.0.0.0         0      listen              0           0
10.11.198.3     23    0.0.0.0         0      listen              0           0
10.11.198.3     23    172.18.48.194   38667  establish          85         446
```

The following is sample output from the **show extended channel tcp-connections** command when you specify the **detail** keyword for an offload device at real IP address 10.10.21.3 with an alias address of 10.2.33.88:

```
Router# show extended channel 3/1 tcp-connections 10.10.21.3 detail

Stack Address 10.10.21.3:
Local IP Addr   Port  Remote IP Addr  Port   State        In Bytes   Out Bytes Addr
0.0.0.0         23    0.0.0.0         0      listen              0           0
10.2.33.88      23    10.70.5.140     61954  establish          59         105
```

Table 48 describes the specified fields shown in the display.

Table 48 show extended channel tcp-connections Field Descriptions

Field	Description
Stack Address	Real IP address of the TCP/IP stack or offload device.
Local IP Addr	Local IP address on the connection.
State	The state of this TCP connection. The only value that may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a “badValue” response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then this has the effect of deleting the Transmission Control Block (TCB) (as defined in RFC 793) of the corresponding connection on the managed node, resulting in immediate termination of the connection. As an implementation-specific option, a reset (RST) segment may be sent from the managed node to the other TCP endpoint. (Note, however, that RST segments are not sent reliably.)

Table 48 show extended channel tcp-connections Field Descriptions (continued)

Field	Description
In Bytes	Number of bytes sent for this TCP connection. **Note** To support Simple Network Management Protocol (SNMP) Version 1 Managers, this variable is supplied as a 32-bit value that can wrap frequently.
Out Bytes	Number of bytes received for this TCP connection. **Note** To support SNMP Version 1 Managers, this variable is supplied as a 32-bit value that can wrap frequently.

The following is sample output from the **show extended channel tcp-connections summary** command:

```
Router# show extended channel 0/1 tcp-connections summary

TCP Connections=12  Input Bytes=      294  Output Bytes=    13049
```

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.
show extended channel tcp-stack	Displays information about the TCP stack running on CMCC adapter interfaces.

show extended channel tcp-stack

To display information about the TCP stack running on Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show extended channel tcp-stack** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tcp-stack** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
tcp-stack	Specifies **tcp stack** display.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn327-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The Alias addresses field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tcp-stack** command is valid on both physical and virtual channel interfaces. If no *ip-address* argument is specified, then information is displayed for all IP addresses configured on the specified interface.

Examples

The following is sample output from the **show extended channel tcp-stack** command:

```
Router# show extended channel 0/1 tcp-stack

TCP Statistics for IP Address 10.11.198.2
  RtoAlgorithm: vanj         RtoMin      : 1000         RtoMax      : 64000
  MaxConn     : -1           ActiveOpens : 1            PassiveOpens: 17
  AttemptFails: 0            EstabResets : 0            CurrEstab   : 5
  InSegs      : 181          OutSegs     : 147          RetransSegs : 0
  InErrs      : 0            OutRsts     : 0
TCP Statistics for IP Address 10.11.198.3
  RtoAlgorithm: vanj         RtoMin      : 1000         RtoMax      : 64000
  MaxConn     : -1           ActiveOpens : 0            PassiveOpens: 1
  AttemptFails: 0            EstabResets : 0            CurrEstab   : 6
  InSegs      : 25           OutSegs     : 23           RetransSegs : 0
  InErrs      : 0            OutRsts     : 0
```

The following is sample output from the **show extended channel tcp-stack** command when you specify the real IP address for an offload device at 10.10.21.3:

```
Router# show extended channel 3/1 tcp-stack 10.10.21.3

TCP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  RtoAlgorithm: vanj         RtoMin      : 1000         RtoMax      : 64000
  MaxConn     : -1           ActiveOpens : 0            PassiveOpens: 1
  AttemptFails: 0            EstabResets : 0            CurrEstab   : 2
  InSegs      : 16           OutSegs     : 7            RetransSegs : 0
  InErrs      : 0            OutRsts     : 0
```

The following is sample output from the **show extended channel tcp-stack** command when you specify the alias IP address for an offload device at 10.2.33.88:

```
Router# show extended channel 3/1 tcp-stack 10.2.33.88

TCP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  RtoAlgorithm: vanj         RtoMin      : 1000         RtoMax      : 64000
  MaxConn     : -1           ActiveOpens : 0            PassiveOpens: 1
  AttemptFails: 0            EstabResets : 0            CurrEstab   : 2
  InSegs      : 16           OutSegs     : 7            RetransSegs : 0
  InErrs      : 0            OutRsts     : 0
```

Table 49 describes the specified fields shown in the display.

Table 49 show extended channel tcp-stack Field Descriptions

Field	Description
Alias addresses	Virtual IP addresses assigned to the real IP address of an offload device.
RtoAlgorithm	The algorithm used to determine the timeout value used for resending unacknowledged octets.
RtoMin	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the LBOUND quantity described in RFC 793.
RtoMax	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre(3), an object of this type has the semantics of the UBOUND quantity described in RFC 793.
MaxConn	The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value –1.
ActiveOpens	Number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
PassiveOpens	Number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.

Table 49 show extended channel tcp-stack Field Descriptions (continued)

Field	Description
AttemptFails	Number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
EstabResets	Number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
CurrEstab	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
InSegs	Total number of segments received, including those received in error. This count includes segments received on established connections.
OutSegs	Total number of segments sent, including those on current connections but excluding those containing only re-sent octets.
RetransSegs	Total number of segments re-sent—that is, the number of TCP segments sent containing one or more previously sent octets.
InErrs	Total number of segments received in error (for example, bad TCP checksums).
OutRsts	Number of TCP segments sent containing the reset (RST) flag.

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.
show extended channel tcp-connections	Displays information about the TCP sockets on a channel interface.

show extended channel tg

To display configuration, operational information, and statistics information for Cisco Multipath Channel (CMPC) or CMPC+ transmission groups configured on the specified Cisco Mainframe Channel Connection (CMCC) adapter's virtual interface, use the **show extended channel tg** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tg** [**oper** | **stats**] [**detailed**] [*tg-name*]

Syntax Description

slot	Slot number.
port	Port number.
oper	(Optional) Operational parameters for the CMPC or CMPC+ Transmission Group (TG) values.
stats	(Optional) Statistical values for the CMPC or CMPC+ TG.
detailed	(Optional) Additional information about the CMPC or CMPC+ TG.
tg-name	(Optional) Name of the TG.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	Support was added for the CMPC+ feature.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tg** command is valid only on the virtual channel interface. If the *tg-name* argument is not specified, information about all TGs configured on the specified interface is displayed.

If neither the **oper** or **stats** keyword is specified, operational values are displayed.

Examples

The following is sample output from the **show extended channel tg oper** command for a CMPC TG:

```
Router# show extended channel 3/2 tg oper detailed MVS2-TG1

CMPC-TG: MVS2-TG1 Status: ACTIVE
   Adapter:token    1  RMAC:4000.4040.1996         LSAP:04         RSAP:04
   TGN    :21          Local CP: NETA.MVS2         Remote CP: NETA.CALEB
   MaxIn  :4105        MaxOut  :4105
   HPR    :NO          HPR LSAP:04                 HPR RSAP :00
   RIF    :0830.1FF1.0041.00A0
Connection LLC2 Information:
   t1-time   = 1000  tpf-time  = 1000  trej-time = 3200  tbusy-tim = 9600
```

```
idle-time =60000  local-win =    7  recv-wind =    7  N2         =    8
N1-Send    = 1033  N1-Rcv     = 1033  ack-delay =  100  ack-max    =    3
Nw         =    0  Ww         =    7
Last Ww Cause = other
Connection Time: 00:00:00 UTC Jan 1 1970
Last modified: 00:00:00 UTC Jan 1 1970
```

Table 50 describes the specified fields shown in the display.

Table 50 show extended channel tg oper Field Descriptions

Field	Description
Status	Connection status of the CMPC TG. Valid values are: • Shutdown—CMCC virtual interface is shut down. In this state, all nonconfigurable values will not be displayed and the Logical Link Control (LLC) connection operational values displayed when the **detailed** keyword is specified also are not displayed. • Inactive—CMPC TG is reset ready to activate. • LocatingRemoteLinkStation—Exploring network for configured CMPC TG peer. • RemoteLinkStationLocated—CMPC TG network peer found. Waiting for connection negotiation to start. • XID3Negotiation—exchange identification (XID) negotiation in progress. • PendingActive—Connect station pending. • ACTIVE—CMPC TG connection active.
Adapter	Identifies the CMCC adapter's internal MAC adapter configured for this CMPC TG. The MAC address configured for this adapter is the local MAC address for the CMPC or CMPC+ TG LLC connection.
RMAC	Remote MAC address configured for the CMPC TG LLC connection.
LSAP	Local service access point (SAP) configured for the CMPC TG LLC connection.
RSAP	Remote SAP configured for the CMPC TG LLC connection.
TGN	TG number for this CMPC TG LLC connection. This value is extracted from the XID3 negotiation exchange.
Local CP	Control point name for virtual telecommunications access method (VTAM). The name is extracted from XID3s received from virtual telecommunications access method (VTAM).
Remote CP	Control point name for the remote node connected by this CMPC TG. The name is extracted from XID3 received from the remote node.
MaxIn	Maximum path information unit (PIU) the remote node is allowed to send to VTAM. The value is the max PIU field in the XID3s received from VTAM.
MaxOut	Maximum PIU VTAM is allowed to send to the remote node. The value is the lowest of the max PIU field in the XID3 received from the remote node, the LF (length field) size in the RIF, and the CMCC virtual interface MTU size.
HPR	Valid values are YES and NO. If HPR is active on this CMPC TG, then the value will display YES.
HPR LSAP	Local SAP value used for HPR traffic. This value will be the same as the configured local service access point (SAP) value.

Table 50 show extended channel tg oper Field Descriptions (continued)

Field	Description
HPR RSAP	Remote SAP value used for HPR traffic. This value is extracted from the XID3s during the connection negotiation between VTAM and the remote node.
RIF	Routing information field. If the CMPC TG LLC connection is established using source-route bridging, then the RIF used for the connection is displayed here.

The following is sample output on a Cisco 7500 router from the **show extended channel tg stats** command for a CMPC TG:

```
Router# show extended channel 3/2 tg stats detailed MVS2-TG1

CMPC-TG:MVS2ISR1
  IFramesIn   :51            IFramesOut  :41
  IBytesIn    :4378          IBytesOut   :51803
  UIFramesIn  :0             UIFramesOut :0
  UIBytesIn   :0             UIBytesOut  :0
  TESTRspsIn  :1             TESTCmdsOut :1
  XIDCmdsIn   :3             XIDCmdsOut  :3
  XIDRspsIn   :0             XIDRspsOut  :0
  ConnectReqs :2             ConnectInds :0
  ConnectRsps :2             ConnectCnfms:0
  DISCReqs    :1             DISCInds    :0
  SweepReqsIn :0             SweepReqsOut:0
  SweepRspsIn :0             SweepRspsOut:0
  Wraps       :0
  LastSeqNoIn :9             LastSeqNoOut:7
  LastSeqNoFailureCause     : None
TimeSinceLastSeqNoFailure : never
  LLC2 Connection Statistics:
 LAN Token  0 Adapter   1 4000.cdcd.cdcd
   Local SAP=04 Remote MAC=4000.4040.1996 Remote SAP=04
     LocalBusies    =          0  RemoteBusies   =          0
     IFramesIn      =         51  IFramesOut     =         41
     IOctetsIn      =       4378  IOctetsOut     =      51803
     SFramesIn      =          0  SFramesOut     =          0
     REJsIn         =          0  REJsOut        =          0
     RetransmitsOut =          0  WwCountChanges =          0
```

Table 51 describes the specified fields shown in the display.

Table 51 show extended channel tg stats Field Descriptions

Field	Description
IFramesIn	Number of connection-oriented PIUs received by this CMPC TG from the remote network node.
IFramesOut	Number of connection-oriented PIUs sent by this CMPC TG to the remote network node.
IBytesIn	Number of bytes for connection-oriented PIUs received by this CMPC TG from the remote network node.
IBytesOut	Number of bytes for connection-oriented PIUs sent by this CMPC TG to the remote network node.
UIFramesIn	Number of connectionless PIUs (HPR frames) received by this CMPC TG from the remote network node.

Table 51 show extended channel tg stats Field Descriptions (continued)

Field	Description
UIFramesOut	Number of connectionless PIUs (HPR frames) sent by this CMPC TG to the remote network node.
UIBytesIn	Number of bytes for connectionless PIUs received by this CMPC TG from the remote network node.
UIBytesOut	Number of bytes for connectionless PIUs sent by this CMPC TG to the remote network node.
TESTRspsIn	Number of TEST responses received for this CMPC TG.
TESTCmdsOut	Number of TEST commands sent by this CMPC TG to the configured remote MAC address.
XIDCmdsIn	Number of XID commands received for this CMPC TG.
XIDCmdsOut	Number of XID commands sent by this CMPC TG.
XIDRspsIn	Number of XID responses received for this CMPC TG.
XIDRspsOut	Number of XID responses sent by this CMPC TG.
ConnectReqs	Number of connect requests received from the host by this CMPC TG.
ConnectInds	Number of connect indications sent to the host by this CMPC TG.
ConnectRsps	Number of connect responses received from the host by this CMPC TG.
ConnectCnfms	Number of connect confirms sent to the host by this CMPC TG.
DISCReqs	Number of disconnect requests received from the host by this CMPC TG.
DISCInds	Number of disconnect indications sent to the host by this CMPC TG.
SweepReqsIn	Number of CMPC sweep requests received from VTAM on this CMPC TG.
SweepReqsOut	Number of CMPC sweep requests sent to VTAM on the CMPC TG.
SweepRspsIn	Number of CMPC responses received from VTAM on this CMPC TG.
SweepRspsOut	Number of CMPC responses sent to VTAM on this CMPC TG.
Wraps	The number of times the sequence numbers wrapped for this CMPC TG.
LastSeqNoIn	The sequence number on the last CMPC data block sent to the host from this CMPC TG.
LastSeqNoOut	The sequence number on the last CMPC data block received from the host for this CMPC TG.

Table 51 show extended channel tg stats Field Descriptions (continued)

Field	Description
LastSeqNoFailureCause	The cause of the last sequence number failure for this CMPC TG. Valid values are as follows: • None—No sequence number failures have occurred on this CMPC TG since it was configured or the interface was last "no shut." • Block—The sequence number failure occurred on an Multi-Path Channel plus (MPC) data block received from the host for this CMPC TG. • Sweep—The sequence number failure occurred on a sweep command received from the host for this CMPC TG.
TimeSinceLastSeqNoFailure	Time since the last CMPC sequence number failure for this CMPC TG. If there have been no failures, "never" is displayed.

The following is sample output on a Cisco 7500 router from the **show extended channel tg stats** command for a CMPC TG when the interface is shut down:

```
Router# show extended channel 3/2 tg stats detailed MVS2-TG1

CIP LLC-TG:MVS2ISR1 -Statistics Not Available
```

The following is sample output from the **show extended channel tg** command for a CMPC+ TG:

```
CMPC-TG:MPCPTG2   Status:Active
  Local IP address:10.44.4.1                    Remote IP Address :10.44.4.2

  Connection Info: Type=TCP/IP
  Local VC Token  :0500109002                    Local Conn. Token :0500109003
  Remote VC Token :0500201002                    Remote Conn. Token:0500201002
  VC Status       :Active                        Connection Status :Active

CMPC-TG:MPCPTG3   Status:Active
  Local IP address:172.18.3.1                    Remote IP Address :172.18.3.2

  MPC+ Connection Info: Type=HSAS IP
  Local VC Token  :0500109002                    Local Conn. Token :0500109003
  Remote VC Token :0500201002                    Remote Conn. Token:0500201002
  VC Status       :Active                        Connection Status :PendingActive
```

Table 52 describes the specified fields shown in the display.

Table 52 show extended channel tg Field Descriptions

Field	Description
Status	Connection status of the CMPC+ TG. Valid values are: • Shutdown—CMCC virtual interface is shut down. In this state, all nonconfigurable values will not be displayed and the connection operational values displayed when the **detailed** keyword is specified also are not displayed. • Ready—CMCC virtual interface is operational. • Unknown—Unknown status. • Inactive—CMPC+ TG is reset ready to activate. • Active—CMPC+ TG connection active.
Local IP Address	IP address of the CMCC interface for this TG. This address matches the router's IP address configured on the corresponding TG statement.
Remote IP Address	IP address of the host for this TG. This address matches the host IP address configured on the corresponding TG statement.
Type	Valid IP connection types are: • TCP/IP—Indicates that the connection is via the TCP/IP stack. • HSAS IP—Indicates that the connection is via the High Speed Access Services (HSAS) stack.
Local VC Token	CMCC adapter's token for the virtual circuit.
Remote VC Token	Host's token for the virtual circuit.
VC Status	Valid states for the virtual circuit are: • Reset—Awaiting a connection request from the host or CMCC adapter. • Active—Virtual circuit active indication was received from the host and the CMCC adapter sent a virtual circuit active indication to the host. The virtual circuit is now ready to send and receive connection requests.
Local Conn Token	CMCC adapter's token for the Multi-Path Channel plus (MPC+) connection.
Remote Conn Token	Host's token for the MPC+ connection.
Connection Status	The valid states for a connection are: • Reset—Awaiting a connection request from the host or CMCC adapter. • ConnectionRequestSent—CMCC adapter sent a Connection Request to the host and is waiting a Connection Confirm from the host. • PendingActive—CMCC adapter is waiting for the host to enable traffic flow on the connection. • Active—Connection is active and both the CMCC adapter and the host have enabled traffic flow on the connection. At this point, the CMCC adapter has added a static route on the router for the host's IP address. Verify with the **show ip route static** command.

The following sample shows output on a CMCC adapter from the **show extended channel tg stats** command for a CMPC+ TG:

```
Router# show extended channel 3/2 tg stats MVS2-TG1

CMPC-TG:MPCPTG2
  PacketsIn     :        81361   PacketsOut     :        71369
  BytesIn       :   3874888438   BytesOut       :    377499994
  ConnNr        :            0   ConnNs         :            0
  SweepReqsIn   :            0   SweepReqsOut   :            0
  SweepRspsIn   :            0   SweepRspsOut   :            0
  Wraps         :            0
  LastSeqNoIn   :     56047093   LastSeqNoOut   :      6751136
  LastSeqNoFailureCause     : None
  TimeSinceLastSeqNoFailure : never
CMPC-TG:MPCPTG3
  PacketsIn      :        44361   PacketsOut     :        63369
  BytesIn        :   6834888438   ByteOuts       :    954539994
  ConnNr         :            0   ConnNs         :            0
  SweepReqsIn    :            0   SweepReqsOut   :            0
  SweepRspsIn    :            0   SweepRspsOut   :            0
  Wraps          :            0
  LastSeqNoIn    :      6274700   LastSeqNoOut   :      1829808
  LastSeqNoFailureCause     : None
  TimeSinceLastSeqNoFailure : never
```

Table 53 describes the specified fields shown in the display.

Table 53 show extended channel tg stats Field Descriptions

Field	Description
PacketsIn	Number of packets sent to the host on this TG.
PacketsOut	Number of packets sent by the host on this TG.
BytesIn	Total byte count for all packets sent to the host on this TG.
BytesOut	Total byte count for all packets sent by the host on this TG.
ConnNr	Sequence number of the last MPC+ frame on this connection from the host. Because IP traffic is all connectionless, the value is always 0.
ConnNs	Sequence number of the last MPC+ frame on this connection sent to the host. Because IP traffic is always connectionless, the value is always 0.
SweepsReqsIn	Number of CMPC+ sweep requests received from the host on this CMPC+ TG.
SweepsReqsOut	Number of CMPC+ sweep requests sent to the host on the CMPC+ TG.
SweepsRspsIn	Number of CMPC+ sweep responses received from the host on the CMPC+ TG.
SweepsRspsOut	Number of CMPC+ responses sent to the host on this CMPC+ TG.
Wraps	Number of times the CMPC+ sequence number for this TG has wrapped on the write subchannel.
LastSeqNoIn	Last block sequence number sent on the read subchannel.
LastSeqNoOut	Last block sequence number received on the write subchannel.

Table 53 show extended channel tg stats Field Descriptions (continued)

Field	Description
Last SeqNoFailureCause	Valid values are: • None—No sequence number failures detected since the program started. • Block—Sequence number received in a data block on the write subchannel was not the expected sequence number. • Sweep—Sequence number received in a sweep message on the write subchannel was not the expected sequence number.
TimeSinceLastSeqNoFailure	Number of seconds since the last sequence number failure.

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
tg (CMPC)	Defines LLC connection parameters for the CMPC transmission group.
tg (CMPC+)	Defines IP connection parameters for the CMPC+ transmission group.
show extended channel cmgr	Displays information about the MPC+ transmission group connection manager.

show extended channel tn3270-server

To display current server configuration parameters and the status of the physical unit (PU)s defined for the TN3270 server, use the **show extended channel tn3270-server** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server**

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
port	Port value for a TN3270 server will always be 2.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The following fields were added to the output display: • lu-termination • lu-deletion
12.2	The Named value was added for the lu-deletion field in the output display.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel tn3270-server** command:

```
Router# show extended channel 3/2 tn3270-server

<current stats> < connection stats >  <response time(ms)>
server-ip:tcp        lu in-use   connect disconn fail   host     tcp
172.28.1.106:23     510     1       12       11     0     54     40
172.28.1.107:23     511     0        0        0     0      0      0
172.28.1.108:23     255     0        0        0     0      0      0
total              1276     1
configured max_lu 20000  unbind-action disconnect
idle-time 0  keepalive 1800 (send nop)
tcp-port 23  generic-pool permit no timing-mark
lu-termination unbind lu-deletion never
dlur MPX.GOANCP                              status SHUT
dlus MPX.NGMVMPC
name(index)    ip:tcp               xid   state     link   destination   r-lsap
```

```
EXT2(1)      172.28.1.106:23     05D18092 ACTIVE    tok 0  4000.7470.00e7 08 04
PUS10(2)     172.28.1.107:23     05D19010 ACTIVE    tok 0  4000.7470.00e7 08 2C
PUS11(3)     172.28.1.107:23     05D19011 ACTIVE    tok 0  4000.7470.00e7 08 28
PUS12(4)     172.28.1.108:23     05D19012 ACTIVE    tok 0  4000.7470.00e7 08 24
PUS9(5)      172.28.1.109:23     05D18509 SHUT      tok 0  4001.3745.1088 04 40
SDTF(7)      172.28.1.107:23     12345678 ACTIVE    tok 0  0800.5a4b.1cbc 04 08
TEST(8)      172.28.1.106:23     05D18091 ACTIVE    tok 0  4000.7470.00e7 08 30
INT1(6)      172.28.1.106:23     05D18091 SHUT      dlur
```

Table 54 describes the significant fields in the display. Those fields not described correspond to configured values.

Table 54 show extended channel tn3270-server Field Descriptions

Field	Description
server	IP address and TCP port number, listen point, configured on one or more PUs.
lu	Total number of logical unit (LU)s available for this listen point.
in-use	Number of LUs in use.
connect	Total number of connections since the TN3270 feature was started.
disconn	Total number of disconnects since the TN3270 feature was started.
fail	Total number of failed connections since the TN3270 feature was started.
response time, host	The average response time from the host across all sessions through this server IP address. This is measured from sending Carrier Detect (CD) to the host to receiving the reply.
response time, tcp	Average response time from the clients on this server IP address. This is measured only when TIMING MARKs are sent. If **no timing-mark** is configured, they are sent only on special occasions, such as Bind.
idle-time *number*	Configured idle-time for this physical unit (PU).
keepalive	Configured keepalive time for this PU. *action* is one of the following: • **send nop**—The Telnet command for no operation is sent to the TN3270 client to verify the physical connection. • **send timing mark** *number*—Number of seconds within which the TN3270 server expects a response to the DO TIMING-MARK from the TN3270 client.
unbind-action	Configured unbind action for LUs on this PU.
tcp-port	Configured TCP port number.
generic-pool	Configured generic pool for LUs on this PU.

Table 54 show extended channel tn3270-server Field Descriptions (continued)

Field	Description
lu-termination	Displays the value configured for the **lu termination** siftdown command for the PUs supported by the TN3270 server. The **lu termination** command specifies whether a TERMSELF or UNBIND request/response unit (RU) is sent by the TN3270 server when a client turns off the device or disconnects. The values are: • termself—Termination of all sessions and session requests associated with an LU is ordered upon disconnect. • unbind—Termination of the session by the application is requested upon LU disconnect.
lu-deletion	Displays the value configured for the **lu deletion** siftdown command for the PUs supported by the TN3270 server. The **lu deletion** command specifies whether the TN3270 server sends a REPLY-PSID poweroff request to virtual telecommunications access method (VTAM) to delete the corresponding LU when a client disconnects. The values are: • always—Dynamic LUs for this PU are always deleted upon disconnect. • named—Only named LUs for this PU are deleted upon disconnect. • normal—Only screen LUs for this PU are deleted upon disconnect. • non-generic—Only specified LUs for this PU are deleted upon disconnect. • never—None of the LUs for this PU are ever deleted upon disconnect.
dlur	Configured fully qualified Dependent Logical Unit Requestor (DLUR) CP name(fq-cpname).
status	Shows the status of the DLUR-DLUS pipe followed by the state of the pipe. Values for the status are: • RESET—The pipe is reset. • PND-ACTV—The pipe is pending active. • ACTIVE—The pipe is active. • PND-INAC—The pipe is pending inactive. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
dlus	Active DLUS.
name	This is the name of the PU as configured.
ip:tcp	IP address and TCP port number configured for the PU.
xid	Configured exchange identification (XID)—idblk and idnum.

Table 54 show extended channel tn3270-server Field Descriptions (continued)

Field	Description
state	STATE values and their meanings are: • SHUT—The PU is configured but in shut state. • RESET—The link station of this PU is not active. • TEST—PU is sending a TEST to establish link. • XID—TEST is responded, XID is sent. • P-ACTPU—The link station is up but no Activate Physical Unit (ACTPU) is received. • ACTIVE—ACTPU is received and acknowledged positively. • ACT/BUSY—Awaiting host to acknowledge the system services control points (SSCP) data. • WAIT—Waiting for PU status from CMCC adapter. • OTHER—PU in undefined state. • P-RQACTPU-R—DLUR PU is pending request ACTPU response. • P-ACTIVE—ACTPU received by DLUR but not yet passed to PU. • P-DACTPU—PU is pending Deactivate Physical Unit (DACTPU). • UNKNOWN—State cannot be obtained.
link *type*	Link type is either internal adapter type and internal adapter number or dlur if it is a Systems Network Architecture (SNA) Session Switch PU.
Destination	If a direct PU, then it is the destination MAC address; otherwise, it is the name of the partner PU.
r-lsap	Remote and local service access point (SAP) values.

show extended channel tn3270-server client-ip-address

To display information about all clients at a specific IP address, use the **show extended channel tn3270-server client-ip-address** command in user EXEC or privileged EXEC mode.

show extended channel *slot/port* **tn3270-server client-ip-address** *ip-address* [**disconnected** | **in-session** | **pending**]

Syntax Description

slot	Slot number.
port	Port number.
ip-address	IP address of the client.
disconnected	(Optional) Displays all clients with the *ip-address* argument in disconnected state. Disconnected state refers to an logical unit (LU) session state of ACTIVE or INACTIVE. In this case, the *ip-address* argument refers to the client that last used the LU.
in-session	(Optional) Displays all clients with the *ip-address* argument in active session state. Active session state refers to an LU session state of ACT/SESS.
pending	(Optional) Displays all clients with the *ip-address* argument in pending state. Pending session state refers to an LU session state of P-SDT, P-ACTLU, P-NTF/AV, P-NTF/UA, P-RESET, P-PSID, P-BIND, P-UNBIND, WT-UNBND, WT-SDT, or UNKNOWN.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server client-ip-address** command is valid only on the virtual channel interface. Note that this command does not display information about LUs that have never been connected.

Examples

The following is sample output from the **show extended channel tn3270-server client-ip-address** command. The example shows only active sessions because no other session types exist at this client IP address.

```
Router# show extended channel 3/2 tn3270-server client-ip-address 192.195.80.40

lu    name   client-ip:tcp        nail state    model   frames in out   idle for
1   PUS11001 192.195.80.40:3169    Y   ACT/SESS 327804   5       5       0:5:47
```

```
pu is PUS11, lu is DYNAMIC type 2, negotiated TN3270
bytes 155 in, 1758 out; RuSize 1024 in, 3840 out; NegRsp 0 in, 0 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
```

The following is sample output using the **disconnected** keyword:

```
Router# show extended channel 2/2 tn3270 client-ip-address 10.14.1.21 disconnected

Total 2 clients found using 10.14.1.21
```

The following is sample output using the **in-session** keyword:

```
Router# show extended channel 2/2 tn3270 client-ip-address 10.14.1.21 in-session

Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail state    model   frames in out   idle for
3    PU1L03 10.14.1.21:35215      N   ACT/SESS 327804    317     316     0:0:1

pu is PU1, lu is DYNAMIC type 2, negotiated TN3270
bytes 12167 in, 225476 out; RuSize 2048 in, 1536 out; NegRsp 0 in, 0 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail state    model   frames in out   idle for
4    PU1L04 10.14.1.21:35216      N   ACT/SESS 327804   317     316     0:0:1

pu is PU1, lu is DYNAMIC type 2, negotiated TN3270
bytes 12167 in, 225476 out; RuSize 2048 in, 1536 out; NegRsp 0 in, 0 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
Note: if state is ACT/NA then the client is disconnected
Total 2 clients found using 10.14.1.21
```

The following is sample output using the **pending** keyword:

```
Router# show extended channel 2/2 tn3270 client-ip-address 10.14.1.21 pending

Total 2 clients found using 10.14.1.21
```

Table 55 describes the significant fields in the display.

Table 55 show extended channel tn3270-server client-ip-address Field Descriptions

Field	Description
lu	Local address of the logical unit (LU).
name	If the physical unit (PU) is directly connected, then the name shown is the one generated by the seed. If LU, then only the unqualified portion is shown. The network entity title (NET) ID portion will be the same as the current Dependent Logical Unit Server (DLUS)
client-ip:tcp	Client's IP address and TCP port number.
nail	Status of LU nailing, either Y or N.

Table 55 show extended channel tn3270-server client-ip-address Field Descriptions (continued)

Field	Description
state	LU state values and their meanings are: • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive activate logical unit (ACTLU). • ACT/NA—LU received ACTLU and acknowledged positively. • P-SDT—LU is bound but there is no Structured Data Transfer (SDT) yet.
state (continued)	• ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet connects in and is waiting for ACTLU. • P-NTF/AV—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Awaiting a buffer to send Deactivate LU (DACTLU) response. • P-PSID—Awaiting NMVT Reply PSID response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model	IBM 3278 model type of client; blank if Static LU.
frames in	Number of frames sent inbound to the host.
frames out	Number of frames sent outbound from the host.
idle for	Time the client has been idle. The time is in HH:MM:SS.
pu is	Name of the PU.
lu is	Whether LU is DYNAMIC or STATIC.
negotiated	Whether client is TN3270 or TN3270E.
bytes in/out	Total number of bytes sent to and received from the host.
RuSize in/out	Request/response unit (RU) size as configured in the bind.
NegRsp in/out	Number of Systems Network Architecture (SNA) negative responses sent to and received from the host.
pacing window in/out	SNA pacing window as configured in the bind.
credits in	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue size in	Indicates the number of SNA frames waiting to be sent to the host that are blocked and are waiting for a pacing response.
queue-size out	SNA frames not yet acknowledged by an isolated pacing response by the TN3270 server.

Related Commands

Command	Description
client ip lu	Defines a specific LU or range of LUs to a client at the IP address or subnet.

show extended channel tn3270-server client-name

To display information about all connected clients with a specific machine name, use the **show extended channel tn3270-server client-name** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server client-name** *name*

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
name	Specifies the client machine name. This name is specified originally in the **client pool** command.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

Examples

The following is sample output from the **show extended channel tn3270-server client-name** command:

```
Router# show extended channel 4/2 tn3270-server client-name dhcp-rtp-34-40.cisco.com

Note: if state is ACT/NA then the client is disconnected

lu    name   client-name           nail state    model    frames in out   idle for
6            dhcp-rtp-34-40.cisco. N    P-ACTLU  3278S2E  1         0     0:1:59

pu is T240CA, lu is DYNAMIC unbound, negotiated TN3270E
bytes 101 in, 0 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
response time buckets 0 0 0 0 0
average total response time 0 average IP response time 0
number of transactions 0
Note: if state is ACT/NA then the client is disconnected
lu    name   client-name         nail    state    model frames in out   idle for
7   T240DA07 dhcp-rtp-34-40.cisco. N    P-BIND   3278S2E  4       3       0:1:32
```

```
pu is T240CA, lu is DYNAMIC unbound, negotiated TN3270E
bytes 199 in, 407 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
response time buckets 0 0 0 0 0
average total response time 0 average IP response time 0
number of transactions 0
Total 2 clients found using dhcp-rtp-34-40.cisco.com
```

Table 56 describes the significant fields in the display.

Table 56 show extended channel tn3270-server client-name Field Descriptions

Field	Description
lu	Local address of the logical unit (LU).
name	If the physical unit (PU) is directly connected, then the name shown is the one generated by the seed. If LU, then only the unqualified portion is shown. The network entity title (NET) ID portion will be the same as the current Dependent Logical Unit Server (DLUS)
client-name	Client’s machine name.
nail	Status of LU nailing, either Y or N.
state	LU state values and their meanings are: • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive activate logical unit (ACTLU). • ACT/NA—LU received ACTLU and acknowledged positively. • P-SDT—LU is bound but there is no Structured Data Transfer (SDT) yet. • ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet connects in and is waiting for ACTLU. • P-NTF/AV—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Awaiting a buffer to send Deactivate LU (DACTLU) response. • P-PSID—Awaiting NMVT Reply PSID response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model	IBM 3278 model type of client; blank if Static LU.
frames in	Number of frames sent inbound to the host.
frames out	Number of frames sent outbound from the host.
idle for	Time the client has been idle. The time is in HH:MM:SS.
pu is	Name of the PU.
lu is	Whether LU is DYNAMIC or STATIC.
negotiated	Whether client is TN3270 or TN3270E.

Table 56 show extended channel tn3270-server client-name Field Descriptions (continued)

Field	Description
bytes in/out	Total number of bytes sent to and received from the host.
RuSize in/out	Request/response unit (RU) size as configured in the bind.
NegRsp in/out	Number of Systems Network Architecture (SNA) negative responses sent to and received from the host.
pacing window in/out	SNA pacing window as configured in the bind.
credits in	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue size in	Indicates the number of SNA frames waiting to be sent to the host that are blocked and are waiting for a pacing response.
response time buckets	Number of transactions in each response-time "bucket" for the specified LU. The bucket boundaries are defined using the **response-time group** command.
average total response time	Average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Average IP transit response time (in tenths of seconds) for the total number of response-time transactions.
number of transactions	Total number of response-time transactions across all response-time buckets.

show extended channel tn3270-server dlur

To display information about the Systems Network Architecture (SNA) session switch, use the **show extended channel tn3270-server dlur** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server dlur**

Syntax Description

slot	Slot number.
port	Port number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server dlur** command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel tn3270-server dlur** command:

```
Router# show extended channel 3/2 tn3270-server dlur

dlur MPX.GOANCP
current dlus MPX.NGMVMPC                dlur-dlus status ACTIVE
preferred dlus MPX.NGMVMPC              backup dlus MPX.NGMVMPB
preferred server MPX.NGMVMPA
lsap token-adapter   0 5C     vrn MPX.LAN4           status ACTIVE
link P390                 remote 4000.7470.00e7 08  status ACTIVE
```

Table 57 describes the significant fields in the display.

Table 57 show extended channel tn3270-server dlur Field Descriptions

Field	Description
dlur	Fully qualified control point (CP) name used by the SNA session switch and the logical unit (LU) name for the Dependent Logical Unit Requestor (DLUR) function configured as the fully qualified CP named on the dlur statement.
current dlus	Name of the active Dependent Logical Unit Server (DLUS), either the primary DLUS or the backup DLUS.

Table 57 show extended channel tn3270-server dlur Field Descriptions (continued)

Field	Description
dlur-dlus status	Values for the status of the DLUR-DLUS pipe and their meanings are: • RESET—The pipe is reset. • PND-ACTV—The pipe is pending active. • ACTIVE—The pipe is active. • PND-INAC—The pipe is pending inactive. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the Cisco Mainframe Channel Connection (CMCC) adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
preferred dlus	Name of the DLUS as configured on the DLUR statement.
backup dlus	Name of the DLUS that is used if the preferred DLUS is unavailable.
preferred server	Fully qualified name of the preferred network node server.
lsap	Configured value for the local service access point (SAP) on the configured internal adapter. Token-adapter specifies the type of internal adapter used.
vrn	Name of the connection network as configured by the vrn statement for this Link Service Access Point (LSAP) and internal adapter pair.
lsap...status	LSAP values and their meanings are: • ACTIVE—The SAP is open. • INACTIVE—Not connected to the adapter. • PDN-ACTV—SAP activation in progress. • PND-INAC—SAP deactivation in progress. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
link	Name of the configured link. If not a configured link, then the name is an invented name, @DLUR

Table 57 show extended channel tn3270-server dlur Field Descriptions (continued)

Field	Description
remote	Remote MAC and SAP for this link.
link status	Values and their meanings are: • ACTIVE—Link is active. • INACTIVE—Not connected to host. • PND-ACTV—Link activation in progress. • PND-INAC—Link deactivation in progress. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.

show extended channel tn3270-server dlurlink

To display information about the Dependent Logical Unit Requestor (DLUR) components, use the **show extended channel tn3270-server dlurlink** command in user EXEC or privileged EXEC mode.

show extended channel *slot***/***port* **tn3270-server dlurlink** *name*

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
port	Port number.
name	Name of the Systems Network Architecture (SNA) session switch link to be displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server dlurlink** command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel tn3270-server dlurlink** command:

```
Router# show extended channel 3/2 tn3270-server dlurlink P390

lsap token-adapter  0 5C  vrn MPX.LAN4             status ACTIVE
link P390                 remote 4000.7470.00e7 08  status ACTIVE
partner MPX.NGMVMPC       tgn 1                     maxdata   1033
```

Table 58 describes the significant fields in the display.

Table 58 show extended channel tn3270-server dlurlink Field Descriptions

Field	Description
lsap vrn status	Values and their meanings are: • ACTIVE—The service access point (SAP) is open. • INACTIVE—Not connected to the adapter. • PDN-ACTV—SAP activation in progress. • PND-INAC—SAP deactivation in progress. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
link	Name is an invented name, @DLUR*nn*, if not a configured link.
link status	Values and their meanings are: • ACTIVE—The SAP is open. • INACTIVE—Not connected to the adapter. • PDN-ACTV—SAP activation in progress. • PND-INAC—SAP deactivation in progress. • OTHER—Status is an undefined value. • WAIT—Waiting for status from the CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
partner	Control point (CP) name of the remote node for this link.
tgn	Transmission group (TG) number for this link. Because the SNA session switch supports only one TG per pair of CP names, it is typically 0 or 1.
maxdata	Maximum frame size allowed on this link.

Related Commands

Command	Description
client pool	Nails clients to pools.

show extended channel tn3270-server nailed-domain

To list all nailing statements with a specific nailed-domain name, use the **show extended channel tn3270-server nailed-domain** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server nailed-domain** *name*

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
name	Specifies the *exact* nailed-domain name, as specified originally in the **client pool** command. Output is displayed for the nailed-domain name *exactly* as specified. That is, specifying "cisco.com" is different from specifying ".cisco.com."

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

Examples

The following is sample output from the **show extended channel tn3270-server nailed-domain** command:

```
Router# show extended channel 1/2 tn3270-server nailed-domain .cisco.com

.CISCO.COM  listen-point 172.18.4.18  pool PCPOOL
```

Table 59 describes the significant fields in the display.

Table 59 show extended channel tn3270-server nailed-domain Field Descriptions

Field	Description
.CISCO.COM	Nailed domain name.
listen point	Listen point IP address under which the **client pool** command was configured.
pool	Pool name to which the client is nailed.

show extended channel tn3270-server nailed-ip

To display mappings between a nailed client IP address and nailed logical unit (LU)s, use the **show extended channel tn3270-server nailed-ip** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server nailed-ip** *ip-address*

Syntax Description

slot	Slot number.
port	Port number.
ip-address	Remote client IP address.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server nailed-ip** command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel tn3270-server nailed-ip** command:

```
Router# show extended channel 3/2 tn3270-server nailed-ip 172.28.0.0

172.28.1.0  255.255.255.192    pu BAGE1  lu 1     50
172.28.1.80 255.255.255.248    pu BAGE2  lu 100  200    printer
172.28.1.83                    pu BAGE3  lu 1     60    printer
172.28.1.82                    pu BAGE1  lu 100  200
```

Table 60 describes the significant fields in the display.

Table 60 show extended channel tn3270-server nailed-ip Field Descriptions

Field	Description
172.28.1.0	IP address of the nailed client.
255.255.255.192	Network mask for the range of configured nailed clients.
pu BAGE1	PU name under which the **client** command was configured.

Table 60 show extended channel tn3270-server nailed-ip Field Descriptions (continued)

Field	Description
lu 1 50	LU local address range showing the first local address and last local address. There need not be a last local address if only a single local address rather than a range is configured.
printer	Type of device being nailed to the local addresses. If printer is specified, only clients that are printers are nailed to the local addresss. If screen is specified, only clients that are screens are nailed to the local addresss. If neither is specified, both screens and printers can use the local addresss. A printer client is any client with a device type of “328*”. A screen client is a client with any other device type.

show extended channel tn3270-server nailed-name

To list all nailing statements with a specific nailed machine name, use the **show extended channel tn3270-server nailed-name** command in user EXEC or privileged EXEC mode.

show extended channel *slot***/***virtual-channel* **tn3270-server nailed-name** *name*

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
name	Specifies the nailed machine name. This name is specified originally in the **client pool** command.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show extended channel tn3270-server nailed-name** command:

```
Router# show extended channel 1/2 tn3270-server nailed-name myclient.cisco.com

MYCLIENT.CISCO.COM     listen-point 172.18.4.18  pool PCPOOL
HISCLIENT.CISCO.COM    listen-point 172.18.4.18  pool UNIXPOOL
HERCLIENT.CISCO.COM    listen-point 172.18.4.19  pool GENERALPOOL
```

Table 61 describes the significant fields in the display.

Table 61 show extended channel tn3270-server nailed-name Field Descriptions

Field	Description
MYCLIENT.CISCO.COM	Fully qualified domain name of nailed client.
listen point	Listen point IP address under which the **client pool** command was configured.
pool	Pool name to which the client is nailed.

show extended channel tn3270-server pu

To display configuration parameters for a physical unit (PU) and all the logical unit (LU)s attached to the PU, including the logical unit (LU) cluster layout and pool name, use the **show extended channel tn3270-server pu** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server pu** *pu-name* [**cluster** | **client-name**]

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
pu-name	Name that uniquely identifies this PU.
cluster	(Optional) Displays cluster information for the LUs within the pool.
client-name	(Optional) Displays client name information for the LUs within the pool.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
11.2(2.1)	ACT/NA replaced ACTIVE status for logical unit (LU) states. A note was added to the output to describe its meaning.
11.2(18)BC	The **cluster** keyword was added.
12.0(5)T	The following fields were added to the output display: • lu-termination • lu-deletion
12.1(5)T	The **client-name** keyword was added.
12.2	The named value was added for the lu-deletion field in the output display.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server pu** command is valid only on the virtual channel interface. The display shown depends on whether the PU is a direct PU or a Systems Network Architecture (SNA) session switch PU.

The output from the **show extended channel tn3270-server pu** command varies based on use of the optional **cluster** keyword. Without the **cluster** keyword, the output column headings for the LU information appear as “model,” “frames in out,” and “idle for.”

When you use the **cluster** keyword, the output column headings for the LU information appear as “cluster,” “pool,” and “count.” The cluster heading lists the specific cluster within the pool to which the LU belongs, along with the specific cluster layout after the slash.

The pool heading identifies the corresponding pool name, and the count heading identifies the cluster number out of the total number of clusters in the pool.

There is not a **no** form for this command.

Examples

The following example shows a sample router configuration and the corresponding output using the **show extended channel tn3270-server pu** command:

```
interface Channel6/1
 no ip address
 no keepalive
 csna E160 40
!
interface Channel6/2
 ip address 172.18.4.17 255.255.255.248
 no keepalive
 lan TokenRing 15
  source-bridge 15 1 500
  adapter 15 4000.b0ca.0015
 lan TokenRing 16
  source-bridge 16 1 500
  adapter 16 4000.b0ca.0016
 tn3270-server
  pool PCPOOL   cluster layout 4s1p
  pool SIMPLE   cluster layout 1a
  pool UNIXPOOL cluster layout 49s1p
  dlur NETA.SHEK NETA.MVSD
   lsap token-adapter 15 04
    link SHE1     rmac 4000.b0ca.0016
  listen-point 172.18.4.18 tcp-port 23
   pu PU1      91903315 dlur
    allocate lu 1 pool PCPOOL   clusters 10
    allocate lu 51 pool UNIXPOOL clusters 2
    allocate lu 200 pool SIMPLE   clusters 50
  listen-point 172.18.4.19 tcp-port 2023
   pu PU2      91913315 token-adapter 16 08
    allocate lu 1 pool UNIXPOOL clusters 2
    allocate lu 101 pool SIMPLE   clusters 100
    allocate lu 201 pool PCPOOL   clusters 10
```

The following sample output from the **show extended channel tn3270-server pu** command without the cluster keyword for a PU named PU1:

```
Router# show extended channel 6/2 tn3270-server pu pu1

name(index)    ip:tcp               xid   state     link   destination r-lsap
PU1(1)       172.18.4.18:23      91903315 ACTIVE    dlur   NETA.SHPU1

idle-time 0  keepalive 1800 (send nop)  unbind-act disconnect  generic-poolperm
ip-preced-screen 0  ip-preced-printer 0  ip-tos-screen 0  ip-tos-printer 0
lu-termination unbind  lu-deletion never
bytes 27019 in, 73751 out; frames 1144 in, 869 out; NegRsp 0 in, 0 out
actlus 5, dactlus 0, binds 5
Note: if state is ACT/NA then the client is disconnected
```

```
lu    name   client-ip:tcp       nail state    model   frames in out  idle for
1   SHED1001 10.44.100.162:1538   N   ACT/SESS 3278S2E  228     172    0:0:2
51  SHED1051 10.44.100.162:1539   N   ACT/SESS 3278S2E  240     181    0:0:2
151 SHED1151 10.44.100.162:1536   N   ACT/SESS 327802E  212     160    0:0:5
152 SHED1152 10.44.100.162:1537   N   ACT/SESS 3278S2E  220     166    0:0:4
200 SHED1200 10.44.100.162:1557   N   ACT/SESS 3278S2E  244     184    0:0:2
```

The following is sample output from the **show extended channel tn3270-server pu** command with the cluster keyword for a PU named PU1. In the example, 1/1a identifies cluster 1 with a layout of 1a, which contains one LU of any type.

```
Router# show extended channel 6/2 tn3270-server pu pu1 cluster

name(index)    ip:tcp              xid   state     link   destination  r-lsap
PU1(1)       172.18.4.18:23      91903315 ACTIVE    dlur   NETA.SHPU1

idle-time 0  keepalive 1800 (send nop)  unbind-act discon  generic-poolperm
ip-preced-screen 0  ip-preced-printer 0  ip-tos-screen 0  ip-tos-printer 0
lu-termination unbind lu-deletion never
bytes 27489 in, 74761 out; frames 1164 in, 884 out; NegRsp 0 in, 0 out
actlus 5, dactlus 0, binds 5
Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail state    cluster   pool  count
1   SHED1001 10.44.100.162:1538   N   ACT/SESS 1/4s1p  PCPOOL   1/5
51  SHED1051 10.44.100.162:1539   N   ACT/SESS 1/49s1p UNIXPOOL 1/50
151 SHED1151 10.44.100.162:1536   N   ACT/SESS 1/1a    :GENERIC 1/1
152 SHED1152 10.44.100.162:1537   N   ACT/SESS 1/1a    :GENERIC 1/1
200 SHED1200 10.44.100.162:1557   N   ACT/SESS 1/1a    SIMPLE   1/1
```

Note If the cluster layout is very long, only the first eight bytes are displayed under the cluster column. The pool called: GENERIC is shown for all LUs that are not allocated to any specific pool name.

The following is sample output from the **show extended channel tn3270-server pu** command with the **client-name** keyword for a PU named JADOEPU:

```
Router# show extended channel 1/2 tn3270-server pu jadoepu client-name

  name(index)    ip:tcp              xid   state     link   destination   r-lsap
  JADOEPU(1)   172.18.5.168:23     91922362 ACTIVE    tok 31 4000.4000.0001 04 10

  idle-time    0      keepalive   30      unbind-act discon   generic-pool perm
  ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen  0 ip-tos-printer  0
  lu-termination unbind lu-deletion never
  bytes 824 in, 2619 out; frames 36 in, 39 out; NegRsp 0 in, 0 out
  actlus 4, dactlus 0, binds 3
  Note: if state is ACT/NA then the client is disconnected

  lu    name   client-name            nail  state    model frames in out  idle for
  1   VINCDP01 never connected          Y  ACT/NA          1       1       2:31:43
  2   VINCDP02 never connected          Y  ACT/NA          1       1       2:31:43
  5   VINDG005 HERCLIENT.CISCO.COM      Y  ACT/SESS 327904E 22      21      0:0:6
  6   VINDG006 HISCLIENT.CISCO.COM      Y  ACT/NA   327904E 12      12      1:44:47

  client-ip        mask             nail-type  lu-first  lu-last
  10.20.30.40                       screen     1         2
  20.30.40.50                       screen     9         10

  client-name                       nail-type  lu-first  lu-last
  MYCLIENT.CISCO.COM                screen     5         10
  .CISCO.COM                        screen     11        15
```

Table 62 describes the significant fields in the display.

Table 62 show extended channel tn3270-server pu Field Descriptions

Field	Description
name (index)	Name and index of the PU as configured.
ip:tcp	IP address and TCP port number configured for the PU.
xid	Configured XID—idblk and idnum.
state	pu-state values and their meaning are: • SHUT—PU is configured but in shut state. • RESET—Link station of this PU is not active. • TEST—PU is sending a TEST to establish link. • XID—TEST is responded, exchange identification (XID) is sent. • P-ACTPU—Link station is up but no Activate Physical Unit (ACTPU) is received. • ACTIVE—ACTPU is received and acknowledged positively. • ACT/BUSY—Awaiting host to acknowledge the system services control points (SSCP)-PU data. • WAIT—Waiting for PU status from CMCC adapter. • UNKNOWN—Direct PU in undefined state. • P-RQACTPU-R—PU is pending request ACTPU response. • P-ACTIVE—Dependent Logical Unit Requestor (DLUR) PU and direct PU states disagree. • P-DACTPU—PU is pending Deactivate Physical Unit (DACTPU). • OTHER—State is an undefined value.
link	LINK type is either internal adapter type and internal adapter number, or dlur if it is an SNA Session Switch PU.
destination	If a direct PU, then it is the destination MAC address; otherwise, it is the name of the partner PU.
r-lsap	Remote and local service access point (SAP) values.
idle-time	Configured idle time for this PU.
keepalive	Configured keepalive time for this PU. The *action* is one of the following: • **send nop**—The Telnet command for no operation is sent to the TN3270 client to verify the physical connection. • **send timing mark** *number*—Number of seconds within which the TN3270 server expects a response to the DO TIMING-MARK from the TN3270 client.
unbind-act	Configured unbind action for LUs on this PU.
generic-pool	Configured generic pool for LUs on this PU.
ip-preced-screen	IP precedence value for screen LUs on this PU.
ip-preced-printer	IP precedence value for printer LUs on this PU.

Table 62 show extended channel tn3270-server pu Field Descriptions (continued)

Field	Description
ip-tos-screen *number*	IP type of service (ToS) value for screen LUs on this PU.
ip-tos-printer *number*	IP ToS value for printer LUs on this PU.
lu-termination	Value configured in the PU for the **lu termination** siftdown command. The **lu termination** command specifies whether a TERMSELF or UNBIND request/response unit (RU) is sent by the TN3270 server when a client turns off the device or disconnects. The values are: • termself—Termination of all sessions and session requests associated with an LU is ordered upon disconnect. • unbind—Termination of the session by the application is requested upon LU disconnect.
lu-deletion	Value configured in the PU for the **lu deletion** siftdown command. The **lu deletion** command specifies whether the TN3270 server sends a REPLY-PSID poweroff request to virtual telecommunications access method (VTAM) to delete the corresponding LU when a client disconnects. The values are: • always—Dynamic LUs for this PU are always deleted upon disconnect. • named—Only named LUs for this PU are deleted upon disconnect. • normal—Only screen LUs for this PU are deleted upon disconnect. • non-generic—Only specified LUs for this PU are deleted upon disconnect. • never—None of the LUs for this PU are ever deleted upon disconnect.
bytes in/out	Total number of bytes sent to or received from the host for this PU.
frames in/out	Total number of frames sent to or received from the host for this PU.
NegRsp in/out	Total number of SNA negative responses sent to or received from the host.
actlus	Total number of ACTLUs received from the host.
dactlus	Total number of DACTLUs received from the host.
binds	Total number of BINDs received from the host.
lu	Local address of the LU.
name	Name of the TN3270 LU.
client-name	Client’s IP address and TCP port number.
nail	Status of LU nailing, either Y or N

Table 62 show extended channel tn3270-server pu Field Descriptions (continued)

Field	Description
state	LU state values and their meanings: • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive activate logical unit (ACTLU). • ACT/NA—LU received ACTLU and acknowledged positively. If a client IP address is shown, then the client is disconnected. • P-SDT—LU is bound but there is no Structured Data Transfer (SDT) yet. • ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet has connected and is awaiting ACTLU. • P-NTF/av—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Waiting for a buffer to send Deactivate LU (DACTLU) response. • P-PSID—Waiting for NMVT Reply psid response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model	IBM 3278 model type of client.
frames in	Number of frames sent inbound to the host.
frames out	Number of frames sent outbound from the host.
idle for	Time the client has been idle. The time is in HH:MM:SS.
client-ip	Remote client IP address.
mask	Current network mask.
nail-type	LU nailing type, screen or printer.
lu-first	First LU address in the range.
lu-last	Last LU address in the range, if one is specified in the **client** configuration command.
client-name	Client machine name or domain name.
nail-type	LU nailing type, screen or printer.
lu-first	First LU address in the range.
lu-last	Last LU address in the range, if one is specified in the **client** configuration command.

Related Commands

Command	Description
allocate lu	Assigns LUs to a pool.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.

show extended channel tn3270-server pu lu

To display information about the TN3270 server logical unit (LU)s running on the Cisco Mainframe Channel Connection (CMCC) adapter interface, use the **show extended channel tn3270-server pu lu** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **tn3270-server pu** *pu-name* **lu** *locaddr* [**history**]

Syntax Description

slot	Specifies a particular CMCC adapter in the router where the *slot* argument is the slot number. The port value for a TN3270 server will always be 2.
port	Port value for a TN3270 server will always be 2.
pu-name	Physical unit (PU) name that uniquely identifies this PU.
locaddr	Logical unit (LU) local address that uniquely identifies the LU.
history	(Optional) Displays the LU trace history.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
11.2(2.1)	ACT/NA replaced ACTIVE status for LU states. A note was added to the output to describe its meaning.
11.2(18)BC	The response time buckets, average total response time, average IP response time, and the number of transactions fields were added to the output display.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server pu lu** command is valid only on the virtual channel interface.

Examples

The following is sample output from the **show extended channel tn3270-server pu lu** command for a Systems Network Architecture (SNA) session switch PU:

```
Router# show extended channel 3/2 tn3270 pu int1 lu 1

Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail  state      model   frames in out   idle for
```

```
1   GOAN1X01 10.69.176.77:3828    N    ACT/NA              4       4       0:4:51

pu is INT1, lu is STATIC type 0, negotiated TN3270E
bytes 74 in, 1219 out; RuSize 0 in, 0 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
```

The following is sample output from the **show extended channel tn3270-server pu lu history** command:

```
Router# show extended channel 3/2 tn3270 pu pus20 lu 1 history

Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail  state      model   frames in out   idle for
1   PUS20001 10.195.80.40:2480    N    ACT/SESS  327804    5       4       0:0:8

pu is PUS20, lu is DYNAMIC type 2, negotiated TN3270
bytes 155 in, 1752 out; RuSize 1024 in, 3840 out; NegRsp 0 in, 0 out>pacing window 0 in, 1
out; credits 0 in, queue-size 0 in, 0 out
traces:
         Client connect req
         Reply PSID pos rsp
         actlu req
         bind req
         sdt req
OUT len=12   2Dxxxxxxxx456B80000D0201
IN  len=25   xxxxxxxxxx45EB80000D0201000000
OUT len=53   2Dxxxxxxxx466B800031010303B1
IN  len=10   2D0001010646EB800031
OUT len=10   2D00010106476B8000A0
IN  len=10   2D0001010647EB8000A0
OUT len=1677 2Cxxxxxxxx010381C07EC7114040
IN  len=9    2C0001010001838100
```

The following example shows the response-time information using the **show extended channel tn3270-server pu lu** command for the LU at local address 1 associated with the PU named vincdpu:

```
sydney# show extended channel 1/2 tn3270-server pu vincdpu lu 1
Note: if state is ACT/NA then the client is disconnected

lu    name   client-ip:tcp       nail   state    model frames in out   idle for
1   VINDG001 10.44.100.210:1315   N   ACT/NA   3278S2E  12      11      0:0:18

pu is VINCDPU, lu is DYNAMIC unbound, negotiated TN3270E
bytes 253 in, 954 out; RuSize 0 in, 0 out; NegRsp 1 in, 0 out
pacing window 0 in, 1 out; credits 0 in, queue-size 0 in, 0 out
response time buckets 14 31 15 3 1
average total response time 19 average IP response time 8
number of transactions 64
```

Table 63 describes the significant fields in the display.

Table 63 show extended channel tn3270-server pu lu Field Descriptions

Field	Description
lu	Local address of the LU.
name	Name of the TN3270 LU.
client-ip:tcp	Client’s IP address and TCP port number.

Table 63 show extended channel tn3270-server pu lu Field Descriptions (continued)

Field	Description
state	LU state values and their meanings are: • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive activate logical unit (ACTLU). • ACT/NA—LU received ACTLU and acknowledged positively. If a client IP address is shown, then the client is disconnected. • P-SDT—LU is bound but there is no Structured Data Transfer (SDT) yet. • ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet connects in and is awaiting ACTLU. • P-NTF/AV—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Waiting for a buffer to send Deactivate LU (DACTLU) response. • P-PSID—Waiting for NMVT Reply PSID response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model	IBM 3278 model type of client; blank if Static LU.
frames in	Number of frames sent inbound to the host.
frames out	Number of frames sent outbound from the host.
idle for	Time the client has been idle. The time is in HH:MM:SS.
pu is	Name of the PU.
lu is	Whether LU is DYNAMIC or STATIC.
negotiated	Whether client is TN3270 or TN3270E.
bytes in/out	Total number of bytes sent to or received from the host.
RuSize in/out	Request/response unit (RU) size as configured in the bind.
NegRsp in/out	Number of Systems Network Architecture (SNA) negative responses sent to or received from the host.
pacing window in/out	SNA pacing window as configured in the bind.
credits in	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue-size in	If nonzero, indicates the number of SNA frames waiting to be sent to the host that are blocked, waiting for a pacing response.
queue-size out	SNA frames not yet acknowledged by an isolated pacing response by the TN3270 server.

Table 63 show extended channel tn3270-server pu lu Field Descriptions (continued)

Field	Description
response time buckets	Displays the number of transactions in each response-time “bucket” for the specified LU. The bucket boundaries are defined using the **response-time group** command.
average total response time	Average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
response-time group	Configures a client subnet group for response-time measurements.

show extended channel tn3270-server response-time application

To display information for application client groups, use the **show extended channel tn3270-server response-time application** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time application** [*appl-name* [**detail**]]

Syntax Description

slot	Slot number.
virtual-channel	Virtual channel number.
appl-name	(Optional) Display only the client group corresponding to the virtual telecommunications access method (VTAM) application name.
detail	(Optional) List client members and their response-time statistics following the client group entry.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If optional keywords are not used for the **show extended channel tn3270-server response-time application** command, a complete list of existing per-application client groups is displayed along with their collection control parameters. If you specify the *appl-name* argument, only the client group corresponding to that application is displayed. If you specify the **detail** keyword, the client group entry is followed by a list of its client members and their response-time statistics.

Examples

The following is sample output from the **show extended channel tn3270-server response-time application** command:

```
Router# show extended channel 3/2 tn3270-server response-time application MYAPPL
group APPL MYAPPL
  aggregate NO excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
```

Table 64 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 64 show extended channel tn3270-server response-time application Field Descriptions

Field	Description
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to NO by the TN3270 server for application client response-time groups.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to NO by the TN3270 server for application client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
response time buckets	Displays the number of transactions in each response-time “bucket” for the specified application group. The bucket boundaries are defined using the **response-time group** command.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.

Command	Description
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

show extended channel tn3270-server response-time global

To display collection control parameters for the global client group, use the **show extended channel tn3270-server response-time global** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time global**

Syntax Description

slot	Slot number.
virtual-channel	Virtual channel number.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server response-time global** command displays collection control parameters for the global client group.

Examples

The following is sample output from the **show extended channel tn3270-server response-time global** command:

```
Router# show extended channel 3/2 tn3270-server response-time global

group CLIENT GLOBAL
  aggregate YES excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 105 118 211 109 104
  average total response time 33 average IP response time 24
  number of transactions 647
```

Table 65 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 65 show extended channel tn3270-server response-time global Field Descriptions

Field	Description
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to YES by the TN3270 server for global client response-time groups.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to NO by the TN3270 server for global client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
bucket boundaries	Displays the value of the response-time bucket boundaries in tenths of seconds. The bucket boundaries are defined using the **response-time group** command.
buckets	Displays the number of transactions in each response-time bucket for the specified application group.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

show extended channel tn3270-server response-time link

To display information about host link client groups, use the **show extended channel tn3270-server response-time link** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time link** [*link-name*]

Syntax Description

slot	Slot number.
virtual-channel	Port number.
link-name	(Optional) physical unit (PU) name for a direct PU or link name for a Dependent Logical Unit Requestor (DLUR) PU.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was first introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays information clients groups by host link. If no optional arguments are specified, a complete list of existing client groups by host link is displayed along with their collection control parameters and aggregate response-time statistics. If a value for the *link-name* argument is specified, only the client group corresponding to that link is displayed.

Examples

The following is sample output from the **show extended channel tn3270-server response-time link** command without optional arguments. It shows all client groups by host link:

```
Router# show extended channel 3/2 tn3270-server response-time link

group DIRECT LINK MYLINK
  aggregate YES excludeip YES dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 10 18 21 10 10
  average total response time 37 average IP response time 23
  number of transactions 69
group DLUR LINK HISLINK
  aggregate YES excludeip YES dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 14 31 15 3 1
  average total response time 19 average IP response time 8
  number of transactions 64
```

The following is sample output from the **show extended channel tn3270-server response-time link** command for the link named Direct link mylink:

```
Router# show extended channel 3/2 tn3270-server response-time link direct link mylink

group DIRECT LINK MYLINK
  aggregate YES excludeip YES dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 10 18 21 10 10
  average total response time 37 average IP response time 23
  number of transactions 69
```

Table 66 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 66 show extended channel tn3270-server response-time link Field Descriptions

Field	Description
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to YES by the TN3270 server for link client response-time groups.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to YES by the TN3270 server for link client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
bucket boundaries	Displays the value of the response-time bucket boundaries in tenths of seconds. The bucket boundaries are defined using the **response-time group** command.
buckets	Displays the number of transactions in each response-time bucket for the specified application group.

Table 66 show extended channel tn3270-server response-time link Field Descriptions

Field	Description
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

show extended channel tn3270-server response-time listen-point

To display information about listen-point client groups, use the **show extended channel tn3270-server response-time listen-point** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time listen-point**

Syntax Description

slot	Slot number.
virtual-channel	Virtual channel number.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was first introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel tn3270-server response-time listen-point** command displays information about groups of clients summarized by listen point. A complete list of currently existing listen-point client groups is displayed along with their collection control parameters and aggregate response-time statistics.

Examples

The following is sample output from the **show extended channel tn3270-server response-time listen-point** command:

```
Router# show extended channel 3/2 tn3270-server response-time listen-point

group LP 10.20.30.40:23
  aggregate YES excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 10 18 21 10 10
  average total response time 37 average IP response time 23
  number of transactions 69
group LP 50.60.70.80:23
  aggregate YES excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  buckets 310 418 521 510 210
```

```
average total response time 27 average IP response time 20
number of transactions 1969
```

Table 67 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 67 show extended channel tn3270-server response-time listen-point Field Descriptions

Field	Description
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to YES by the TN3270 server for link client response-time groups.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to NO by the TN3270 server for link client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
bucket boundaries	Displays the value of the response-time bucket boundaries in tenths of seconds. The bucket boundaries are defined using the **response-time group** command.
buckets	Displays the number of transactions in each response-time bucket for the specified application group.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

show extended channel tn3270-server response-time subnet

To display information about subnet client groups, use the **show extended channel tn3270-server response-time subnet** command in privileged EXEC mode.

show extended channel *slot*/*virtual-channel* **tn3270-server response-time subnet** [**ip-address** *ip-mask* [**detail**]]

Syntax Description

slot	Slot number.
virtual-channel	Virtual channel number.
ip-address	(Optional) Subnet IP address.
ip-mask	(Optional) Subnet mask.
detail	(Optional) Each client group entry is followed by a list of its client members and their respective response-time statistics.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2(18)BC	This command was first introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays information about client subnet client groups. This includes all configured groups and the CLIENT SUBNET OTHER group. If no optional parameters are specified, a complete list of client subnet client groups is displayed along with their collection control parameters. If you specify values for the **ip-address** keyword and *ip-mask* argument, only client groups containing that subnet are displayed. If you specify the **detail** keyword, each client group entry is followed by a list of its client members and their response-time statistics.

Examples

The following is sample output from all configured client groups using the **show extended channel tn3270-server response-time subnet** command:

```
Router# show extended channel 3/2 tn3270-server response-time subnet

group SUBNETGROUP1
  subnet 10.10.10.0 255.255.255.192
  aggregate NO excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
```

```
group SUBNETGROUP2
  subnet 10.10.10.128 255.255.255.192
  subnet 10.10.10.192 255.255.255.192
  aggregate NO exclude ip NO dynamic definite response NO
  sample period multiplier 40
  bucket boundaries 20 30 60 120
group CLIENT SUBNET OTHER
  aggregate NO exclude ip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
```

The following is sample output from subnet 10.10.10.0 with IP mask 255.255.255.192, which shows a list of the client members and their response-time statistics:

```
Router# show extended channel 3/2 tn3270-server response-time subnet
10.10.10.0 255.255.255.192 detail

group SUBNETGROUP1
  subnet 10.10.10.0 255.255.255.192
  aggregate NO excludeip NO dynamic definite response NO
  sample period multiplier 30
  bucket boundaries 10 20 50 100
  client 10.10.10.129:23
    buckets 5 8 11 9 4
    average total response time 33 average IP response time 24
    number of transactions 37
  client 10.10.10.130:23
    buckets 6 9 10 10 2
    average total response time 32 average IP response time 25
    number of transactions 37
  client 10.10.10.131:23
    buckets 11 14 10 8 7
    average total response time 27 average IP response time 19
    number of transactions 50
```

Table 68 describes the significant fields in the display.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 68 show extended channel tn3270-server response-time subnet Field Descriptions

Field	Description
subnet	Displays the IP address and IP mask of the client subnet group for which response-time statistics are being shown.
aggregate	Displays whether the response time statistics for the clients in this response-time group are reported collectively for the group (YES) or individually by client (NO). This value is automatically set to NO by the TN3270 server for subnet client response-time groups.

Table 68 show extended channel tn3270-server response-time subnet Field Descriptions (continued)

Field	Description
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the Systems Network Architecture (SNA) component (the server/host path) is included in the response time for any transaction (YES). This value is automatically set to NO by the TN3270 server for subnet client response-time groups.
dynamic definite response	Displays whether the server adds a Definite Response request to the first-in-chain (FIC) reply in each transaction, to get a response from the client so that the IP component can be included in the response time. The value is automatically set to NO by the TN3270 server for all types of response-time groups.
sample period multiplier	Displays the number that is multiplied by an interval of 20 seconds to determine the collection interval for the response-time group. The multiplier value is defined using the **response-time group** command. For example, a sample period multiplier of 30 results in a collection interval of 600 seconds (30 x 20 seconds), or 10 minutes, for this client group.
bucket boundaries	Displays the value of the response-time bucket boundaries in tenths of seconds. The bucket boundaries are defined using the **response-time group** command.
buckets	Displays the number of transactions in each response-time bucket for the specified application group.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Displays the average response time in tenths of seconds (including IP transit time) for the total number of response-time transactions.
number of transactions	Displays the total number of response-time transactions across all response-time buckets.

Related Commands

Command	Description
response-time group	Configures a client subnet group for response-time measurements.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.

show extended channel tn3270-server security

To display information about the TN3270 security enhancement, use the **show extended channel tn3270-server security** command in user EXEC or privileged EXEC mode.

show extended channel *slot***/***virtual-channel* **tn3270-server security** [**sec-profile** *profilename*] [**listen-point** *ip-address* [**tcp-port** *number*]]

Syntax Description

slot	Specifies a particular Cisco Mainframe Channel Connection (CMCC) adapter in the router where the *slot* argument is the slot number.
virtual-channel	Virtual channel number.
sec-profile *profilename*	(Optional) Alphanumeric name that specifies the security profile name to be associated with a listen point. The character range is from 1 to 24. This name is specified originally in the **profile** command.
listen-point *ip-address*	(Optional) IP address that the clients should use as the host IP address to map to logical unit (LU) sessions under this physical unit (PU) and listen point.
tcp-port *number*	(Optional) Port number used for the listen operation. The default value is 23.

Defaults

The default **tcp-port** value is 23.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There is not a **no** form for this command.

Examples

The following is sample output from the **show extended channel tn3270-server security** command with the optional **sec-profile** keyword configured:

```
Router# show extended channel 3/2 tn3270-server security sec-profile cert40

status:ENABLE Default Profile: (Not Configured)
Name               Active LUs  keylen encryptorder            Mechanism
CERT40                    0     40    RC4 RC2 RC5 DES 3DES    SSL
Servercert:slot0:coach188.pem
```

```
Certificate Loaded:YES Default-Profile:NO
```

The following is sample output from the **show extended channel tn3270-server security** command with the optional **listen-point** keyword configured:

```
Router# show extended channel 3/2 tn3270-server security listen-point 172.18.5.188

status:ENABLE Default Profile: (Not Configured)
IPaddress      tcp-port   Security-Profile   active-sessions  Type    State
172.18.5.188    23        CERT40                0             Secure  ACTIVE
Active Sessions using Deleted Profile:0
```

Table 69 describes the significant fields in the display.

Table 69 show extended channel tn3270-server security Field Descriptions

Field	Description
status ENABLE	Status of TN3270 server security. Enable or Disable.
Default Profile (Not Configured)	Displays if a default profile is configured. (Not Configured) or (Configured).
Name	Name of the security profile as specified in the **profile** command.
Active LUs	Number of active LUs.
keylen	Maximum encryption key length in bits.
encryptorder	Order of encryption algorithms. Choices are DES, 3DES, RC4, RC2, or RC5.
Mechanism	Type of security protocol being used. Values are SSL or none.
Servercert	Location of the TN3270 server's security certificate status in the Flash memory.
Certificate Loaded	Security certificate is loaded. YES or NO.
Default-Profile	Default profile is configured. YES or NO.
IPaddress	IP address that the clients should use as the host IP address to map to LU sessions under this PU and listen point.
tcp-port	Port number used for the listen operation. The default value is 23.
Security-Profile	Name of the security profile as specified in the **profile** command.
active-sessions	Number of active sessions.
Type	Type of connection.
State	State of the listen point.
Active Sessions using Deleted Profile:	Number of sessions using a security profile that has been deleted.

Related Commands

Command	Description
sec-profile	Specifies the security profile to be associated with a listen point.
listen-point	Defines an IP address for the TN3270 server.

show extended channel udp-listeners

To display information about the User Datagram Protocol (UDP) listener sockets running on the Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show extended channel udp-listeners** command in user EXEC or privileged EXEC mode.

show extended channel *slot***/***port* **udp-listeners** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
udp-listeners	Specifies UDP listener port display.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn3270-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel udp-listeners** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show extended channel udp-listeners** command:

```
Router# show extended channel 0/1 udp-listeners

UDP Listener: IP Address 10.11.198.3        LocalPort 7
UDP Listener: IP Address 10.11.198.3        LocalPort 9
UDP Listener: IP Address 10.11.198.3        LocalPort 19
```

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.

Command	Description
pu (TN3270)	Creates a PU entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.

show extended channel udp-stack

To display information about the User Datagram Protocol (UDP) stack running on the Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show extended channel udp-stack** command in user EXEC or privileged EXEC mode.

show extended channel *slot*/*port* **udp-stack** [*ip-address*]

Syntax Description

slot	Slot number.
port	Port number.
udp-stack	Selects UDP stack display.
ip-address	(Optional) IP address specified by the **offload** interface configuration command or the **tn3270-server pu** command.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	The Alias addresses field was added to the output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show extended channel udp-stack** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show extended channel udp-stack** command:

```
Router# show extended channel o1 udp-stack

UDP Statistics for IP Address 10.11.198.2
  InDatagrams : 6           NoPorts     : 6
  InErrors    : 0           OutDatagrams: 0
UDP Statistics for IP Address 10.11.198.3
  InDatagrams : 6           NoPorts     : 6
  InErrors    : 0           OutDatagrams: 1
```

The following examples show sample output from the **show extended channel udp-stack** command when you specify the real IP address or the alias IP address, for an offload device at real IP address 10.10.21.3 and alias IP address of 10.2.33.88:

```
Router# show extended channel 3/1 udp-stack 10.10.21.3

UDP Statistics for IP Address 10.10.21.3
```

```
 Alias addresses: 10.2.33.88
  InDatagrams : 6           NoPorts     : 6
  InErrors    : 0           OutDatagrams: 1

Router# show extended channel 3/1 udp-stack 10.2.33.88

UDP Statistics for IP Address 10.10.21.3
 Alias addresses: 10.2.33.88
  InDatagrams : 6           NoPorts     : 6
  InErrors    : 0           OutDatagrams: 1
```

Table 70 describes the specified fields shown in the display.

.

Table 70 show extended channel udp-stack Field Descriptions

Field	Description
Alias addresses	Virtual IP addresses assigned to the real IP address of an offload device.
InDatagrams	Total number of UDP datagrams delivered to UDP users.
NoPorts	Total number of received UDP datagrams for which there was no application at the destination port.
InErrors	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
OutDatagrams	Total number of UDP datagrams sent from this entity.

Related Commands

Command	Description
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
pu (TN3270)	Creates a physical unit (PU) entity that has its own direct link to a host and enters PU configuration mode.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters Dependent Logical Unit Requestor (DLUR) PU configuration mode.

show fras

To display notification that the Frame Relay access support (FRAS) dial backup over data-link switching plus (DLSw+) feature is active, information about the connection state in FRAS, and information about current boundary network node, boundary access node (BAN), and dial backup, use the **show fras** command in privileged EXEC mode.

show fras

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show fras** command:

```
Router# show fras

Boundary Network Node (BNN):
DLCI: 66
  Type   Destination      Int    LSap  RSap   Role  State
  fr                             4      4     S     ls_reset (Backup is enabled)
  llc    0000.f63a.2f50   To0    4      4     P     ls_contacted
```

Table 71 describes the significant fields shown in the display.

Table 71 show fras Field Descriptions

Field	Description
Type	Connection type. The display example shows Logical Link Control (LLC) and Frame Relay.
Destination	Destination MAC address from the perspective of the Cisco IOS software.
Int	Interface on which the connection resides.
LSap	Local service access point (SAP) value.
RSap	Remote SAP value.
Role	Local link station role; P means primary and S means secondary.

Table 71 show fras Field Descriptions (continued)

Field	Description
State	Link station protocol machine state. This value may be one of the following states: • ls_reset—Initial state. • ls_RqOpnStnSent—TEST frame sent; request to open a connection endpoint. • ls_ExchgXid—exchange identification (XID) negotiation taking place. • ls_ConnRqSent—Set Asynchronous Balanced Mode Extended (SABME) sent (connecting side). • ls_SigStnWait—Waiting for signal to clean up the congestion and respond to polling with an Receiver Not Ready (RNR). • ls_ConnRspWait—Wait for the other connection endpoint to bring up the link. • ls_ConnRspSent—A unnumbered acknowledgement (UA) has been sent and the router is waiting for a Receive Ready (RR) to clear up the flow. • ls_Contacted—Everything is connected • ls_DiscWait—Wait for acknowledge to disconnect request.
Backup is enabled	Notification displayed when the FRAS dial backup feature is configured.

show fras map

To display the mapping and connection state of Frame Relay access support (FRAS), use the **show fras map** command in privileged EXEC mode.

show fras map

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show fras map** command:

```
Router# show fras map

Type Destination    Int   LSap   RSap   Role   State
tr   0800.5a8f.8802 tr0   4      4      P      ls_contacted
fr   200            s0    4      4      S      ls_contacted
```

Table 72 describes the significant fields shown in the display.

Table 72 show fras map Field Descriptions

Field	Description
Type	Connection type. The display example shows Logical Link Control (LLC) and Frame Relay.
Destination	Destination MAC address from the perspective of the Cisco IOS software.
Int	Interface on which the connection resides.
LSap	Local service access point (SAP) value.
RSap	Remote SAP value.
Role	Local link station role; P means primary and S means secondary.
State	Connection type. The display example shows Logical Link Control (LLC) and Frame Relay.

show fras-host

To display the status of Logical Link Control, type 2 (LLC2) sessions using the Frame Relay access support (FRAS) Host feature, use the **show fras-host** command in user EXEC or privileged EXEC mode.

show fras-host [*interface*] [**dlci** *dlci-num*] [**detail**]

Syntax Description

interface	(Optional) Only display LLC2 sessions from a specified Frame Relay interface or subinterface.
dlci *dlci-number*	(Optional) Only display LLC2 sessions from a specified data-link connection identifier (DLCI).
detail	(Optional) Display additional information such as the Routing Information Field (RIF)s and statistics associated with the LLC2 sessions.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show fras-host** command:

```
router# show fras-host

Number of Active Control Blocks = 2
Number of Available Control Blocks in Pool = 126

PortDLCITypeFrRsapFrLSapHostSapVMacHostMac
Se0 16  BNN 04  08  04  4000.ABBA.001E4000.3000.2000
Se1 37  BAN 04  04  04  4000.0223.00194000.3000.2000
```

Table 73 describes the significant fields shown in the display.

Table 73 show fras-host Field Descriptions

Field	Description
Port	Frame Relay interface or subinterface associated with this LLC2 session.
DLCI	DLCI number associated with this LLC2 session
Type	FRAS encapsulation type associated with this LLC2 session

Table 73 show fras-host Field Descriptions (continued)

Field	Description
FrRsap	Frame Relay Remote LLC2 service access point (SAP) associated with this LLC2 session. This SAP is the source sap on LLC2 frames sent by the remote Frame Relay access device (FRAD).
FrLSap	Frame Relay Local LLC2 SAP associated with this LLC2 session. This SAP is the destination SAP on LLC2 frames sent by the remote FRAD.
HostSap	Destination SAP on LLC2 frames sent to the Channel Interface Processor (CIP) or LAN-attached AS/400. This SAP is identical to FrLsap unless the **hsap** keyword is specified on the **fras-host bnn** command.
VMac	MAC address associated with the remote FRAD for this LLC2 session.
HostMac	MAC address associated with the host for this LLC2 session.

Related Commands

Command	Description
fras-host ban	Enables the FRAS Host function for BAN.
fras-host bnn	Enables the FRAS Host function for boundary network node.
fras-host dlsw-local-ack	Enables LLC2 local termination for FRAS Host connections using the virtual Token Ring.

show interfaces channel

To display information about the Cisco Mainframe Channel Connection (CMCC) adapter interfaces, use the **show interfaces channel** command in privileged EXEC mode. This command displays information that is specific to the interface hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

show interfaces channel *slot/port* [**accounting**]

Syntax Description

slot	Slot number.
port	Port number.
accounting	(Optional) Displays interface accounting information.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show interfaces channel** command:

```
Router# show interfaces channel 3/0

Channel3/0 is up, line protocol is up
  Hardware is cxBus IBM Channel
  Internet address is 10.92.1.145, subnet mask is 255.255.255.248
  MTU 4096 bytes, BW 0 Kb, DLY 0 usec, rely 255/255, load 1/255
  Encapsulation CHANNEL, loopback not set, keepalive not set
  ECA type daughter card
  Data transfer rate 12 Mbytes  Number of subchannels 1
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 0:00:04
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets, 0 restarts
```

Table 74 describes the fields shown in the display.

Table 74 show interfaces channel Field Descriptions

Field	Description
Channel... is up	Indicates whether the interface hardware is active (whether synchronization is achieved on an ESCON channel, or whether operational out is enabled on a parallel channel) and whether it has been taken down by an administrator.
line protocol is up	Indicates whether the software processes that handle the line protocol "think" the line is usable (that is, whether keepalives are successful).
Hardware is	Hardware type.
Internet address is	IP address and subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes. The calculation uses the value from the **bandwidth** interface configuration command.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether loopbacks are set.
keepalive	Indicates whether keepalives are set.
daughter card	Type of adapter card.
Data transfer rate	Rate of data transfer.
Number of subchannels	Number of subchannels.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface first failed. This counter is updated only when packets are process switched, not when packets are fast switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully sent by an interface. This counter is updated only when packets are process switched, not when packets are fast switched.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of data that took too long to send. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.

Table 74 show interfaces channel Field Descriptions (continued)

Field	Description
Last clearing	The time at which the counters that measure cumulative statistics (such as number of bytes sent and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. These asterisks (***) indicate the elapsed time is too large to be displayed; 0:00:00 indicates the counters were cleared more than 2^{31}ms (and less than 2^{32}ms) ago.
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
Five minute input rate, Five minute output rate	Average number of bits and packets sent per second in the last five minutes.
packets input	Total number of error-free packets received by the system.
bytes input	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
input errors	Total number of buffer, runts, giants, cyclic redundancy checks (CRC), frame, overrun, ignored, and abort counts. Other input-related errors can also increment the count, so that this sum may not balance with the other counts.
CRC	Number of code violation errors seen on the ESCON interface, where a received transmission character is recognized as invalid. On a parallel interface, the number of parity errors seen.
frame	Number of received packets having an incorrect CRC error and a noninteger number of octets. This value is always 0.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data. This value is always 0.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the "no buffer" description. Broadcast storms and bursts of noise can cause the ignored count to be increased.

Table 74 show interfaces channel Field Descriptions (continued)

Field	Description
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data-link equipment. This value is always 0.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Sum of all errors that prevented the final sending of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
output errors	Number of output errors.
collisions	Number of collisions detected. This value is always 0.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for sending were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the send clock signal, or by a cable problem. If the system notices that the carrier detect line of a serial interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down. On the CMCC adapter, this may occur if the host software is not requesting data.
restarts	Number of times the controller was restarted because of errors.

show interfaces crb

To display the configuration for each interface that has been configured for routing or bridging, use the **show interfaces crb** command in privileged EXEC mode.

show interfaces crb

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show interfaces crb** command:

```
Router# show interfaces crb

Ethernet0/0

Routed protocols on Ethernet0/0:
appletalk decnet ip novell

Ethernet0/1

Routed protocols on Ethernet0/1:
appletalk  decnet  ip  novell

Ethernet0/2

Routed protocols on Ethernet0/2:
appletalk  ip

Bridged protocols on Ethernet0/2:
clns  decnet  vines  apollo
novell  xns

Software MAC address filter on Ethernet0/2
Hash Len   Address         Matches   Act   Type
0x00: 0    ffff.ffff.ffff  0         RCV   Physical broadcast
0x00: 1    ffff.ffff.ffff  0         RCV   Appletalk zone
0x2A: 0    0900.2b01.0001  0         RCV   DEC spanning tree
0x49: 0    0000.0c36.7a45  0         RCV   Interface MAC address
0xc0: 0    0100.0ccc.cccc  20        RCV   CDP
0xc2: 0    0180.c200.0000  0         RCV   IEEE spanning tree
0xF8: 0    0900.07ff.ffff  0         RCV   Appletalk broadcast
```

```
Ethernet0/3

Routed protocols on Ethernet0/3:
appletalk  ip

Bridged protocols on Ethernet0/3:
clns  decnet  vines  apollo
novell  xns

Software MAC address filter on Ethernet0/3
Hash Len    Address         Matches    Act    Type
0x00: 0     ffff.ffff.ffff  0          RCV    Physical broadcast
0x00: 1     ffff.ffff.ffff  0          RCV    Appletalk zone
0x2A: 0     0900.2b01.0001  0          RCV    DEC spanning tree
0x49: 0     0000.0c36.7a45  0          RCV    Interface MAC address
0xc0: 0     0100.0ccc.cccc  48         RCV    CDP
0xc2: 0     0180.c200.0000  0          RCV    IEEE spanning tree
0xF8: 0     0900.07ff.ffff  0          RCV    Appletalk broadcast
```

Table 75 describes the significant fields shown in the display.

Table 75 show interfaces crb Field Descriptions

Field	Description
Routed protocols on…	List of the routed protocols configured for the specified interface.
Bridged protocols on…	List of the bridged protocols configured for the specified interface.
Software MAC address filter on…	Table of software MAC address filter information for the specified interface.
Hash	Hash key/relative position in the keyed list for this MAC-address entry.
Len	Length of this entry to the beginning element of this hash chain.
Address	Canonical (Ethernet ordered) MAC address.
Matches	Number of received packets matched to this MAC address.
Act	Action to be taken when that address is looked up; choices are to receive or discard the packet.
Type	MAC address type.

show interfaces irb

To display the configuration for each interface that has been configured for integrated routing or bridging, use the **show interfaces irb** command in privileged EXEC mode.

show interfaces {**ethernet** | **fastethernet**} [*interface* | *slot*/*port*] **irb**

Syntax Description

ethernet	Specify Ethernet interface.
fastethernet	Specify Fast Ethernet interface.
interface	(Optional) Specific interface, such as Ethernet 0.
slot/*port*	(Optional) Specific slot and port, such as Fast Ethernet 3/0.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show interfaces irb** command:

```
Router# show interfaces ethernet 2 irb

Ethernet 2

Routed protocols on Ethernet 2:
appletalk ip

Bridged protocols on Ethernet 2:
appletalk   clns   decnet   vines
apollo      ipx    xns

Software MAC address filter on Ethernet 2
Hash Len  Address         Matches  Act   Type
0x00: 0   ffff.ffff.ffff  4886     RCV   Physical broadcast
0x1F: 0   0060.3e2b.a221  7521     RCV   Appletalk zone
0x1F: 1   0060.3e2b.a221  0        RCV   Bridge-group Virtual Interface
0x2A: 0   0900.2b01.0001  0        RCV   DEC spanning tree
0x05: 0   0900.0700.00a2  0        RCV   Appletalk zone
0xC2: 0   0180.c200.0000  0        RCV   IEEE spanning tree
0xF8: 0   0900.07ff.ffff  2110     RCV   Appletalk broadcast
```

The following example shows that IP is configured for the first PA-12E/2FE interface of the port adapter in slot 3:

```
Router# show interfaces fastethernet 3/0 irb

Fast Ethernet3/0
```

```
Routed protocols on Fast Ethernet3/0:
 ip

Bridged protocols on Fast Ethernet3/0:
 appletalk  clns       decnet     ip
 vines      apollo     ipx        xns

Software MAC address filter on Ethernet3/0
 Hash Len    Address      Matches  Act      Type
 0x00:  0 ffff.ffff.ffff         0 RCV Physical broadcast
 0x2A:  0 0900.2b01.0001         0 RCV DEC spanning tree
 0xC2:  0 0180.c200.0000         0 RCV IEEE spanning tree
 0xC7:  0 00e0.f7a4.5130         0 RCV Interface MAC address
 0xC7:  1 00e0.f7a4.5130         0 RCV Bridge-group Virtual Interface
```

Table 76 describes the significant fields shown in the displays.

Table 76 show interfaces irb Field Descriptions

Field	Description
Routed protocols on…	List of the routed protocols configured for the specified interface.
Bridged protocols on…	List of the bridged protocols configured for the specified interface.
Software MAC address filter on…	Table of software MAC address filter information for the specified interface.
Hash	Hash key/relative position in the keyed list for this MAC-address entry.
Len	Length of this entry to the beginning element of this hash chain.
Address	Canonical (Ethernet ordered) MAC address.
Matches	Number of received packets matched to this MAC address.
Act	Action to be taken when that address is looked up; choices are to receive or discard the packet.
Type	MAC address type.

show interfaces tokenring (IBM)

To display information about the Token Ring interface and the state of source-route bridging (SRB), use the **show interfaces tokenring** command in privileged EXEC mode.

show interfaces tokenring [*number*]

Syntax Description

number	(Optional) Interface number. If you do not provide a value, the command will display statistics for all Token Ring interfaces.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show interfaces tokenring** command:

```
Router# show interfaces tokenring

TokenRing 0 is up, line protocol is up
Hardware is 16/4 Token Ring, address is 5500.2000.dc27 (bia 0000.3000.072b)
   Internet address is  10.136.230.203, subnet mask is 255.255.255.0
   MTU 8136 bytes, BW 16000 Kb, DLY 630 usec, rely 255/255, load 1/255
   Encapsulation SNAP, loopback not set, keepalive set (10 sec)
   ARP type: SNAP, ARP Timeout 4:00:00
   Ring speed: 16 Mbps
   Single ring node, Source Route Bridge capable
   Group Address: 0x00000000, Functional Address: 0x60840000
   Last input 0:00:01, output 0:00:01, output hang never
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   Five minute input rate 0 bits/sec, 0 packets/sec
   Five minute output rate 0 bits/sec, 0 packets/sec
   16339 packets input, 1496515 bytes, 0 no buffer
        Received 9895 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     32648 packets output, 9738303 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets, 0 restarts
     5 transitions
```

Table 77 describes the significant fields shown in the display.

Table 77 show interfaces tokenring Field Descriptions

Field	Description
Token Ring is up	Interface is currently active and inserted into ring (up) or inactive and not inserted (down).
Token Ring is Reset	Hardware error has occurred. This is not in the sample output; it is informational only.
Token Ring is Initializing	Hardware is up, in the process of inserting the ring. This is not in the sample output; it is informational only.
Token Ring is Administratively Down	Hardware has been taken down by an administrator. This is not in the sample output; it is informational only. "Disabled" indicates the Cisco IOS software has received over 5000 errors in a keepalive interval, which is 10 seconds by default.
line protocol is up	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether keepalives are successful).
Hardware	Specifies the hardware type. "Hardware is ciscoBus Token Ring" indicates that the board is a CSC-C2CTR board. "Hardware is 16/4 Token Ring" indicates that the board is a CSC-1R, CSC-2R, or a CSC-R16M board. Also shows the address of the interface.
Internet address	Lists the Internet address followed by the subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether loopback is set.
keepalive	Indicates whether keepalives are set.
ARP type	Type of Address Resolution Protocol assigned.
Ring speed	Speed of Token Ring—4 or 16 Mbps.
Single ring node	Indicates whether a node is enabled to collect and use source RIF for routable Token Ring protocols.
Group Address	Interface's group address, if any. The group address is a multicast address; any number of interfaces on the ring may share the same group address. Each interface may have at most one group address.
Functional Address	Bit-significant group address. Each "on" bit represents a function performed by the station.

Table 77 show interfaces tokenring Field Descriptions (continued)

Field	Description
Last input	Number of hours, minutes, and seconds since the last packet was received by an interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because the data took too long to send. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
Five minute input rate, Five minute output rate	Average number of bits and packets sent per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
CRC	Cyclic redundancy check (CRC) generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or problems sending data on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station sending bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Number of times that the far-end sender has been running faster than the near-end router's receiver can handle. This may never be reported on some interfaces.

Table 77 show interfaces tokenring Field Descriptions (continued)

Field	Description
output errors	Sum of all errors that prevented the final sending of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Because a Token Ring cannot have collisions, this statistic is nonzero only if an unusual event occurred when frames were being queued or dequeued by the system software.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Should always be zero for Token Ring interfaces.
transitions	Number of times the ring made a transition from up to down, or vice versa. A large number of transitions indicates a problem with the ring or the interface.

show llc2

To display the Logical Link Control, type 2 (LLC2) connections active in the router, use the **show llc2** command in privileged EXEC mode.

show llc2 [**brief**]

Syntax Description

brief	(Optional) Displays information about the LLC2 connections that are active in the router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show llc2** command:

```
Router# show llc2

TokenRing0 DTE=1000.5A59.04F9,400022224444 SAP=04/04, State=NORMAL
V(S)=5, V(R)=5, Last N(R)=5, Local window=7, Remote Window=127
ack-max=3, n2=8, Next timer in 7768
xid-retry timer 0/60000 ack timer 0/1000
p timer 0/1000 idle timer 7768/10000
rej timer 0/3200 busy timer 0/9600
ack-delay timer 0/3200
CMNS Connections to:
Address 1000.5A59.04F9 via Ethernet2
Protocol is up
Interface type X25-DCE RESTARTS 0/1
Timers: T10 1 T11 1 T12 1 T13 1
```

The display includes a Connection-Mode Network Service (CMNS) addendum, indicating the LLC2 is running with CMNS. When LLC2 is not running with CMNS, the **show llc2** command does not display a CMNS addendum.

Table 78 describes the significant fields shown in the display.

Table 78 show llc2 Field Descriptions

Field	Description
TokenRing0	Name of interface on which the session is established.
DTE=1000.5A59.04F9, 400022224444	Address of the station to which the router is talking on this session. The address is the MAC address of the interface on which the connection is established, except when Local Acknowledgment or SDLC Logical Link Control (SDLLC) is used, in which case the address used by the Cisco IOS software is shown as in this example, following the DTE address and separated by a comma.
SAP=04/04	Other station's and the router's (remote or local) service access point (SAP) for this connection. The SAP is analogous to a "port number" on the router and allows for multiple sessions between the same two stations.

Table 78 show llc2 Field Descriptions (continued)

Field	Description
State=NORMAL	Current state of the LLC2 session. The values are: • ADM—Asynchronous Disconnect Mode. A connection is not established, and either end can begin one. • SETUP—Request to begin a connection has been sent to the remote station, and this station is waiting for a response to that request. • RESET—A previously open connection has been reset because of some error by this station, and this station is waiting for a response to that reset command. • D_CONN—This station has requested a normal, expected, end of communications with the remote, and is waiting for a response to that disconnect request. • ERROR—This station has detected an error in communications and has told the other station of this. This station is waiting for a reply to its posting of this error. • NORMAL—Connection between the two sides is fully established, and normal communication is occurring. • BUSY—Normal communication state exists, except busy conditions on this station make it such that this station cannot receive information frames from the other station at this time. • REJECT—Out-of-sequence frame has been detected on this station, and this station has requested that the other resend this information. • AWAIT—Normal communication exists, but this station has had a timer expire, and is trying to recover from it (usually by resending the frame that started the timer). • AWAIT_BUSY—A combination of the AWAIT and BUSY states. • AWAIT_REJ—A combination of the AWAIT and REJECT states.
V(S)=5	Sequence number of the next information frame this station will send.
V(R)=5	Sequence number of the next information frame this station expects to receive from the other station.
Last N(R)=5	Last sequence number of this station's sent frames acknowledged by the remote station.
Local window=7	Number of frames this station may send before requiring an acknowledgment from the remote station.
Remote Window=127	Number of frames this station can accept from the remote.
ack-max=3	Maximum number of packets to receive before sending an acknowledgment.
n2=8	Number of times to retry operations.
Next timer in 7768	Number of milliseconds before the next timer, for any reason, goes off.

Table 78 show llc2 Field Descriptions (continued)

Field	Description
xid-retry timer 0/60000	Number of milliseconds to wait for a reply to exchange identification (XID) frames before dropping a session. This timer value is in the form of next-time/time-between, where “next-time” is the next time, in milliseconds, that the timer will wake, and “time-between” is the time, in milliseconds, between each timer wakeup. A “next-time” of zero indicates that the timer is not enabled, and will never wake.
ack timer 0/1000	Number of milliseconds to wait before sending an acknowledgment. This timer value is in the form of next-time/time-between, where “next-time” is the next time, in milliseconds, that the timer will wake, and “time-between” is the time, in milliseconds, between each timer wakeup. A “next-time” of zero indicates that the timer is not enabled, and will never wake.
p timer 0/1000	Number of milliseconds to wait for a final response to a poll frame before resending the poll frame. This timer value is in the form of next-time/time-between, where “next-time” is the next time, in milliseconds, that the timer will wake, and “time-between” is the time, in milliseconds, between each timer wakeup. A “next-time” of zero indicates that the timer is not enabled, and will never wake.
idle timer 7768/10000	Number of milliseconds that can pass with no traffic before the LLC2 station sends a Receiver Ready frame. This timer value is in the form of next-time/time-between, where “next-time” is the next time, in milliseconds, that the timer will wake, and “time-between” is the time, in milliseconds, between each timer wakeup. A “next-time” of zero indicates that the timer is not enabled, and will never wake.
rej timer 0/3200	Number of milliseconds to wait for a resend of a rejected frame before sending a reject command to the remote station. This timer value is in the form of next-time/time-between, where “next-time” is the next time, in milliseconds, that the timer will wake, and “time-between” is the time, in milliseconds, between each timer wakeup. A “next-time” of zero indicates that the timer is not enabled, and will never wake.
busy timer 0/9600	Number of milliseconds to wait before repolling a busy remote station. This timer value is in the form of next-time/time-between, where “next-time” is the next time, in milliseconds, that the timer will wake, and “time-between” is the time, in milliseconds, between each timer wakeup. A “next-time” of zero indicates that the timer is not enabled, and will never wake.
ack-delay timer 0/3200	Number of milliseconds to allow incoming information frames to stay unacknowledged. This timer value is in the form of next-time/time-between, where “next-time” is the next time, in milliseconds, that the timer will wake, and “time-between” is the time, in milliseconds, between each timer wakeup. A “next-time” of zero indicates that the timer is not enabled, and will never wake.
CMNS Connections to:	List of values that affect the interface if CMNS is enabled.
Address 1000.5A59.04F9 via Ethernet2	MAC address of remote station.

Table 78 show llc2 Field Descriptions (continued)

Field	Description
Protocol is up	Up indicates that the LLC2 and X.25 protocols are in a state where incoming and outgoing Call Requests can be made on this LLC2 connection.
Interface type X25-DCE	One of X25-DCE, X25-DTE, or X25-DXE (both DTE and DCE).
RESTARTS 0/1	Restarts sent/received on this LLC2 connection.
Timers:	T10, T11, T12, T13 (or T20, T21, T22, T23 for DTE); these are Request packet timers. These are similar in function to X.25 parameters of the same name.

Related Commands

Command	Description
llc2 ack-delay-time	Sets the amount of time the Cisco IOS software waits for an acknowledgment before sending the next set of information frames.
llc2 ack-max	Controls the maximum amount of information frames the Cisco IOS software can receive before it must send an acknowledgment.
llc2 idle-time	Controls the frequency of polls during periods of idle time (no traffic).
llc2 local-window	Controls the maximum number of information frames the Cisco IOS software sends before it waits for an acknowledgment.
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.
llc2 tbusy-time	Controls the amount of time the Cisco IOS software waits until repolling a busy remote station.
llc2 tpf-time	Sets the amount of time the Cisco IOS software waits for a final response to a poll frame before resending the poll frame.
llc2 trej-time	Controls the amount of time the Cisco IOS software waits for a correct frame after sending a reject command to the remote LLC2 station.
llc2 xid-neg-val-time	Controls the frequency of XID transmissions by the Cisco IOS software.
llc2 xid-retry-time	Sets the amount of time the Cisco IOS software waits for a reply to XID frames before dropping the session.

show lnm bridge

Note Effective with release 12.3(4)T, the **show lnm bridge** command is no longer available in Cisco IOS 12.3T releases.

To display all currently configured bridges and all parameters that are related to the bridge as a whole, not to one of its interfaces, use the **show lnm bridge** command in privileged EXEC mode.

show lnm bridge

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show lnm bridge** command:

```
Router# show lnm bridge

Bridge 001-2-003, Ports 0000.3000.abc4, 0000.0028.abcd
Active Links: 0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000
Notification: 0 min, Threshold 00.10%
```

Table 79 describes the significant fields shown in the display.

Table 79 show lnm bridge Field Descriptions

Field	Description
Bridge 001-2-003	Ring and bridge numbers of this bridge.
Ports 0000.3000.abc4....	MAC addresses of the two interfaces of this bridge.
Active Links:	Any LAN Network Manager (LNM) stations that are connected to this bridge. An entry preceded by an asterisk is the controlling LNM.
Notification: 0 min	Current counter notification interval in minutes.
Threshold 00.10%	Current loss threshold (in percent) that will trigger a message to the LNM.

show lnm config

Note Effective with release 12.3(4)T, the **show lnm config** command is no longer available in Cisco IOS 12.3T releases.

To display the logical configuration of all bridges configured in a router, use the **show lnm config** command in privileged EXEC mode. This information is needed to configure an LAN Network Manager (LNM) Management Station to communicate with a router. This is especially important when the router is configured as a multiport bridge, thus employing the concept of a virtual ring.

show lnm config

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show lnm config** command for a simple two-port bridge:

```
Router# show lnm config

Bridge(s) currently configured:

           From     ring 001, address 0000.3000.abc4
           Across bridge 002
           To       ring 003, address 0000.0028.abcd
```

The following is sample output from the **show lnm config** command for a multiport bridge:

```
Router# show lnm config

Bridge(s) currently configured:

           From     ring 001, address 0000.0028.abc4
           Across bridge 001
           To       ring 008, address 4000.0028.abcd

           From     ring 002, address 0000.3000.abc4
           Across bridge 002
           To       ring 008, address 4000.3000.abcd
```

```
From     ring 003, address 0000.3000.5735
Across bridge 003
To       ring 008, address 4000.3000.5735
```

Table 80 describes the significant fields shown in the display.

Table 80 show lnm config Field Descriptions

Field	Description
From ring 001	Ring number of the first interface in the two-port bridge.
address 0000.3000.abc4	MAC address of the first interface in the two-port bridge.
Across bridge 002	Bridge number assigned to this bridge.
To ring 003	Ring number of the second interface in the two-port bridge.
address 0000.0028.abcd	MAC address of the second interface in the two-port bridge.

show lnm interface

Note Effective with release 12.3(4)T, the **show lnm interface** command is no longer available in Cisco IOS 12.3T releases.

To display all LAN Network Manager (LNM)-related information about a specific interface or all interfaces, use the **show lnm interface** command in privileged EXEC mode.

show lnm interface [*type number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.

Defaults

The *type* argument is not specified, information about all interface types is displayed.
If *number* is not specified, information about all interface numbers is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is for all types of interfaces, including Token Ring interfaces. If you want information specific to Token Ring, use the **show lnm ring** command.

Examples

The following is sample output from the **show lnm interface** command:

```
Router# show lnm interface

 nonisolating error counts
interface  ring   Active Monitor  SET   dec   lost   cong.  fc    freq.token
TokenRing1 0001*  1000.5a98.23a0  00200 00001 00000  00000  00000 0000000002

Notification flags: FE00, Ring Intensive: FFFF, Auto Intensive: FFFF
Active Servers: LRM LBS REM RPS CRS
Last NNIN:   never, from 0000.0000.0000.
Last Claim:  never, from 0000.0000.0000.
Last Purge:  never, from 0000.0000.0000.
Last Beacon: never, 'none' from 0000.0000.0000.
Last MonErr: never, 'none' from 0000.0000.0000.

                 isolating error counts
station         int ring   loc.   weight line   inter  burst  ac    abort
1000.5a98.23a0  T1  0001   0000   00 - N00000   00000  00000  00000 00000
1000.5a98.239e  T1  0001   0000   00 - N00000   00000  00000  00000 00000
1000.5a6f.bc15  T1  0001   0000   00 - N00000   00000  00000  00000 00000
0000.3000.abc4  T1  0001   0000   00 - N00000   00000  00000  00000 00000
1000.5a98.239f  T1  0001   0000   00 - N00000   00000  00000  00000 00000
```

Table 81 describes the significant fields shown in the display. See the **show lnm station** command for a description of the fields that follow after the “isolating error counts” line in the sample output.

Table 81 show lnm interface Field Descriptions

Field	Description
interface	Interface about which information was requested.
ring	Number assigned to that Token Ring. An asterisk following the ring number indicates that stations with nonzero error counters are present on that ring.
Active Monitor	Address of the station that is providing “Active Monitor” functions to the ring. The description of this server can be found in the *IBM Token Ring Architecture Reference Manual.*
SET	Current soft error reporting time for the ring in units of tens of milliseconds.
dec	Rate at which the various counters of nonisolating errors are being decreased. This number is in errors per 30 seconds.
lost, cong., fc, freq.token	Current values of the five nonisolating error counters specified in the 802.5 specification. These are Lost Frame errors, Receiver Congestion errors, FC errors, Frequency errors, and Token errors.
Notification flags:	Representation of which types of ring errors are being reported to LNM. The description of this number can be found in the *IBM Token Ring Architecture Reference Manual.*
Ring Intensive:	Representation of which specific ring error messages are being reported to LNM when in the “Ring Intensive” reporting mode. The description of this number can be found in the *IBM Token Ring Architecture Reference Manual.*
Auto Intensive:	Representation of which specific ring error messages are being reported to LNM when in the “Auto Intensive” reporting mode. The description of this number can be found in the *IBM Token Ring Architecture Reference Manual.*

Table 81 show lnm interface Field Descriptions (continued)

Field	Description
Active Servers:	A list of which servers are active on this Token Ring. The acronyms and their meanings are as follows: • CRS—Configuration Report Server • LRM—LAN Reporting Manager • LBS—LAN Bridge Server • REM—Ring Error Monitor • RPS—Ring Parameter Server The description of these servers can be found in the *IBM Token Ring Architecture Reference Manual*.
Last NNIN:	Time since the last "Neighbor Notification Incomplete" frame was received, and the station that sent this message.
Last Claim:	Time since the last "Claim Token" frame was received, and the station that sent this message.
Last Purge:	Time since the last "Purge Ring" frame was received, and the station that sent this message.
Last Beacon:	Time since the last "Beacon" frame was received, the type of the last beacon frame, and the station that sent this message.
Last Mon Err:	Time since the last "Report Active Monitor Error" frame was received, the type of the last monitor error frame, and the station that sent this message.

Related Commands

Command	Description
show lnm ring	Displays all LNM information about a specific Token Ring or all Token Rings.
show lnm station	Displays LNM-related information about a specific station or all known stations on all rings.

show lnm ring

Note Effective with release 12.3(4)T, the **show lnm ring** command is no longer available in Cisco IOS 12.3T releases.

To display all LAN Network Manager (LNM) information about a specific Token Ring or all Token Rings, use the **show lnm ring** command in privileged EXEC mode.

show lnm ring [*ring-number*]

Syntax Description

ring-number	(Optional) Number of a specific Token Ring. It can be a value in the range from 1 to 4095.

Defaults

If the *ring-number* argument is not specified, information about all Token Rings is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a specific interface is requested, it also displays a list of all active stations on that interface.

The output of this command is the same as the output of the **show lnm interface** command. See the **show lnm interface** and **show lnm station** commands for sample output and a description of the fields. The same information can be obtained by using the **show lnm interface** command, but instead of specifying an interface number, you specify a ring number as an argument.

Related Commands

Command	Description
show lnm interface	Displays all LNM-related information about a specific interface or all interfaces.
show lnm station	Displays LNM-related information about a specific station or all known stations on all rings.

show lnm station

Note Effective with release 12.3(4)T, the **show lnm station** command is no longer available in Cisco IOS 12.3T releases.

To display LAN Network Manager (LNM)-related information about a specific station or all known stations on all rings, use the **show lnm station** command in privileged EXEC mode

show lnm station [*address*]

Syntax Description

address	(Optional) Address of a specific LNM station.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a specific station is requested, it also displays a detailed list of that station’s current MAC-level parameters.

Examples

The following is sample output from the **show lnm station** command when a particular address has been specified:

```
Router# show lnm station 1000.5a6f.bc15

                                            isolating error counts
    station      int  ring  loc.   weight   line  inter burst   ac  abort
1000.5a6f.bc15    T1  0001  0000   00 - N   00000 00000 00000 00000 00000

Unique ID:  0000.0000.0000          NAUN: 0000.3000.abc4
Functional: C000.0000.0000         Group: C000.0000.0000
Physical Location:   00000        Enabled Classes:  0000
Allowed Priority:    00000        Address Modifier: 0000
Product ID:     00000000.00000000.00000000.00000000.0000
Ucode Level:    00000000.00000000.0000
Station Status: 00000000.0000
Last transmit status: 00
```

Table 82 describes the significant fields shown in the display.

Table 82 show lnm station Field Descriptions

Field	Description
station	MAC address of the given station on the Token Ring.
int	Interface used to reach the given station.
ring	Number of the Token Ring where the given station is located.
loc.	Physical location number of the given station.
weight	Weighted accumulation of the errors of the given station, and of its nearest active upstream neighbor (NAUN). The three possible letters and their meanings are as follows:[1] • N—not in a reported error condition. • P—in a "preweight" error condition. • W—in a "preweight" error condition.
isolating error counts	Current values of the five isolating error counters specified in the 802.5 specification. These are Line errors, Internal errors, Burst errors, AC errors, and Abort errors.
Values below this point will be zero unless the LNM has previously requested this information.	
Unique ID:	Uniquely assigned value for this station.
NAUN:	MAC address of this station's "upstream" neighbor.
Functional:	MAC-level functional address currently in use by this station.
Group:	MAC-level group address currently in use by this station.
Physical Location:	Number assigned to this station as its "Physical Location" identifier.
Enabled Classes:	Functional classes that the station is allowed to send.
Allowed Priority:	Maximum access priority that the station may use when sending onto the Token Ring.
Address Modifier:	Reserved field.
Product ID:	Encoded 18-byte string used to identify what hardware and software combination is running on this station.
Ucode Level:	10-byte extended binary coded decimal interchange code (EBCDIC) string indicating the microcode level of the station.
Station Status:	Implementation-dependent vector that is not specified anywhere.
Last transmit status:	Contains the strip status of the last "Report Transmit Forward" MAC frame forwarded by this interface.

[1] The description of these error conditions can be found in the *IBM Architecture Reference Manual*.

show local-ack

To display the current state of any current local acknowledgment for both Logical Link Control, type 2 (LLC2) and SDLC Logical Link Control (SDLLC) connections, and for any configured pass-through rings, use the **show local-ack** command in privileged EXEC mode.

show local-ack

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show local-ack** command:

```
Router# show local-ack

local 1000.5a59.04f9, lsap 04, remote 4000.2222.4444, dsap 04
llc2 = 1798136, local ack state = connected
Passthrough Rings: 4 7
```

Table 83 describes the significant fields shown in the display.

Table 83 show local-ack Field Descriptions

Field	Description
local	MAC address of the local Token Ring station with which the route has the LLC2 session.
lsap	Local service access point (LSAP) value of the Token Ring station with which the router has the LLC2 session.
remote	MAC address of the remote Token Ring on whose behalf the router is providing acknowledgments. The remote Token Ring station is separated from the device via the TCP backbone.
dsap	Destination service access point (SAP) value of the Token Ring station on whose behalf the router is providing acknowledgments.
llc2	Pointer to an internal data structure used by the manufacturer for debugging.

Table 83 show local-ack Field Descriptions (continued)

Field	Description
local ack state	State of the local acknowledgment for both LLC2 and Synchronous Data Link Control (SDLC) connections. The states are as follows: • disconnected—No session between the two end nodes. • connected—Full data transfer between the two. • awaiting connect—Cisco IOS software is waiting for the other end to confirm a session establishment with the remote host.
Passthrough Rings	Ring numbers of the virtual rings that have been defined as pass-throughs using the **source-bridge passthrough** command. If a ring is not a pass-through, it is locally terminated.

show ncia circuits

To display the state of all circuits involving this MAC address as a source and destination, use the **show ncia circuits** command in privileged EXEC mode.

show ncia circuits [*id-number*]

Syntax Description

id-number	(Optional) Number assigned to identify the circuit. If no ID number is specified, the command lists information for all circuits.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ncia client** command to list the active circuits by circuit ID number, then use a specific circuit ID number in the **show ncia circuits** command.

Examples

The following is sample output from the **show ncia circuits** command:

```
Router# show ncia circuits

IP              State                   ID         Mac              SAP CW  GP
10.2.20.125     START_DL_RCVD   (Client)10000000   1000.0000.0001   4   0   0
                                (Server)163D04     4000.1060.1000   4   10  0
```

Table 84 describes the significant fields shown in the display.

Table 84 show ncia circuits Field Descriptions

Field	Description
IP	IP address of the client.
State	Communication state of the circuit.
ID	Circuit ID number. The server circuit ID is used by the server to identify a circuit. Use this ID in the **show ncia circuits** command. The client circuit ID is for information only.
Mac	Client MAC address is the MAC address used by the client; server MAC address is the MAC address used by the host. In a downstream physical unit (DSPU) configuration, the server MAC address is the one defined in the **dspu ncia** command as *server-virtual-mac-address*.

Table 84 show ncia circuits Field Descriptions (continued)

Field	Description
SAP	Local address (LSAP), specified in the **dspu enable-pu** command.
CW	Current window, the number of packets that can be increased or decreased for each Increment or Decrement operation.
GP	Granted packets, the number of packets the client or server is permitted to send to the other.

show ncia client

To display the status of the native client interface architecture (NCIA) client, use the **show ncia client** command in user EXEC or privileged EXEC mode.

show ncia client [**sap-list**] [*ip-address*]

Syntax Description

sap-list	(Optional) Display the service access points (SAP) supported by the client. If the **sap-list** option is not specified, the command does not display service access point (SAP) list information.
ip-address	(Optional) Client IP address. If no IP address is specified, the command lists information for all clients.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ncia server** command to list the active clients by IP address, then use a specific IP address in the **show ncia client** command.

Examples

The following are sample outputs from the **show ncia client** command:

```
Router# show ncia client

IP              State  MacAddr         Flags   Num SAP    PktRxd  PktTxd  Drop
10.2.20.123         4  1000.0000.0011  0x0800     3           27      36     0
    Circuit[1] : 791F8C
10.2.20.126         4  1000.0000.0011  0x0800     1           28      58     0
    Circuit[2] : 793500

Router# show ncia client sap-list 10.2.20.123

IP              Num SAPS  Sap List
10.2.20.123        3      4 8 c
```

Table 85 describes the significant fields shown in the display.

Table 85 show ncia client Field Descriptions

Field	Description
IP	IP address of the client.
State	Communication state of the client. Values are: • 0 CLOSED—Read and write pipe closed • 1 OPEN_WAIT—Active open. • 2 CAP_WAIT—Waiting for a cap exchange request. • 3 CAP_NEG—Waiting for a cap exchange req/rsp. • 4 OPENED—Both pipes opened. • 5 BUSY—WAN transport is congested. • 6 CLOSE_WAIT—Close connection. • 7 SHUTDOWN_PENDING—TCP, HOST, or router shutdown.
MacAddr	MAC address of the client.
Flags	Current operational status of the client. Values are: • 0x0100—Client is configured. • 0x0200—Client is registered (a client connects to the server to register itself, and then disconnects). • 0x0800—Client is active.
Num SAP	Number of SAPs supported by this client; 0 indicates that this client supports all SAPs.
PktRxd	Number of packets sent downstream from the server toward a client workstation.
PktTxd	Number of packets the server received from a downstream client workstation.
Drop	Number of packets that should have been sent to a downstream client, but were dropped by the server because the TCP connection has failed. Normally, no packets should be dropped.
Circuit[*x*]	Bracketed decimal indicates the order of the circuit in the list. The hexadecimal circuit ID is used by the server to identify a circuit. The circuit ID can be used to query circuit status in the **show ncia circuits** command.
SAP List	List of SAPs supported by this client. A client can specify a maximum of 16 SAPs. If the "Num SAP" field is 0, no SAPs are displayed in this field.

show ncia server

To display the state of the native client interface architecture (NCIA) server, use the **show ncia server** command in user EXEC or privileged EXEC mode.

show ncia server [*server-number*]

Syntax Description

server-number	(Optional) NCIA server number. If no server number is specified, the command lists information for all servers.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ncia server** command:

```
Router# show ncia server

NCIA Server [1]:
    IP address: 10.2.20.4
    Server Virtual MAC address: 4000.3174.0001
    Starting MAC address: 1000.0000.0001
    MAC address range: 128
    Flags: 0x02
    Number of MAC addresses being used: 0
```

show netbios-cache

To display a list of NetBIOS cache entries, use the **show netbios-cache** command in privileged EXEC mode.

show netbios cache

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show netbios-cache** command:

```
Router# show netbios-cache

  HW Addr          Name            How       Idle      NetBIOS Packet Savings
1000.5a89.449a     IC6W06_B        TR1       6         0
1000.5a8b.14e5     IC_9Q07A        TR1       2         0
1000.5a25.1b12     IC9Q19_A        TR1       7         0
1000.5a25.1b12     IC9Q19_A        TR1       10        0
1000.5a8c.7bb1     BKELSA1         TR1       4         0
1000.5a8b.6c7c     ICELSB1         TR1       -         0
1000.5a31.df39     ICASC_01        TR1       -         0
1000.5ada.47af     BKELSA2         TR1       10        0
1000.5a8f.018a     ICELSC1         TR1       1         0
```

Table 86 describes the significant fields shown in the display.

Table 86 show netbios-cache Field Descriptions

Field	Description
HW Addr	MAC address mapped to the NetBIOS name in this entry.
Name	NetBIOS name mapped to the MAC address in this entry.
How	Interface through which this information was learned.
Idle	Period of time (in seconds) since this entry was last accessed. A hyphen in this column indicates it is a static entry in the NetBIOS name cache.
NetBIOS Packet Savings	Number of packets to which local replies were made (thus preventing sending of these packets over the network).

Related Commands

Command	Description
netbios name-cache	Defines a static NetBIOS name cache entry, tying the server with the name netbios-name to the mac-address, and specifying that the server is accessible either locally through the interface-name specified, or remotely through the ring-group group-number specified.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.

show qllc

To display the current state of any Qualified Logical Link Control (QLLC) connections, use the **show qllc** command in privileged EXEC mode.

show qllc

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show qllc** command.

```
Router# show qllc

QLLC Connections:
Serial2: 1000.5a35.3a4f->1000.5a59.04f9. SAPs 4 4. Rings Src 200, Tgt 100.
State Connect
Remote DTE 1002. QLLC Protocol State NORMAL lci 1 (PVC)
```

In the display, the first two lines of the **show qllc** command show that there is a QLLC session between a Token Ring device and an X.25 remote device. The X.25 device has a virtual MAC address of 100.5a35.3a4f with a service access point (SAP) of 04. It is using a permanent virtual circuit (PVC) with logical channel number 1. The Token Ring device has a MAC address of 1000.5a59.04f9 with a service access point (SAP) of 04. The state of the QLLC session is CONNECTED.

Table 87 describes the fields shown in the display.

Table 87 show qllc Field Descriptions

Field	Description
Serial2	Serial interface for the X.25 link.
1000.5a35.3a4f	Virtual MAC address for the X.25 attached device.
1000.5a59.04f9	MAC address of the Token Ring attached device with which the X.25 attached device is communicating. This device might be on a local Token Ring or attached via source-route bridging (SRB) or remote source-route bridging (RSRB).
SAPs 4 4	Source SAP value at the virtual MAC address and destination SAP value at the Token Ring station.
Rings Src 200	Ring number for the source virtual ring defined by the **qllc srb** command.

Table 87 show qllc Field Descriptions (continued)

Field	Description
Tgt 100	Ring number for the target virtual ring defined by the **source-bridge ring-group** command.
State	State of the QLLC-Logical Link Control, type 2 (LLC2) conversion. This can be any of the following: • DISCONNECT—No connection exists. • NET DISC WAIT—X.25 device is disconnecting. The QLLC conversion is waiting for the Token Ring device to disconnect. • QLLC DISC WAIT—The Token Ring device is disconnecting. The QLLC conversion is waiting for the X.25 device to disconnect. • QLLC PRI WAIT—Connection is being established. The Token Ring device is ready to complete the connection, and the Cisco IOS software is establishing the QLLC connection with the X.25 device. • NET CONTACT REPLY WAIT—Remote X.25 device is a front-end processor (FEP), and has made contact with the Cisco IOS software. The software is attempting to reach Token Ring device. • QLLC SEC WAIT—Connection is being established. • NET UP WAIT—Connection is being established. QLLC connection to X.25 device has been established; awaiting completion on the connection to the Token Ring attached device. • Connect—Connections from the software to X.25 and Token Ring devices are established. Data can flow end to end.
Remote DTE 1002	X.121 address of X.25 connected device.
QLLC Protocol State	State of the QLLC protocol between the software and the X.25 attached device. These states are different from the state of the underlying X.25 virtual circuit. Values are as follows: • ADM—Asynchronous Disconnected Mode. • SETUP—Cisco IOS software has initiated QLLC connection, awaiting confirmation from the X.25 device. • RESET—Cisco IOS software has initiated QLLC reset, awaiting confirmation from the X.25 device. • DISCONNECTING—Cisco IOS software has initiated QLLC disconnect, awaiting confirmation from the X.25 device. • NORMAL—QLLC connection has been completed. Systems Network Architecture (SNA) data can be sent and received.
lci 1 (PVC)	Logical channel number used on the X.25 interface.

show rif

To display the current contents of the Routing Information Field (RIF) cache, use the **show rif** command in privileged EXEC mode.

show rif

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show rif** command:

```
Router# show rif

Codes: * interface, - static, + remote
Hardware Addr  How   Idle (min)  Routing Information Field
5C02.0001.4322 rg5           -   0630.0053.00B0
5A00.0000.2333 TR0           3   08B0.0101.2201.0FF0
5B01.0000.4444 -             -   -
0000.1403.4800 TR1           0   -
0000.2805.4C00 TR0           *   -
0000.2807.4C00 TR1           *   -
0000.28A8.4800 TR0           0   -
0077.2201.0001 rg5          10   0830.0052.2201.0FF0
```

In the display, entries marked with an asterisk (*) are the router's interface addresses. Entries marked with a dash (-) are static entries. Entries with a number denote cached entries. If the RIF timeout is set to something other than the default of 15 minutes, the timeout is displayed at the top of the display. Table 88 describes the significant fields shown in the display.

Table 88 show rif Field Descriptions

Field	Description
Hardware Addr	Lists the MAC-level addresses.
How	Describes how the RIF has been learned. Values are ring group (rg) or interface (TR).
Idle (min)	Indicates how long, in minutes, since the last response was received directly from this node.
Routing Information Field	Lists the RIF.

Related Commands

Command	Description
multiring	Enables collection and use of RIF information.

show sdllc local-ack

To display the current state of any current local acknowledgment connections, and any configured pass-through rings, use the **show sdllc local-ack** command in privileged EXEC mode.

show sdllc local-ack

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show sdllc local-ack** command:

```
Router# show sdllc local-ack

local 1000.5a59.04f9, lsap 04, remote 4000.2222.4444, dsap 04
llc2 = 1798136, local act state = connected
Passthrough Rings: 4 7
```

In the display, the first two lines of the **show sdllc local-ack** command show that there is a local acknowledgment session between two Token Ring devices. The device on the local ring has a MAC address of 1000.5a59.04f9 with a service access point (SAP) of 04. The remote device has a MAC address of 4000.2222.4444 with a SAP of 04. The state of the local acknowledgment session is connected.

The pass-through rings display is independent of the rest of the **show sdllc local-ack** command. The pass-through rings display indicates that there are two rings, 4 and 7, configured for pass-through. This means that stations on these rings will not have their sessions locally acknowledged but will instead have their acknowledgments end-to-end.

Table 89 describes the significant fields shown in the display.

Table 89 show sdllc local-ack Field Descriptions

Field	Description
local	MAC address of the local Token Ring station with which the router has the Logical Link Control, type 2 (LLC2) session.
lsap	Local SAP value of the Token Ring station with which the router has the LLC2 session.

Table 89 show sdllc local-ack Field Descriptions (continued)

Field	Description
remote	MAC address of the remote Token Ring station on whose behalf the router is providing acknowledgments. The remote Token Ring station is separated from the router via the TCP backbone.
dsap	Destination SAP value of the remote Token Ring station on whose behalf the router is providing acknowledgments.
llc2	Pointer to an internal data structure used by technical support staff for debugging.
local ack state	Current state. Values are as follows: • disconnected—No session between the two end hosts. • connected—Full data transfer between the two end hosts. • awaiting connect—This router is waiting for the other end to confirm a session establishment with the remote host.
Passthrough Rings	Ring number of the start ring and destination ring for the two IBM machines when you do not have local acknowledgment for LLC2 configured for your routers using remote source-route bridging (RSRB).

show sna

To display the status of the Systems Network Architecture (SNA) Service Point feature, use the **show sna** command in privileged EXEC mode.

show sna [**pu** *host-name* [**all**]]

Syntax Description

pu	(Optional) Name of a host defined in an **sna host** command.
host-name	(Optional) Name of a host defined in an **sna host** command.
all	(Optional) Displays detailed status.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show sna** command. It shows a summary of the Systems Network Architecture (SNA) features status.

```
Router# show sna

sna host HOST_NAMEA TokenRing1 PU STATUS active
FRAMES RECEIVED 00450 FRAMES SENT 00010
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
```

The following is sample output from the **show sna** command with the **pu** keyword:

```
Router# show sna pu putest

sna host PUTEST TokenRing1 PU STATUS active
RMAC 400000000004 RSAP 04 LSAP 04
XID 05d00001 RETRIES 255 RETRY_TIMEOUT 30
WINDOW 7 MAXIFRAME 1472
FRAMES RECEIVED 0450 FRAMES SENT 0010
LUs USED BY DSPU nnn LUs ACTIVE nnn
LUs USED BY API nnn LUs ACTIVE nnn
LUs ACTIVATED BY HOST BUT NOT USED nnn
```

Because the **all** keyword refers to logical unit (LU)s under the physical unit (PU), this has no significance for the service point host.

show snasw class-of-service

To display the class of service (CoS) definitions predefined to Switching Services (SNASw), use the **show snasw class-of-service** command in privileged EXEC mode.

show snasw class-of-service [**brief** | **detail**]

Syntax Description

brief	(Optional) Indicates a one-line display per displayed resource. The brief version displays CoS name, transmission priority, and number of node and Transmission Group (TG) rows.
detail	(Optional) Indicates a detailed, multiline display of all fields returned for CoS display.

Command Modes

Privileged EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is a truncated example of the **show snasw class-of-service** command:

```
Router# show snasw class-of-service

Number of class of service definitions 7

      SNA Classes of Service
        Name    Trans. Pri.  Node Rows  TG Rows
      --------  -----------  ---------  -------
   1> #BATCH    Low               8         8
   2> #INTER    High              8         8
   3> CPSVCMG   Network           8         8
   4> #BATCHSC  Low               8         8
   5> #CONNECT  Medium            8         8
   6> #INTERSC  High              8         8
   7> SNASVCMG  Network           8         8

Router# show snasw class-of-service detail

Number of class of service definitions 7

1>
Class of service name                                 #BATCH
Transmission priority                                 Low
Number of node rows                                   8
Number of TG rows                                     8
```

```
1.1>Node row weight                                   5
Congestion min                                        No
Congestion max                                        No
Route additional resistance min                       0
Route additional resistance max                       31
```

Related Commands

Command	Description
show snasw mode	Displays the SNASw modes.

show snasw connection-network

To display the connection networks (virtual nodes) defined to the local node, use the **show snasw connection-network** command in privileged EXEC.

show snasw connection-network [**brief** | **detail**]

Syntax Description

brief	(Optional) Indicates a one-line display per resource. The brief version displays the connection network name, the number of attached ports, and the port names in the connection network.
detail	(Optional) Indicates a detailed, multiline display of all fields returned for connection-network display.

Command Modes

Privileged EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output form the **show snasw connection-network** command:

```
Router# show snasw connection-network

Connection network definitions 1

      SNA Connection Networks
        Resource Name    Attached Ports            Port Name(s)
      -----------------  --------------  --------------------------------
   1> CISCO.VN                     1     TR0

Router# show snasw connection-network detail

Connection network definitions 1

1>
Connection network name                            CISCO.VN
Effective capacity                                 16 Mbps
Cost per connect time                              0
Cost per byte                                      0
Propagation delay                                  384 microseconds
User defined parameter 1                           128
User defined parameter 2                           128
User defined parameter 3                           128
```

```
Security                                            Nonsecure

1.1>Port name                                       TR0
```

Related Commands

Command	Description
show snasw link	Displays the Switching Services (SNASw) link objects.

show snasw directory

To display the Switching Services (SNASw) directory entries, use the **show snasw directory** command in EXEC mode.

show snasw directory [**name** *resource-name-filter*] [**brief** | **detail**]

Syntax Description

name *resource-name-filter*	(Optional) Indicates the fully qualified name of the resource (1 to 17 characters). Only resource names that match the specified name are displayed.
brief	(Optional) Indicates a one-line display for each resource. The brief version displays resource name, owning control point (CP) name, network node server name, and entry type.
detail	(Optional) Indicates a detailed, multiline display of all fields returned for the directory display.

Command Modes

EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw directory** and **show snasw directory detail** commands:

```
Router# show snasw directory

Total Directory Entries 2

      SNA Directory Entries
        Resource Name     Owning CP Name       NN Server      Entry Type
      -----------------  -----------------  -----------------  ----------
   1> CISCO.A           CISCO.A            CISCO.B            Registry
   2> CISCO.B           CISCO.B            CISCO.B            Home

Router# show snasw directory detail

Total Directory Entries 2

1>
Resource name                                     CISCO.A
NN server name                                    CISCO.B
```

```
Entry type                                          Registry
Location                                            Local to this domain
Resource owner's CP name                            CISCO.A
Apparent resource owner's CP name
Wildcard                                            Explicit

2>
Resource name                                       CISCO.B
NN server name                                      CISCO.B
Entry type                                          Home
Location                                            Local to this node
Resource owner's CP name                            CISCO.B
Apparent resource owner's CP name
Wildcard                                            Explicit
```

Related Commands

Command	Description
snasw location	Configures the location of a resource.

show snasw dlctrace

To display the captured Data-link control (DLC) trace information to the console, use the **show snasw dlctrace** command.

show snasw dlctrace [**id** *recordid*] [**all** | **last** *number-records* | **next** *number-records*] [**brief** | **detail**] [**filter** *filter-string*]

Syntax Description

id *recordid*	(Optional) Indicates that the 1 to 999,999 trace record identifier. Only the frame ID that matches the record specified is displayed.
all	(Optional) Indicates that all records in the dlctrace buffer are displayed.
last *number-records*	(Optional) Indicates that the last *x* frames before the record identified in the ID operand (or before the last record in the trace if the ID operand is not coded) are displayed.
next *number-records*	(Optional) Indicates that the next frames after the record identified in the ID operand (or from the beginning of the trace if the ID operand is not coded) are displayed.
brief	(Optional) Indicates a one-line display per trace entry describing the type of frame traced.
detail	(Optional) Indicates a detailed, multiline display of the frame that displays the brief information plus a hexadecimal dump of the entire frame.
filter *filter-string*	(Optional) Indicates that a string follows against which the formatted trace output is filtered. Only frames that contain the filter string are displayed.

Command Modes

EXEC

Defaults

If **id** *recordid* is specified, **next** is the default parameter; if not, **last** is the default parameter.

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw dlctrace** command:

```
Router# show snasw dlctrace id 2467 next 20
DLC Trace Output

2467   LINKT    In  sz:43   HPR +Rsp IPM     slctd nws:0007
2468   LINKT    In  sz:212  HPR +Rsp IPM     slctd nws:0007
```

```
2469   LINKT    In  sz:52   HPR CP CAPABILITIES
2470   LINKT    In  sz:221  HPR CP CAPABILITIES
2471   LINKT    Out sz:282  HPR MIS
2472   LINKT    Out sz:43   HPR +Rsp IPM     slctd nws:0007
2473   LINKT    In  sz:154  HPR Rq Bind CISCO.B CISCO.A
2474   LINKT    In  sz:323  HPR Rq Bind CISCO.B CISCO.A
2475   LINKT    Out sz:361  HPR MIS
2476   LINKT    Out sz:132  HPR +Rsp Bind
2477   LINKT    In  sz:102  HPR fmh5 CP CAPABILITIES
2478   LINKT    In  sz:271  HPR fmh5 CP CAPABILITIES
2479   LINKT    Out sz:282  HPR MIS
2480   LINKT    Out sz:43   HPR +Rsp IPM     slctd nws:0007
2481   LINKT    Out sz:291  HPR MIS
2482   LINKT    Out sz:52   HPR CP CAPABILITIES
2483   LINKT    In  sz:43   HPR +Rsp IPM     slctd nws:0007
2484   LINKT    In  sz:212  HPR +Rsp IPM     slctd nws:0007
2485   LINKT    Out sz:45   HPR
2486   LINKT    In  sz:45   HPR

Router# show snasw dlctrace id 2486 detail

DLC Trace Output

2486   LINKT    In  sz:45   HPR
 10:08:36.14, 14 March 1993
   0000 C60080FF 00000000 00010000 00000400  *F...............*
   0010 0A000000 00000001 7E050E00 00000000  *........=.......*
   0020 01000001 7E000000 00000000 00        *....=........   *
```

Related Commands

Command	Description
snasw dlctrace	Traces frames arriving and leaving SNASw.
snasw dlcfilter	Filters frames being captured.

show snasw dlus

To display the Switching Services (SNASw) Dependent Logical Unit Server (DLUS) objects, use the **show snasw dlus** command.

show snasw dlus [**brief** | **detail**]

Syntax Description

brief	(Optional) Indicates that one line per DLUS is displayed. The brief version includes the DLUS name, state (active or inactive), port name, cpname, node type, and number of active physical unit (PU)s on the DLUS.
detail	(Optional) Indicates the detailed, multiline display that shows all fields returned for DLUS displayed.

Command Modes

EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw dlus** command:

```
Router# show snasw dlus

Number of Dependent LU Servers2
SNA Dependent LU Servers
          DLUS Name      Default?  Backup?  Pipe State         PUs
      -----------------  --------  -------  ----------------  -------
   1> NETA.SJMVS3        Yes       No       Active               1
   2> NETA.SJMVS4        No        Yes      Inactive             0

Router# show snas dlus detail

Number of Dependent LU Servers2

1>
DLUS name                                          NETA.SJMVS3
Is this the default DLUS                           Yes
Is this the backup default DLUS                    No
Pipe state                                         Active
Number of active PUs                               1
DLUS pipe statistics:
  REQACTPUs sent                                   1
  REQACTPU responses received                      1
```

```
ACTPUs received                                 1
ACTPU responses sent                            1
DACTPUs received                                0
DACTPU responses sent                           0
REQDACTPUs sent                                 0
REQDACTPU responses received                    0
ACTLUs received                                 16
ACTLU responses sent                            1
DACTLUs received                                0
DACTLU responses sent                           0
SSCP-PU MUs sent                                0
SSCP-PU MUs received                            0
SSCP-LU MUs sent                                19
SSCP-LU MUs received                            3
```

Related Commands

Command	Description
snasw dlus	Specifies parameters related to DLUR/DLUS functionality.

show snasw ipstrace

To display the interprocess signal (IS) trace on the router console, use the **show snasw ipstrace** command.

> **show snasw ipstrace** [**id** *recordid*] [**all** | **next** *number-records* | **last** *number-records*] [**filter** *filter-string*]

Syntax Description

id *recordid*	(Optional) Indicates that the 1 to 999,999 trace record identifier. Only the frame ID that matches the record specified is displayed.
all	(Optional) Specifies that all records are displayed
next *number-records*	(Optional) Displays records from beginning or following record IS.
last *number-records*	(Optional) Indicates that the last *x* frames before the record identified in the ID operand (or before the last record in the trace if the ID operand is not coded) are displayed.
filter *filter-string*	(Optional) Indicates that a string follows against which the formatted trace output is filtered. Only frames that contain the filter-string are displayed.

Command Modes

EXEC

Defaults

No default behaviors or values

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw ipstrace** command:

```
Router# show snasw ipstrace

423452 : DLC_UI_MU : PC(2350000) -> DLC(2300000) Q 2
 03/14/1993 10:11:36.18
    00000000 00000000 61BB3F50 00800000 00000000 00000000 00000000 00000000
    000000FF 000000FF 00000000 00000000 05010000 000000FF 50130000 002D00D2
    02340000 03000000 00000000 61BB3FB0 00140050 0000017E 000100FF 00000000
    00000000 01000000 00000000 00000000 0000017E 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00C6C600 80FF0000 00000001 00000000
    04000A00 00000000 00017E05 0E000000 01000100 00017E00 00000000 00000000
```

Related Commands

Command	Description
snasw ipstrace	Sets up a trace buffer and begins tracing IPS trace elements
snasw ipsfilter	Filters interprocess signal trace elements being traced using the **snasw ipstrace** or **debug snasw ips** commands.

show snasw link

To display the Switching Services (SNASw) link objects, use the **show snasw link** command.

show snasw link [**brief** | **detail**] [**active** | **not-active**] [**cpname** *cp-name-filter*] [**name** *linknamefilter*] [**port** *port-name-filter*] [**rmac** *mac-filter*] [**xid** *xid-filter*]

Syntax Description

brief	(Optional) Indicates that one line per link is displayed. The brief version includes the link name, state (active or inactive), port name, adjacent control point (CP) name, node type information, number of sessions, and HPR support. The number of sessions does not include HPR sessions.
detail	(Optional) Indicates that a detailed, multiline display that shows all fields returned for links are displayed.
active	(Optional) Displays active snasw links.
not-active	(Optional) Displays snasw links that are not active.
cpname *cp-name-filter*	(Optional) Indicates a fully qualified cpname (1 to 17 characters). Only links with CP names (as known to the router) that match the specified cpname are displayed.
name *linknamefilter*	(Optional) Indicates the name of the link to be displayed. Only links matching this name are displayed.
port *port-name-filter*	(Optional) Indicates the handle "naming" for the specific port (1 to 8 characters). All links associated with a port matching the filter are displayed.
rmac *mac-filter*	(Optional) Indicates a 48-bit MAC address in hexadecimal form. Only links with a remote MAC address matching the MAC address specified are displayed.
xid *xid-filter*	(Optional) Indicates a 4-byte exchange identification (XID) (idnum/idblk) specified in hexadecimal form. Only links matching the configured XID are displayed.

Command Modes

EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show snasw link** command:

```
Router# show snasw link

Number of links 1

      SNA Links                                                          HPR
      Link Name   State    Port Name Adjacent CP Name  Node Type     Sess  Sup
      ---------  -------   --------- ----------------  ------------  ----  ---
   1> LINKT      Active    TR0       CISCO.B           Network Node     0  Yes

Router# show snasw link detail

Number of links 1

1>
Link name                                          LINKT
Port name                                          TR0
DLC type                                           Token-ring
Destination DLC Address                            000B.1AA4.9280.04
Link state                                         Active
Link substate                                      Active
Number of active sessions traversing link          0
Adjacent Node Id                                   X'FFF00000'
Max send frame data (BTU) size                     4400
Adjacent node CP name                              CISCO.B
Adjacent node type                                 Network Node
CP-CP session support                              Yes
Link station role                                  Secondary
Transmission group number                          21
Limited resource                                   No
Effective capacity                                 16 Mbps
Cost per connect time                              0
Cost per byte                                      0
Propagation delay                                  384 microseconds
User defined parameter 1                           128
User defined parameter 2                           128
User defined parameter 3                           128
Security                                           Nonsecure
Routing Information Field
Primary DLUS Name
Backup DLUS Name
Downstream PU Name
Retry link station                                 Yes
Dynamic link station                               No
Adjacent node is a migration node                  No
Link station statistics:
  Total XID bytes sent                             466
  Total XID bytes received                         344
  Total XID frames sent                            5
  Total XID frames received                        4
  Total data bytes sent                            752
  Total data bytes received                        685
  Total data frames sent                           8
  Total data frames received                       9
  Total session control frames sent                0
  Total session control frames received            0
  Total number of successful XID exchanges         1
  Total number of unsuccessful XID exchanges       0
```

Related Commands

Command	Description
snasw link	Configures upstream links.

show snasw lu

To display the SNA Switching Services (SNASw) dependent logical units (LU)s, use the **show snasw lu** command in user EXEC or privileged EXEC mode.

show snasw lu [**brief** | **detail**] [**name** *lu-name*] [**pu** *pu-name*]

Syntax Description

brief	(Optional) Indicates that one line per LU is displayed. The brief display includes LU name, physical unit (PU) name, dependent logical unit server (DLUS) name, and primary logical unit (PLU) name.
detail	(Optional) Indicates that a detailed, multiline display that shows all fields returned for the link is displayed.
name *lu-name*	(Optional) Indicates an LU name to filter. Only LUs matching the specified name are displayed.
pu *pu-name*	(Optional) Indicates a PU name to filter. Only LUs for the specified name are displayed.

Defaults

The default display is brief.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following sample display is from the **show snasw lu** command:

```
Router# show snasw lu

Number of DLUR LUs 49

      SNA DLUR LUs
      LU Name   PU Name   DLUS Name          PLU Name
      --------  --------  -----------------  -----------------
   1> CWBC0601  CWBC06    NETA.MVSD
   2> CWBC0602  CWBC06    NETA.MVSD
```

The following is sample output from the **show snasw lu detail** command:

```
Router# show snasw lu detail

Number of DLUR LUs 49

1>
LU name                                                   CWBC0601
LU status                                                 Active
SLU status                                                No session
PU name                                                   CWBC06
DLUS name                                                 NETA.MVSD
Primary LU name
LU location                                               Downstream
LU  FSM history                                           (00,00)->(01,01)->(02,0E)->(03,03)->04
SLU FSM history                                           (00,10)->00
```

Table 90 describes the significant fields shown in the output.

Table 90 show snasw lu Field Descriptions

Field	Description
LU name	The name of the LU.
PU name	The physical unit this LU is defined to.
DLUS name	Dependent LU server for the PU and LU.
PLU name	The name of the host LU that this LU is in session with. If the LU is not in session, no PLU name will be displayed.
LU status	The state of the system services control points (SSCP)-LU session. States are: • Active—The SSCP-LU is active and available for LU-LU sessions. • Pend ACTLU rsp—The SSCP-LU session is pending activation. • Pend DACTLU rsp—The SSCP-LU session is pending deactivation. • Reset—The SSCP-LU session is not active.
SLU status	The current state of the LU-LU session. States are: • In Session—The LU-LU session is active. • No Session—The LU-LU session is not active. • Pend BIND rsp—The LU-LU session is pending activation. • Pend UNBIND rsp—The LU-LU session is pending deactivation.
Primary LU name	The name of the host LU that this LU is in session with. If the LU is not in session, no PLU name will be displayed.
LU location: Downstream	Indicates that the LU resides on a node downstream from this SNASw node.
LU FSM history	A history of the states and actions of the SSCP-LU session for diagnostic use by Cisco technical support.
SLU FSM history	A history of the states and actions of the LU-LU session for diagnostic use by Cisco technical support.

Related Commands

Command	Description
show snasw dlus	Displays the SNASw DLUS objects.
show snasw pu	Displays the SNASw PUs that require or request SSCP-PU services.

show snasw mode

To display the Switching Services (SNASw) modes, use the **show snasw mode** command.

show snasw mode

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Defaults

No default behaviors or values

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw mode** command:

```
Router# show snasw mode

Number of modes 8

      SNA Modes
        Name     Associated COS
      ---------  --------------
   1> #BATCH     #BATCH
   2> #INTER     #INTER
   3> CPSVCMG    CPSVCMG
   4>            #CONNECT
   5> #BATCHSC   #BATCHSC
   6> #INTERSC   #INTERSC
   7> CPSVRMGR   SNASVCMG
   8> SNASVCMG   SNASVCMG
```

Related Commands

Command	Description
show snasw class-of-service	Displays the class of service (CoS) definitions predefined to SNASw.

show snasw node

To display details and statistics of the Switching Services (SNASw) operation, use the **show snasw node** command.

show snasw node

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Defaults

No default behaviors or values

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.1	Additional fields were added to the command output.
12.2	Additional fields were added to the command output to describe RTP information.
12.3	The Alert focal point field was added to the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw node** command:

```
Router# show snasw node

Node type                                          Branch Network Node
Node name                                          NETA.NODE
CP alias                                           NODE
Node ID                                            X'FFF00000'
Time active                                        9 days,  11 hrs,  57 mins,  13 secs
Defined LS good XID exchanges                      2
Defined LS bad XID exchanges                       0
Dynamic LS good XID exchanges                      243
Dynamic LS bad XID exchanges                       0
Number of active ISR sessions                      0
DLUR release level                                 1
Branch extender architecture version               1
Mode to COS mapping supported                      No
MS includes Multiple Domain Support                Yes
MDS send alert queue size                          10
Maximum locates                                    10000
Directory cache size                               10000
Maximum directory entries (0 is unlimited)         0
Locate timeout in seconds (0 is no timeout)        540
```

```
COS cache size                                    8
Topology database routing tree cache size         8
Topology database routing tree cache use limit    1
Maximum nodes stored in database (0 unlimited)    0
Maximum TGs stored in database (0 unlimited)      0
Maximum allowed ISR sessions                      22000
Maximum receive RU size for ISR sessions          61440
Maximum receive pacing window                     7
Storing endpoint RSCVs for debug                  Yes
Storing ISR RSCVs for debug                       No
Storing DLUR RSCVs for debug                      No
DLUR support                                      Yes
HPR support                                       Yes
RTP short request retry limit                     6
RTP path switch route attempts                    6
RTP path switch time LOW priority                 480 seconds
RTP path switch time MEDIUM priority              240 seconds
RTP path switch time HIGH priority                120 seconds
RTP path switch time NETWORK priority             60 seconds
Alert focal point                                 NETA.ND
PD log capture level                              Problem level entries
PD log size                                       500 kilobytes
PD log path                                       disk0:
IPS tracing                                       Inactive
DLC tracing                                       Active
DLC trace format                                  Detailed
DLC trace size                                    500 kilobytes
DLC trace path                                    tftp://10.102.16.25/tftp/node.dlct
Number of links                                   3
Number of local endpoint sessions                 4
Number of non-DLUR intermediate sessions          0
Number of DLUR intermediate sessions              0
Number of DLUR PUs                                0
Number of DLUR LUs                                0
```

Related Commands

Command	Description
show snasw statistics	Displays the SNASw node-wide information.

show snasw pdlog

To display entries in the cyclical problem determination log to the console, use the **show snasw pdlog** command.

show snasw pdlog [**brief** | **detail**] [**id** *record-id*] [**all** | **next** *number-records* | **last** *number-records*] [**filter** *filter-string*]

Syntax Description

brief	(Optional) Indicates that a one-line description for each pdlog entry is returned.
detail	(Optional) Indicates that a multiline display is returned.
id *record-id*	(Optional) Indicates that the 1 to 99999 trace record identifier. Only the frame ID that matches the record specified is displayed.
all	(Optional) Specifies that all records are displayed.
next *number-records*	(Optional) Displays records from the beginning, or following a record ID.
last *number-records*	(Optional) Displays records from the end or prior to the record ID. Indicates that the last *x* frames before the record identified in the ID operand (or before the last record in the trace if the ID operand is not coded) are displayed.
filter *filter-string*	(Optional) Indicates that a string follows against which the formatted trace output is filtered. Only frames that contain the *filter-string* argument are displayed.

Command Modes

EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw pdlog** command:

```
Router# show snasw pdlog

Problem Determination Log Output

**** 00000014 - AUDIT 512:727 (0) ****
CP-CP sessions established
 Adjacent CP name = CISCO.A
 1015 compliant   = 01
 Topology awareness of CP-CP sessions support = 01
 CP Capabilities :

   000C12C1 00000000 82844000
>From ../dcl/nssrcctp.c 589 :at 0:10:24, 1 March 93
```

Related Commands

Command	Description
snasw pdlog	Controls message logging to the console and the Systems Network Architecture (SNA) problem determination log cyclic buffer.

show snasw port

To display the Switching Services (SNASw) port objects, use the **show snasw port** command.

show snasw port [**brief** | **detail**] [**active** | **not-active**] [**name** *port-name-filter*]

Syntax Description

brief	(Optional) Indicates that a one-line description for each port entry is displayed.
detail	(Optional) Indicates that a multiline display is returned.
active	(Optional) Displays all active snasw ports.
not-active	(Optional) Displays all snasw ports that are not active.
name *port-name-filter*	(Optional) Indicates the name of the port to filter for which information is displayed. Only ports matching name are displayed.

Command Modes

EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show snasw port** command:

```
Router# show snasw port

Number of ports 3

      SNA Ports
        Name     State    SAP  HPR-SAP  Interface
      --------  --------  ---  -------  ---------------------
   1> ETH0      Active    x04    xC8    Ethernet0/0
   2> SER1      Active           xC8    Serial0/0
   3> TR0       Active    x04    xC8    TokenRing0/0

Router# show snasw port detail

Number of ports 3

1>
Port name                                          ETH0
Interface name                                     Ethernet0/0
DLC name                                           ETH0
Port state                                         Active
SAP                                                X'04'
HPR SAP                                            X'C8'
Port type                                          Shared Access Transport Facility
Port number                                        0
```

```
Link station role                                   Negotiable
Limited resource                                    No
Max send frame data (BTU) size                      1436
Maximum receive BTU size                            1436
Effective capacity                                  16 Mbps
Cost per connect time                               0
Cost per byte                                       0
Propagation delay                                   384 microseconds
User defined parameter 1                            128
User defined parameter 2                            128
User defined parameter 3                            128
Security                                            Nonsecure
Total available link stations                       3000
Number reserved for inbound link stations           0
Number reserved for outbound link stations          0
HPR support                                         No
HPR requires link level error recovery              No
Retry link stations                                 Yes
Maximum activation attempts                         0
Implicit links are uplink to End Nodes              No
Activation XID exchange limit                       9
Non-activation XID exchange limit                   5
Target pacing window size                           7
```

Related Commands

Command	Description
snasw port	Specifies the DLCs used by SNASw.

show snasw pu

To display the Switching Services (SNASw) physical unit (PU)s that require or request system services control points (SSCP)-PU services, use the **show snasw pu** command.

show snasw pu [**brief** | **detail**] [**active** | **not-active**] [**dlus** *dlus-filter*] [**name** *pu-name-filter*]

Syntax Description

brief	(Optional) Indicates that one line per PU is displayed. The brief version includes the PU name, PU ID, state, defined Dependent Logical Unit Server (DLUS), and current DLUS.
detail	(Optional) Indicates that a detailed, multiline display that shows all fields returned for a link is displayed.
active	(Optional) Displays the active snasw PUs.
not-active	(Optional) Displays the PUs that are not active.
dlus *dlus-filter*	(Optional) Indicates the fully qualified DLUS name (1 to 17 characters). Only PUs that are served by the DLUS specified are displayed.
name *pu-name-filter*	(Optional) Indicates a PU name to filter (1 to 8 characters). Only PUs matching this name are displayed.

Command Modes

EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show snasw pu** command:

```
Router# show snasw pu

Number of DLUR PUs 1
SNA DLUR PUs
      PU Name    PU ID     State    Defined DLUS       Current DLUS
      --------  --------  --------  -----------------  -----------------
   1> PL9101    19103001  Active                       NETA.SJMVS3

Router# show snasw pu detail

Number of DLUR PUs 1
1>
PU name                                            PL9101
Define DLUS name
Backup DLUS name
Active DLUS name                                   NETA.SJMVS3
PU ID (IDBLK/IDNUM)                                X'19103001'
PU location                                      Downstream
PU status                                        Active
DLUS session state                               Active
Automatic Network Shutdown support               Stop
DLUS retry timeout (seconds)                     0
DLUS retry limit                                 0
DLUS pipe PCID                                   X'FC0B862E4B1CE8FB'
DLUS pipe CP Name                                NETA.DLUR2
```

Related Commands

Command	Description
show snasw dlus	Displays the SNASw DLUS objects.

show snasw rtp

To display the SNA Switching Services (SNASw) Rapid Transit Protocol (RTP) connections, use the **show snasw rtp** command in user EXEC or privileged EXEC mode.

show snasw rtp [**brief** | **detail**] [**class-of-service** *cos-name*] [**cpname** *netid.cpname*] [**name** *connection-name-filter*] [**tcid** *tcid-connection*] [**history**] [**connected** | **pathswitch**]

Syntax Description

brief	(Optional) Indicates that one-line per RTP is displayed. The brief version of the display includes the RTP name, local transport connection identifier (TCID), remote TCID, remote control point (CP) name, and class of service (CoS).
detail	(Optional) Indicates that a detailed, multiline display, which shows all the fields for RTP is displayed.
class-of-service *cos-name*	(Optional) Shows specific High-Performance Routing (HPR) RTP connections by CoS name.
cpname *netid.cp-name*	(Optional) Displays specific HPR RTP connections by a fully qualified partner CP name, consisting of both the network ID and the CP name.
name *connection-name-filter*	(Optional) Indicates the name of the RTP connection (1 to 8 characters). Only the origins of transmission group (TG) records or destinations that match the specified name or node records appear.
tcid *tcid-connection*	(Optional) Displays the specific HPR RTP connection for the local TCID connections.
history	(Optional) Displays the HPR RTP rate graphs for each RTP connection. These graphs include the last 60 seconds, 60 minutes, and 72 hours for the Adaptive Rate Based (ARB) allowed send rate and actual receive rate. Graphs are not available for RSETUP pipes.
connected	(Optional) Displays RTP connections that are active and not currently path switching.
pathswitch	(Optional) Displays RTP connections that are currently attempting a path switch.

Defaults

The default display is brief.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(10)	The **history** keyword was added to provide the history of HPR RTP rate graphs for each RTP connection.

Usage Guidelines

HPR RTP pipes use a unique flow and congestion control algorithm called ARB flow control. ARB allows HPR pipes to measure the network's level of congestion and dynamically adjust the rate of data input into the network, so that the network is highly utilized and congestion is avoided. If actual losses occur, ARB can also react to those losses.

Examples

show snasw rtp Command Example

The following is sample output from the **show snasw rtp** command and shows a CP-CP session pipe to CISCO.B:

```
Router# show snasw rtp

Number of RTP connections 1

      SNA RTP Connections
      Local TCID (hex)  Remote TCID (hex)   Remote CP Name      COS
      ----------------  -----------------  -----------------  --------
   1> 0000000001000000  0000000001000000   CISCO.B            CPSVCMG

Router# show snasw rtp detail

Number of RTP connections 1
1>
Local NCEID                                         X'4052303030303031'
Local TCID                                          X'0000000001000000'
Remote TCID                                         X'0000000001000000'
Remote CP name                                      CISCO.B
Class of service name                               CPSVCMG
Liveness timer                                      180
Short request timer                                 704
Number of short request timeouts                    0
Total bytes sent                                    484
Total bytes received                                484
Total bytes resent                                  0
Total bytes discarded                               0
Total packets sent                                  24
Total packets received                              25
Total packets resent                                0
Total packets discarded                             0
Total Session Connector frames sent                 2
Total Session Connector frames received             2
Number of invalid SNA frames received               0
Number of gaps detected                             0
Minimum send rate                                   1597
Current send rate                                   1597
Maximum send rate                                   1597
Minimum receive rate                                0
Current receive rate                                0
Maximum receive rate                                0
Burst size                                          8192
Smoothed round trip delay time                      352
Last round trip delay time                          8
```

```
Number of active sessions                            2
Link name of first hop                               LINKT
Performing ISR boundary function                     No
RTP connection type                                  CP-CP session
RSCV Length                                          18
Route                                                CISCO.A
                                                     <-tg21-> CISCO.B
```

show snasw session

To display the Switching Services (SNASw) session objects, use the **show snasw session** command.

show snasw session [**local** | **dlur** | **intermediate**] [**name** *session-name-filter*] [**pcid** *pcid-filter*] [**brief** | **detail** | **intermediate**] [**active** | **not-active**]

Syntax Description

local	(Optional) Indicates that the scope of the display is limited to the types of sessions indicated. Local sessions are those that terminate on the node. Examples include control point (CP)-CP sessions and Dependent Logical Unit Requestor (DLUR)-Dependent Logical Unit Server (DLUS) sessions.
dlur	(Optional) Indicates that the scope of the display is limited to the types of sessions indicated. DLUS sessions are logical unit (LU)-LU sessions passing through the node, which are using the DLUR for dependent session.
intermediate	(Optional) Indicates that the scope of the display is limited to the types of sessions indicated. Intermediate sessions are LU-LU sessions passing through the node and are not DLUR-associated.
name *session-name-filter*	(Optional) Indicates the fully qualified name (1 to 17 characters). Only sessions that have a local or remote endpoint LU name matching the supplied name are displayed.
pcid *pcid-filter*	(Optional) Indicates an 8-byte procedure correlation identifier (PCID) specified in hexadecimal form. All sessions matching the PCID filter are displayed.
brief	(Optional) Indicates that one line per session is displayed. The brief version includes PCID, state (active or inactive), session endpoint LU names, and mode.
detail	(Optional) Indicates that a detailed, multiline display that shows all fields returned for the session is displayed.
active	(Optional) Displays the active snasw sessions.
not-active	(Optional) Displays the snasw sessions that are not active.

Command Modes

EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show snasw session** command:

```
Router# show snasw session

Number of local endpoint sessions 4

      SNA Local Endpoint Sessions
         PCID (hex)      Partner LU Name   Link Name   Mode     COS
      ----------------  -----------------  --------- -------- -------
   1> F4276146FE1472AB  CISCO.C            @I000003  CPSVCMG  CPSVCMG
   2> F42754959A918058  CISCO.C            @I000003  CPSVCMG  CPSVCMG
   3> F4276146FE1472AA  CISCO.A            @R000002  CPSVCMG  CPSVCMG
   4> F4276DF74485118B  CISCO.A            @R000002  CPSVCMG  CPSVCMG

Number of intermediate sessions 2

      SNA Intermediate Sessions
         PCID (hex)     Primary LU Name    Secondary LU Name   Mode      COS
      ----------------  -----------------  -----------------  -------- -------
   1> F42754959A918059  CISCO.C            CISCO.A            SNASVCMG SNASVCMG
   2> F42754959A91805A  CISCO.C            CISCO.A            #INTER   #INTER

Number of intermediate DLUR sessions 0

      SNA DLUR Assisted Intermediate Sessions
         PCID (hex)     Primary LU Name    Secondary LU Name   Mode      COS
      ----------------  -----------------  -----------------  -------- -------
```

The following is sample output from the **show snasw session detail** command:

```
Router# show snasw session detail

Number of local endpoint sessions 4

1>
Partner LU name                                   CISCO.C
Mode name                                         CPSVCMG
Class of service name                             CPSVCMG
Transmission priority                             Network
Carried over a limited resource                   No
Polarity                                          Primary
Contention                                        CONWINNER
SSCP ID received in ACTPU                         X'000000000000'
Session timeout period (ms)                       0
Outbound LFSID (SIDH,SIDL,ODAI)                   X'02',X'00',B'0'
Procedure correlator ID (PCID)                    X'F4276146FE1472AB'
PCID generator CP name                            CISCO.B
FID2 Session ID                                   X'F4276146FE1472AB'
Link name                                         @I000003
Session statistics:
  Maximum send RU size                            1152
  Maximum receive RU size                         1152
  Total data frames sent                          3
  Total data frames received                      1
  Total FMD data frames sent                      3
  Total FMD data frames received                  1
  Total bytes sent                                511
  Total bytes received                            15
  Max send pacing window                          7
  Max receive pacing window                       7
  Current send pacing window                      7
  Current receive pacing window                   7
```

Related Commands

Command	Description
show snasw link	Displays SNASw link objects.

show snasw statistics

To display Switching Services (SNASw) node-wide information, use the **show snasw statistics** command.

show snasw statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Defaults

No default behaviors or values

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw statistics** command:

```
Router# show snasw statistics

SNASw Subsystem Uptime                       3 hrs, 19 mins, 36 secs

Directory Statistics:
  Maximum number of cache entries                 10000
  Current number of cache entries                 0
  Current number of home entries                  2
  Current number of registry entries              4
  Total number of entries in directory            6
  Total cache hits                                0
  Total cache misses                              0
  Number of directed locates sent                 2
  Number of directed locates returned not found   0
  Number of directed locates received             0
  Number of broadcast locates sent                0
  Number of broadcast locates returned not found  0
  Number of broadcast locates received            0
  Number of locates outstanding                   0

Topology Statistics:
  Maximum number of nodes                         0
  Current number of nodes                         4
  Total number of received TDUs                   0
  Total number of sent TDUs                       0
  Total received TDUs with lower RSN              0
  Total received TDUs with equal RSN              0
  Total received TDUs with higher RSN            0
  Total received TDUs with higher odd value RSN   0
  Total node state changes requiring TDUs         0
  Total database inconsistencies detected         0
  Total number of timer based TDUs generated      0
  Total number of node records purged             0
  Total received TG updates with lower RSN        0
  Total received TG updates with equal RSN        0
  Total received TG updates with higher RSN       0
  Total received TG updates with higher odd RSN   0
  Total TG state changes requiring TG updates     5
  Total TG database inconsistencies detected      0
  Total number of timer TG updates generated      0
  Total number of TG records purged               0
  Total number of routes calculated               2
  Total number of routes rejected                 0
  Total number of cache hits in route calculation  0
  Total number of cache misses in rte calculation  7
  Total number of TDU wars detected               0

Number of processes 23
      CPU/Memory usage per SNA Switch process
      Process Name                         CPU Time (ms)  Memory Used (bytes)
      -----------------------------------  -------------  -------------------
   1> NOF API                                        20                  20
   2> N-Base allocated memory                         0               79484
   3> Buffer Manager (BM)                            12                 232
   4> Node Operator Facility (NOF)                  152               13188
   5> Address Space Manager (ASM)                    28                1296
   6> Address Space (AS)                             24                   0
   7> Session Services (SS)                          36                1676
   8> Directory Services (DS)                        92              550036
   9> Configuration Services (CS)                    48                9148
  10> Management Services (MS)                        4                 252
  11> Multiple Domain Support (MDS)                   0                3792
  12> Topology & Routing Services (TRS)              24               22368
  13> Session Connector Manager (SCM)                12                2232
  14> Session Connector (SCO)                         0                1232
  15> Session Manager (SM)                           56               13416
  16> Resource Manager (RM)                          64                   0
  17> Presentation Services (PS)                     68                   0
  18> Half Session (HS)                              29                   0
  19> Path Control (PC)                             188               50712
  20> Data Link Control (DLC)                       112                 144
  21> Dependent LU Requester (DR)                    12                7032
  22> High Performance Routing (HPR)                 12                3632
  23> Rapid Transport Protocol (RTP)                116               18460
```

Related Commands

Command	Description
show snasw node	Displays details and statistics of the SNASw operation.

show snasw summary-ipstrace

To display the continuously running "footprint" summary interprocess signal trace on the router console, use the **show snasw summary-ipstrace** command.

show snasw summary-ipstrace [**id** *recordid*] [**all** | **next** *number-records* | **last** *number-records*] [**filter** *filter-string*]

Syntax Description

id *recordid*	(Optional) Indicates that the 1 to 99999 trace record identifier. Only the frame ID that matches the record specified is displayed.
all	(Optional) Specifies that all records are displayed.
next *number-records*	(Optional) Displays records from the beginning, or following a record ID.
last *number-records*	(Optional) Displays records from the end or prior to the record ID. Indicates that the last *x* frames before the record identified in the ID operand (or before the last record in the trace if the ID operand is not coded) are displayed.
filter *filter-string*	(Optional) Indicates that a string follows against which the formatted trace output is filtered. Only frames that contain the *filter-string* argument are displayed.

Command Modes

EXEC

Defaults

No default behaviors or values

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw summary-ipstrace** command:

```
Router# show snasw summary-ipstrace

IPS Trace Output

433414 : VERB_SIGNAL : SCM(20E0000) -> TRS(20D0000) Q 1
433415 : VERB_SIGNAL : --(0) -> TRS(20D0000) Q 1
433416 : VERB_SIGNAL : TRS(20D0000) -> SS(2080000) Q 1
433417 : VERB_SIGNAL : --(0) -> SS(2080000) Q 1
433418 : VERB_SIGNAL : SS(2080000) -> CS(20A0000) Q 2
433419 : VERB_SIGNAL : --(0) -> CS(20A0000) Q 2
433420 : VERB_SIGNAL : CS(20A0000) -> --(2040000) Q 1
```

```
433421 : VERB_SIGNAL : --(0) -> --(2040000) Q 1
433422 : VERB_SIGNAL : --(0) -> NOF(2050000) Q 80
433423 : VERB_SIGNAL : --(0) -> NOF(2050000) Q 80
433424 : VERB_SIGNAL : NOF(2050000) -> DS(2090000) Q 1
433425 : VERB_SIGNAL : --(0) -> DS(2090000) Q 1
433426 : VERB_SIGNAL : DS(2090000) -> --(2040000) Q 1
433427 : VERB_SIGNAL : --(0) -> --(2040000) Q 1
433428 : VERB_SIGNAL : --(0) -> NOF(2050000) Q 80
433429 : VERB_SIGNAL : --(0) -> NOF(2050000) Q 80
433430 : VERB_SIGNAL : NOF(2050000) -> TRS(20D0000) Q 1
433431 : VERB_SIGNAL : --(0) -> TRS(20D0000) Q 1
433432 : VERB_SIGNAL : TRS(20D0000) -> --(2040000) Q 1
433433 : VERB_SIGNAL : --(0) -> --(2040000) Q 1
```

Related Commands

Command	Description
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.

show snasw topology

To display Switching Services (SNASw) topology records, use the **show snasw topology** command.

show snasw topology [**name** *cp-name-filter*] [**brief** | **detail**]

Syntax Description

name *cp-name-filter*	(Optional) Indicates the fully qualified name of the control point (CP) (1 to 17 characters). Only records that match the cpname specified are displayed.
brief	(Optional) Indicates one line per topology record is displayed.
detail	(Optional) Indicates that a detailed, multiline display of topology information.

Command Modes

EXEC

Defaults

The default display is brief.

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show snasw topology** command:

```
Router# show snasw topology

Number of topology entries 2

      SNA Topology Entries
       Dest. Node Name   Type  TG#      TG Type             TG Status
      -----------------  ----  ---  ----------------  ---------------------
   1> NETA.MVSD          Intr   21  Uplink            CP-CP sessions active
   2> NETA.BERNIEPU      Enpt    0  Downlink          Active
```

The following is sample output from the **show snasw topology detail** command:

```
Router# show snasw topo detail
Number of topology entries 2

1>
Destination node name                              NETA.MVSD
Destination node type                              Intermediate
Transmission Group Number                          21
Destination address
Resource Sequence Number                           0
TG status                                          CP-CP sessions active
Active CP-CP sessions for this TG                  Yes
Is this a branch TG                                No
```

```
Branch link type                                   Uplink
Effective capacity                                 16 Mbps
Cost per connect time                              196
Cost per byte                                      196
Propagation delay                                  384 microseconds
User defined parameter 1                           128
User defined parameter 2                           128
User defined parameter 3                           128
Security                                           Nonsecure


2>
Destination node name                              NETA.BERNIEPU
Destination node type                              Endpoint
Transmission Group Number                          0
Destination address
Resource Sequence Number                           0
TG status                                          Active
Active CP-CP sessions for this TG                  No
Is this a branch TG                                No
Branch link type                                   Downlink
Effective capacity                                 16 Mbps
Cost per connect time                              196
Cost per byte                                      196
Propagation delay                                  384 microseconds
User defined parameter 1                           128
User defined parameter 2                           128
User defined parameter 3                           128
Security                                           Nonsecure
```

Related Commands

Command	Description
show snasw link	Displays SNASw link objects.

show source-bridge

To display the current source bridge configuration and miscellaneous statistics, use the **show source-bridge** command in privileged EXEC mode.

show source-bridge [**interface**]

Syntax Description

interface	(Optional) Displays the current source bridge configuration over all interfaces and a summary of all packets sent and received over each interface, not just the number of packets forwarded through the bridge.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2	The **interface** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show source-bridge** command:

```
Router# show source-bridge

Local Interfaces:                          receive     transmit
             srn bn  trn r p s n  max hops     cnt         cnt        drops
TR0            5  1   10 *   *          7    39:1002     23:62923

Ring Group 10:
  This peer: TCP 10.136.92.92
   Maximum output TCP queue length, per peer: 100
  Peers:                 state   lv  pkts_rx  pkts_tx  expl_gn    drops TCP
   TCP  10.136.92.92     -       2       0        0          0      0     0
   TCP  10.136.93.93     open    2*     18       18          3      0     0
Rings:
   bn: 1 rn: 5    local  ma: 4000.3080.844b TokenRing0            fwd: 18
   bn: 1 rn: 2   remote  ma: 4000.3080.8473 TCP  10.136.93.93     fwd: 36

Explorers: ------- input -------             ------- output -------
       spanning  all-rings     total      spanning  all-rings     total
  TR0         0          3         3             3          5         8
```

The following is sample output from the **show source-bridge** command when Token Ring LAN emulation (LANE) is configured.

```
Router# show source-bridge

Local Interfaces:                           receive     transmit
             srn bn  trn r p s n  max hops     cnt         cnt       drops
AT2/0.1     2048  5  256 *   f     7  7  7     5073        5072          0
To3/0/0        1  1  256 *   f     7  7  7     4719        4720          0

Global RSRB Parameters:
 TCP Queue Length maximum: 100

Ring Group 256:
  No TCP peername set, TCP transport disabled
   Maximum output TCP queue length, per peer: 100
  Rings:
   bn: 5  rn: 2048 local  ma: 4000.0ca0.5b40 ATM2/0.1              fwd: 5181
   bn: 1  rn: 1    local  ma: 4000.3005.da06 TokenRing3/0/0        fwd: 5180

Explorers: ------- input -------             ------- output -------
         spanning  all-rings     total      spanning  all-rings     total
AT2/0.1         9          1        10            10          0        10
To3/0/0        10          0        10             9          1        10

  Local: fastswitched 20        flushed 0         max Bps 38400

         rings      inputs          bursts          throttles     output drops
       To3/0/0          10               0                 0                0
```

The following is sample output from the **show source-bridge** command with the **interface** keyword specified:

```
Router# show source-bridge interface

                                           v p s n r                   Packets
 Interface  St  MAC-Address    srn  bn  trn r x p b c IP-Address          In   Out

 To0/0      up 0000.300a.7c06    1  1 2009 *   b   F 10.2.0.9        63836 75413
 To0/1      up 0000.300a.7c86    2  1 2009 *   b   F 10.1.0.9        75423 63835
 To0/2      up 0000.300a.7c46 1001  1 2009 *   b   F                  5845  5845
```

Table 91 describes the significant fields shown in the displays.

Table 91 show source-bridge Field Descriptions

Field	Description
Local Interfaces:	Description of local interfaces.
srn	Ring number of this Token Ring.
bn	Bridge number of this router for this ring.
trn	Group in which the interface is configured. Can be the target ring number or virtual ring group.
r	Ring group is assigned. An asterisk (*) in this field indicates that a ring group has been assigned for this interface.
p	Interface can respond with proxy explorers. An asterisk (*) in this field indicates that the interface can respond to proxy explorers.

Table 91 show source-bridge Field Descriptions (continued)

Field	Description
s	Spanning-tree explorers enabled on the interface. An asterisk (*) indicates that this interface will forward spanning-tree explorers.
n	Interface has NetBIOS name caching enabled. An asterisk (*) in this field indicates that the interface has NetBIOS name caching enabled.
max hops	Maximum number of hops.
receive cnt	Bytes received on the interface for source bridging.
transmit cnt	Bytes sent on the interface for source bridging.
drops	Number of dropped packets.
Ring Group *n*:	The number of the ring group.
This peer:	Address and address type of this peer.
Maximum output TCP queue length, per peer:	Maximum number of packets queued on this peer before the Cisco IOS software starts dropping packets.
Peers:	Addresses and address types of the ring group peers.
state	Current state of the peer, open or closed. A hyphen indicates this router.
lv	Indicates local acknowledgment.
pkts_rx	Number of packets received.
pkts_tx	Number of packets sent.
expl_gn	Explorers generated.
drops	Number of packets dropped.
TCP	Lists the current TCP backup queue length.
Rings:	Describes the ring groups. Information displayed is the bridge groups, ring groups, whether each group is local or remote, the MAC address, the network address or interface type, and the number of packets forwarded. A type shown as “locvrt” indicates a local virtual ring used by SDLLC or SR/TLB; a type shown as “remvrt” indicates a remote virtual ring used by SDLC Logical Link Control (SDLLC) or source-route translational bridging (SR/TLB).
Explorers:	This section describes the explorer packets that the Cisco IOS software has sent and received.
input	Explorers received by Cisco IOS software.
output	Explorers generated by Cisco IOS software.
TR0	Interface on which explorers were received.
spanning	Spanning-tree explorers.
all-rings	All-rings explored.
total	Summation of spanning and all-rings.
fastswitched	Number of fast-switched packets.
flushed	Number of flushed packets.
max Bps	Maximum bytes per second.
rings	Interface for the particular ring.

Table 91 show source-bridge Field Descriptions (continued)

Field	Description
inputs	Number of inputs.
bursts	Number of bursts.
throttles	Number of throttles.
output drops	Number of output drops.

show span

To display the spanning-tree topology known to the router, use the **show span** command in user EXEC or privileged EXEC mode.

show span

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show span** command:

```
Router# show span

Bridge Group 1 is executing the IBM compatible Spanning Tree Protocol
  Bridge Identifier has priority 32768, address 0000.0c0c.f68b
  Configured hello time 2, max age 6, forward delay 4
  Current root has priority 32768, address 0000.0c0c.f573
  Root port is 001A (TokenRing0/0), cost of root path is 16
  Topology change flag not set, detected flag not set
  Times:  hold 1, topology change 30, notification 30
          hello 2, max age 6, forward delay 4, aging 300
  Timers: hello 0, topology change 0, notification 0
Port 001A (TokenRing0/0) of bridge group 1 is forwarding. Path cost 16
   Designated root has priority 32768, address 0000.0c0c.f573
   Designated bridge has priority 32768, address 0000.0c0c.f573
   Designated port is 001B, path cost 0, peer 0
   Timers: message age 1, forward delay 0, hold 0
Port 002A (TokenRing0/1) of bridge group 1 is blocking. Path cost 16
   Designated root has priority 32768, address 0000.0c0c.f573
   Designated bridge has priority 32768, address 0000.0c0c.f573
   Designated port is 002B, path cost 0, peer 0
   Timers: message age 0, forward delay 0, hold 0
Port 064A (spanRSRB) of bridge group 1 is disabled. Path cost 250
   Designated root has priority 32768, address 0000.0c0c.f573
   Designated bridge has priority 32768, address 0000.0c0c.f68b
   Designated port is 064A, path cost 16, peer 0
   Timers: message age 0, forward delay 0, hold 0
```

A port (spanRSRB) is created with each virtual ring group. The port will be disabled until one or more peers go into open state in the ring group.

show spanning-tree

To display spanning-tree information for the specified spanning-tree instances, use the **show spanning-tree** command in privileged EXEC mode.

Cisco 2600, 3660, and 3845 Series Switches

show spanning-tree [*bridge-group*] [**active** | **backbonefast** | **blockedports** | **bridge** | **brief** | **inconsistentports** | **interface** *interface-type interface-number*| **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*]

Cisco 6500/6000 Catalyst Series Switches and Cisco 7600 Series Routers

show spanning-tree [*bridge-group* | **active** | **backbonefast** | **bridge** [*id*] | **detail** | **inconsistentports** | **interface** *interface-type interface-number* [**portfast** [**edge**]] | **mst** [*list* | **configuration** [**digest**]] | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id* | **port-channel** *number* | **pathcost** *method*]

Syntax Description

bridge-group	(Optional) Specifies the bridge group number. The range is 1 to 255.
active	(Optional) Displays spanning-tree information on active interfaces only.
backbonefast	(Optional) Displays spanning-tree BackboneFast status.
blockedports	(Optional) Displays blocked port information.
bridge	(Optional) Displays status and configuration of this switch.
brief	(Optional) Specifies a brief summary of interface information.
configuration [**digest**]	(Optional) Displays the multiple spanning-tree current region configuration.
inconsistentports	(Optional) Displays information about inconsistent ports.
interface *interface-type interface-number*	(Optional) Specifies the type and number of the interface. Enter each interface designator, using a space to separate it from the one before and the one after. Ranges are not supported. Valid interfaces include physical ports and virtual LANs (VLANs). See the "Usage Guidelines" for valid values.
list	(Optional) Specifies a multiple spanning-tree instance list.
mst	(Optional) Specifies multiple spanning-tree.
portfast [**edge**]	(Optional) Displays spanning-tree PortFast edge interface operational status. Beginning with Cisco IOS Release 12.2(33)SXI, the **edge** keyword is required. In earlier releases, the **edge** keyword is not used.
root	(Optional) Displays root-switch status and configuration.
summary	(Optional) Specifies a summary of port states.
totals	(Optional) Displays the total lines of the spanning-tree state section.
uplinkfast	(Optional) Displays spanning-tree UplinkFast status.
vlan *vlan-id*	(Optional) Specifies the VLAN ID. The range is 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094. If the *vlan-id* value is omitted, the command applies to the spanning-tree instance for all VLANs.

id	(Optional) Identifies the spanning tree bridge.
detail	(Optional) Shows status and configuration details.
port-channel *number*	(Optional) Identifies the Ethernet channel associated with the interfaces.
pathcost *method*	(Optional) Displays the default path-cost calculation method that is used. See the "Usage Guidelines" section for the valid values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(5.2)WC(1)	This command was integrated into Cisco IOS Release 12.0(5.2)WC(1).
12.1(6)EA2	This command was integrated into Cisco IOS Release 12.1(6)EA2. The following keywords and arguments were added: *bridge-group*, **active**, **backbonefast**, **blockedports**, **bridge**, **inconsistentports**, **pathcost** *method*, **root**, **totals**, and **uplinkfast**.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	The syntax added in Cisco IOS Release 12.1(6)EA2 was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(4)T	The platform support and syntax added in Cisco IOS Release 12.2(15)ZJ was integrated into Cisco IOS Release 12.3(4)T.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1–4094 for specified platforms.
12.2(33)SXI	This command was modified to require the **edge** keyword after **portfast**. The command output was modified to show the status of Bridge Assurance and PVST Simulation.

Usage Guidelines

The keywords and arguments that are available with the **show spanning-tree** command vary depending on the platform you are using and the network modules that are installed and operational.

Cisco 2600, 3660, and 3845 Series Switches

The valid values for **interface** *interface-type* are:

- **fastethernet**—Specifies a Fast Ethernet IEEE 802.3 interface.
- **port-channel**—Specifies an Ethernet channel of interfaces.

Cisco 6500/6000 Catalyst Switches and 7600 Series Routers

The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

When checking spanning tree-active states and you have a large number of VLANs, you can enter the **show spanning-tree summary total** command. You can display the total number of VLANs without having to scroll through the list of VLANs.

The valid values for **interface** *interface-type* are:

- **fastethernet**—Specifies a Fast Ethernet IEEE 802.3 interface.
- **port-channel**—Specifies an Ethernet channel of interfaces.
- **atm**—Specifies an Asynchronous Transfer Mode (ATM) interface.
- **gigabitethernet**—Specifies a Gigabit Ethernet IEEE 802.3z interface.
- **multilink**—Specifies a multilink-group interface.
- **serial**—Specifies a serial interface.
- **vlan**—Specifies a catalyst VLAN interface.

The valid values for keyword **pathcoast** *method* are:

- **append**—Appends the redirected output to a URL (supporting the append operation).
- **begin**—Begins with the matching line.
- **exclude**—Excludes matching lines.
- **include**—Includes matching lines.
- **redirect**—Redirects output to a URL.
- **tee**—Copies output to a URL.

When you run the **show spanning-tree** command for a VLAN or an interface the switch router will display the different port states for the VLAN or interface. The valid spanning-tree port states are listening, learning, forwarding, blocking, disabled, and loopback. See Table 0-92 for definitions of the port states:

Table 0-92 show spanning-tree vlan Command Port States

Field	Definition
LIS	Listening is when the port spanning tree initially starts to listen for BPDU packets for the root bridge.
LRN	Learning is when the port sets the proposal bit on the BPDU packets it sends out
FWD	Forwarding is when the port is sending and listening to BPDU packets and forwarding traffic.
BLK	Blocked is when the port is still sending and listening to BPDU packets but is not forwarding traffic.
DIS	Disabled is when the port is not sending or listening to BPDU packets and is not forwarding traffic.
LBK	Loopback is when the port receives its own BPDU packet back.

Examples

Cisco 2600, 3660, and 3845 Series Switches

The following example shows that bridge group 1 is running the VLAN Bridge Spanning Tree Protocol:

```
Router# show spanning-tree 1

Bridge group 1 is executing the VLAN Bridge compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, address 0000.0c37.b055
Configured hello time 2, max age 30, forward delay 20
We are the root of the spanning tree
Port Number size is 10 bits
Topology change flag not set, detected flag not set
Times: hold 1, topology change 35, notification 2
      hello 2, max age 30, forward delay 20
Timers: hello 0, topology change 0, notification 0
  bridge aging time 300

Port 8 (Ethernet1) of Bridge group 1 is forwarding
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 0000.0c37.b055
   Designated bridge has priority 32768, address 0000.0c37.b055
   Designated port is 8, path cost 0
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 184, received 0
```

The following is sample output from the **show spanning-tree summary** command:

```
Router# show spanning-tree summary

UplinkFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN1                23       0         0        1          24
-------------------- -------- --------- -------- ---------- ----------
              1 VLAN 23       0         0        1          24
```

Table 93 describes the significant fields shown in the display.

Table 93 show spanning-tree summary Field Descriptions

Field	Description
UplinkFast	Indicates whether the spanning-tree UplinkFast feature is enabled or disabled.
Name	Name of VLAN.
Blocking	Number of ports in the VLAN in a blocking state.
Listening	Number of ports in a listening state.
Learning	Number of ports in a learning state.
Forwarding	Number of ports in a forwarding state.
STP Active	Number of ports using the Spanning-Tree Protocol.

The following is sample output from the **show spanning-tree brief** command:

```
Router# show spanning-tree brief

VLAN1
  Spanning tree enabled protocol IEEE
  ROOT ID    Priority 32768
             Address 0030.7172.66c4
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN1
  Spanning tree enabled protocol IEEE
  ROOT ID    Priority 32768
             Address 0030.7172.66c4
Port                               Designated
Name     Port ID Prio Cost Sts  Cost  Bridge ID      Port ID
------- ------- ---- ---- ---  ----  -------------- -------
Fa0/11  128.17  128  100  BLK  38    0404.0400.0001 128.17
Fa0/12  128.18  128  100  BLK  38    0404.0400.0001 128.18
Fa0/13  128.19  128  100  BLK  38    0404.0400.0001 128.19
Fa0/14  128.20  128  100  BLK  38    0404.0400.0001 128.20
Fa0/15  128.21  128  100  BLK  38    0404.0400.0001 128.21
Fa0/16  128.22  128  100  BLK  38    0404.0400.0001 128.22
Fa0/17  128.23  128  100  BLK  38    0404.0400.0001 128.23
Fa0/18  128.24  128  100  BLK  38    0404.0400.0001 128.24
Fa0/19  128.25  128  100  BLK  38    0404.0400.0001 128.25
Fa0/20  128.26  128  100  BLK  38    0404.0400.0001 128.26
Fa0/21  128.27  128  100  BLK  38    0404.0400.0001 128.27

Port                               Designated
Name     Port ID Prio Cost Sts  Cost  Bridge ID      Port ID
------- ------- ---- ---- ---  ----  -------------- -------
Fa0/22  128.28  128  100  BLK  38    0404.0400.0001 128.28
Fa0/23  128.29  128  100  BLK  38    0404.0400.0001 128.29
Fa0/24  128.30  128  100  BLK  38    0404.0400.0001 128.30 Hello Time   2 sec  Max Age 20
sec  Forward Delay 15 sec
```

Table 94 describes the significant fields shown in the display.

Table 94 show spanning-tree brief Field Descriptions

Field	Description
VLAN1	VLAN for which spanning-tree information is shown.
Spanning tree enabled protocol	Type of spanning tree (IEEE, IBM, CISCO).
ROOT ID	Indicates the root bridge.
Priority	Priority indicator.
Address	MAC address of the port.
Hello Time	Amount of time, in seconds, that the bridge sends bridge protocol data units (BPDUs).
Max Age	Amount of time, in seconds, that a BPDU packet should be considered valid.
Forward Delay	Amount of time, in seconds, that the port spends in listening or learning mode.
Port Name	Interface type and number of the port.
Port ID	Identifier of the named port.
Prio	Priority associated with the port.

Table 94 show spanning-tree brief Field Descriptions (continued)

Field	Description
Cost	Cost associated with the port.
Sts	Status of the port.
Designated Cost	Designated cost for the path.
Designated Bridge ID	Bridge identifier of the bridge assumed to be the designated bridge for the LAN associated with the port.

The following is sample output from the **show spanning-tree vlan 1** command:

```
Router# show spanning-tree vlan 1

Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00e0.1eb2.ddc0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0010.0b3f.ac80
  Root port is 5, cost of root path is 10
  Topology change flag not set, detected flag not set, changes 1
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0

Interface Fa0/1  in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 0010.0b3f.ac80
Designated bridge has priority 32768, address 00e0.1eb2.ddc0
   Designated port is 1, path cost 10
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
```

Table 95 describes the significant fields shown in the display.

Table 95 show spanning-tree vlan Field Descriptions

Field	Description
Spanning tree	Type of spanning tree (IEEE, IBM, CISCO).
Bridge Identifier	Part of the bridge identifier and taken as the most significant part for bridge ID comparisons.
address	Bridge MAC address.
Root port	Identifier of the root port.
Topology change	Flags and timers associated with topology changes.

The following is sample output from the **show spanning-tree interface fastethernet0/3** command:

```
Router# show spanning-tree interface fastethernet0/3

Interface Fa0/3 (port 3) in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 6000, address 0090.2bba.7a40
   Designated bridge has priority 32768, address 00e0.1e9f.4abf
   Designated port is 3, path cost 410
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
```

Cisco 6500/6000 Series Catalyst Switches and 7600 Series Routers

This example shows how to display a summary of interface information:

```
Router# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     0004.9b78.0800
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     0004.9b78.0800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Port ID                     Designated                Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID            Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Gi2/1            128.65           4 LIS         0  4097 0004.9b78.0800 128.65
Gi2/2            128.66           4 LIS         0  4097 0004.9b78.0800 128.66
Fa4/3            128.195         19 LIS         0  4097 0004.9b78.0800 128.195
Fa4/4            128.196         19 BLK         0  4097 0004.9b78.0800 128.195

Router#
```

Table 96 describes the fields that are shown in the example.

Table 96 show spanning-tree Command Output Fields

Field	Definition
Port ID Prio.Nbr	Port ID and priority number.
Cost	Port cost.
Sts	Status information.

This example shows how to display information about the spanning tree on active interfaces only:

```
Router# show spanning-tree active

UplinkFast is disabled
BackboneFast is disabled

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0050.3e8d.6401
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 16384, address 0060.704c.7000
  Root port is 265 (FastEthernet5/9), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 18:13:54 ago
  Times:  hold 1, topology change 24, notification 2
          hello 2, max age 14, forward delay 10
  Timers: hello 0, topology change 0, notification 0

Router#
```

This example shows how to display the status of spanning-tree BackboneFast:

```
Router# show spanning-tree backbonefast

BackboneFast is enabled

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs)     : 0
Number of RLQ request PDUs received (all VLANs)   : 0
Number of RLQ response PDUs received (all VLANs)  : 0
Number of RLQ request PDUs sent (all VLANs)       : 0
Number of RLQ response PDUs sent (all VLANs)      : 0
Router#
```

This example shows how to display information about the spanning tree for this bridge only:

```
Router# show spanning-tree bridge

VLAN1
  Bridge ID  Priority    32768
             Address     0050.3e8d.6401
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
.
Router#
```

This example shows how to display detailed information about the interface:

```
Router# show spanning-tree detail

VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 4096, address 00d0.00b8.1401
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 9 last change occurred 02:41:34 ago
from FastEthernet4/21
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 1, topology change 0, notification 0, aging 300


Port 213 (FastEthernet4/21) of VLAN1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.213.
Designated root has priority 4096, address 00d0.00b8.1401
Designated bridge has priority 4096, address 00d0.00b8.1401
Designated port id is 128.213, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 4845, received 1
Router#
```

This example shows how to display information about the spanning tree for a specific interface:

```
Router# show spanning-tree interface fastethernet 5/9

Interface Fa0/10 (port 23) in Spanning tree 1 is ROOT-INCONSISTENT
Port path cost 100, Port priority 128
Designated root has priority 8192, address 0090.0c71.a400
Designated bridge has priority 32768, address 00e0.1e9f.8940
```

This example shows how to display information about the spanning tree for a specific bridge group:

```
Router# show spanning-tree 1

UplinkFast is disabled
 BackboneFast is disabled

  Bridge group 1 is executing the ieee compatible Spanning Tree protocol
   Bridge Identifier has priority 32768, address 00d0.d39c.004d
   Configured hello time 2, max age 20, forward delay 15
   Current root has priority 32768, address 00d0.d39b.fddd
   Root port is 7 (FastEthernet2/2), cost of root path is 19
   Topology change flag set, detected flag not set
   Number of topology changes 3 last change occurred 00:00:01 ago
           from FastEthernet2/2
   Times:  hold 1, topology change 35, notification 2
           hello 2, max age 20, forward delay 15
   Timers: hello 0, topology change 0, notification 0  bridge aging time 15

Port 2 (Ethernet0/1/0) of Bridge group 1 is down

    Port path cost 100, Port priority 128
    Designated root has priority 32768, address 0050.0bab.1808
    Designated bridge has priority 32768, address 0050.0bab.1808
    Designated port is 2, path cost 0
    Timers: message age 0, forward delay 0, hold 0
    BPDU: sent 0, received 0
Router#
```

This example shows how to display a summary of port states:

```
Router# show spanning-tree summary

Root bridge for: Bridge group 1, VLAN0001, VLAN0004-VLAN1005
 VLAN1013-VLAN1499, VLAN2001-VLAN4094
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
1 bridge               0        0         0        1          1
3584 vlans 3584 0 0 7168 10752


Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                  3584     0         0        7169       10753
Router#
```

This example shows how to display the total lines of the spanning-tree state section:

```
Router#  show spanning-tree summary total
Root bridge for:Bridge group 10, VLAN1, VLAN6, VLAN1000.
Extended system ID is enabled.
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
```

```
Default pathcost method used is long

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
           105 VLANs 3433     0         0        105        3538

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) :0
Number of inferior BPDUs received (all VLANs)     :0
Number of RLQ request PDUs received (all VLANs)   :0
Number of RLQ response PDUs received (all VLANs)  :0
Number of RLQ request PDUs sent (all VLANs)       :0
Number of RLQ response PDUs sent (all VLANs)      :0
Router#
```

This example shows how to display information about the spanning tree for a specific VLAN:

```
Router# show spanning-tree vlan 200
VLAN0200
 Spanning tree enabled protocol ieee
 Root ID Priority 32768
    Address 00d0.00b8.14c8
    This bridge is the root
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID Priority 32768
    Address 00d0.00b8.14c8
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Aging Time 300
Interface Role Sts Cost Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4 Desg FWD 200000 128.196 P2p
Fa4/5 Back BLK 200000 128.197 P2p
Router#
```

Table 0-97 describes the fields that are shown in the example.

Table 0-97 show spanning-tree vlan Command Output Fields

Field	Definition
Role	Current 802.1w role; valid values are Boun (boundary), Desg (designated), Root, Altn (alternate), and Back (backup).
Sts	Spanning-tree states; valid values are BKN* (broken)[1], BLK (blocking), DWN (down), LTN (listening), LBK (loopback), LRN (learning), and FWD (forwarding).
Cost	Port cost.

Table 0-97 show spanning-tree vlan Command Output Fields (continued)

Field	Definition
Prio.Nbr	Port ID that consists of the port priority and the port number.
Status	Status information; valid values are as follows: • P2p/Shr—The interface is considered as a point-to-point (resp. shared) interface by the spanning tree. • Edge—PortFast has been configured (either globally using the **default** command or directly on the interface) and no BPDU has been received. • *ROOT_Inc, *LOOP_Inc, *PVID_Inc and *TYPE_Inc—The port is in a broken state (BKN*) for an inconsistency. The port would be (respectively) Root inconsistent, Loopguard inconsistent, PVID inconsistent, or Type inconsistent. • Bound(type)—When in MST mode, identifies the boundary ports and specifies the type of the neighbor (STP, RSTP, or PVST). • Peer(STP)—When in PVRST rapid-pvst mode, identifies the port connected to a previous version of the 802.1D bridge.

[1] For information on the *, see the definition for the Status field.

This example shows how to determine if any ports are in the root-inconsistent state:

```
Router#  show spanning-tree inconsistentports

Name                 Interface            Inconsistency
-------------------- -------------------- ------------------
 VLAN1               FastEthernet3/1      Root Inconsistent

Number of inconsistent ports (segments) in the system :1
Router#
```

Related Commands

Command	Description
spanning-tree backbonefast	Enables BackboneFast on all Ethernet VLANs.
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree guard	Enables or disables the guard mode.
spanning-tree pathcost method	Sets the default path-cost calculation method.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
spanning-tree portfast bpdufilter default	Enables BPDU filtering by default on all PortFast ports.
spanning-tree portfast bpduguard default	Enables BPDU guard by default on all PortFast ports.
spanning-tree port-priority	Sets an interface priority when two bridges vie for position as the root bridge.
spanning-tree uplinkfast	Enables UplinkFast.
spanning-tree vlan	Enables the Spanning Tree Protocol (STP) on a VLAN.

show stun

To display the current status of serial tunnel (STUN) connections, use the **show stun** command in privileged EXEC mode.

show stun [**group** *stun-group-number*] [**address** *address-list*]

Syntax Description

group *stun-group-number*	(Optional) STUN group number. Valid numbers are decimal integers in the range from 1 to 255.
address *address-list*	(Optional) List of poll addresses.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(11)T	The **group** and **address** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show stun** command:

```
Router# show stun

This peer: 10.108.10.1
Serial0 -- 3174 Controller for test lab (group 1 [sdlc])
                          state   rx-pkts  tx-pkts  drops  poll
  7[1] IF Serial1         open     20334    86440      5  8P
 10[1] TCP 10.108.8.1     open      6771     7331      0
all[1] TCP 10.108.8.1     open    612301  2338550   1005
```

In the display, the first entry reports proxy that polling is enabled for address 7 and that serial 0 is running with modulus 8 on the primary side of the link. The link has received 20,334 packets, sent 86,440 packets, and dropped 5 packets.

Table 98 describes the significant fields shown in the output.

Table 98 show stun Field Descriptions

Field	Description
This peer	Lists the peer name or address. The interface name (as defined by the **description** command), its STUN group number, and the protocol associated with the group are shown on the header line.
STUN address	Address or the word *all* if the default forwarding entry is specified, followed by a repeat of the group number given for the interface.

Table 98 show stun Field Descriptions (continued)

Field	Description
Type of link	Description of link, either a serial interface using serial transport (indicated by IF followed by interface name), or a TCP connection to a remote router (TCP followed by IP address).
state	State of the link: open is the normal, working state; direct indicates a direct link to another line, as specified with the **direct** keyword in the **stun route** command.
rx-pkts	Number of received packets.
tx-pkts	Number of sent packets.
drops	Number of packets that for whatever reason had to be dropped.
poll	Report of the proxy poll parameters, if any. P indicates a primary and S indicates a secondary node. The number before the letter is the modulus of the link.

show subscriber-policy

To display the details of a subscriber policy, use the **show subscriber-policy** command in user EXEC or privileged EXEC mode.

show subscriber-policy *range*

Syntax Description

range	Range of subscriber policy numbers (range 1 to 100).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show subscriber-policy** command:

```
Router# show subscriber-policy 1

ARP: Permit
Broadcast: Deny
Multicast: Permit
Unknown: Deny
STP: Disable
CDP: Disable
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.
bridge subscriber-policy	Binds a bridge group with a subscriber policy.
show bridge	Displays classes of entries in the bridge forwarding database.
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

shutdown (CMCC)

To shut down an interface or the virtual interface on the Cisco Mainframe Channel Connection (CMCC) adapter when the router is in interface configuration mode, use the **shutdown** command in interface configuration mode. The **shutdown** TN3270 server command also shuts down TN3270 entities, such as physical unit (PU), Dependent Logical Unit Requestor (DLUR), and DLUR service access point (SAP), depending on which configuration mode the router is in when the command is issued. To restart the interface or entity, use the **no** form of this command. The entity affected depends on the mode in which the command is issued.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

The interface or entity is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When using this command on a channel interface, the command applies to the entire CMCC adapter.

Examples

The following example issued in interface configuration mode shuts down the entire CMCC adapter:

```
shutdown
```

shutdown (TN3270)

To shut down TN3270 entities, such as physical unit (PU), Dependent Logical Unit Requestor (DLUR), and DLUR service access point (SAP), use the **shutdown** command in the appropriate TN3270 server command modes. To restart the interface or entity, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

The interface or entity is enabled.

Command Modes

TN3270 server configuration

PU configuration

DLUR configuration

DLUR PU configuration

DLUR SAP configuration

Listen-point configuration

Listen-point PU configuration

Command History

Release	Modification
10.2	This command was introduced.
11.2	Support was added for the following configuration modes: • TN3270 • PU • DLUR • DLUR SAP
11.2(18)BC	Support was added for the following configuration modes: • Listen-point • Listen-point PU
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **shutdown** TN3270 command shuts down the TN3270 entities according to which configuration mode the router is in when the command is issued.

- In TN3270 server configuration mode, the command shuts down the entire TN3270 server function.
- In PU configuration mode, the command shuts down an individual PU entity within the TN3270 server.
- In DLUR configuration mode, the command shuts down the whole DLUR subsystem within the TN3270 server.
- In DLUR PU configuration mode, the command shuts down an individual PU within the Systems Network Architecture (SNA) session switch configuration in the TN3270 server.
- In DLUR SAP configuration mode, the command shuts down the local SAP (LSAP) and its associated links within the SNA session switch configuration.

Examples

The following example issued in TN3270 server configuration mode shuts down the entire TN3270 server:

```
shutdown
```

sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI)

To enable Systems Network Architecture (SNA) on the interface, use the **sna enable-host** command in interface configuration mode. To disable SNA on the interface, use the **no** form of this command.

sna enable-host [**lsap** *lsap-address*]

no sna enable-host [**lsap** *lsap-address*]

Syntax Description

lsap	(Optional) Activate a local service access point (SAP) as an upstream SAP, for both receiving ConnectIn attempts and for starting ConnectOut attempts.
lsap-address	(Optional) The default is 12.

Defaults

The default LSAP parameter is 12.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables SNA on the interface and specifies that the local SAP (LSAP) 10 will be activated as an upstream SAP:

```
sna enable-host lsap 10
```

Related Commands

Command	Description
show sna	Displays the status of the SNA Service Point feature.
sna host (Frame Relay)	Defines a link to an SNA host over a Frame Relay connection.
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.

sna enable-host (QLLC)

To enable an X.121 subaddress for use by the Systems Network Architecture (SNA) Service Point feature on the interface, use the **sna enable-host** command in interface configuration mode. To disable SNA Service Point on the interface, use the **no** form of this command.

sna enable-host qllc *x121-subaddress*

no sna enable-host qllc *x121-subaddress*

Syntax Description

qllc	Required keyword for Qualified Logical Link Control (QLLC) data-link control.
x121-subaddress	X.121 subaddress.

Defaults

No default X.121 subaddress is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, X.121 subaddress 320108 is enabled for use by host connections:

```
sna enable-host qllc 320108
```

Related Commands

Command	Description
sna host (QLLC)	Defines a link to an SNA host over an X.25/QLLC connection.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.

sna enable-host (SDLC)

To enable a Synchronous Data Link Control (SDLC) address for use by host connections, use the **sna enable-host** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

sna enable-host sdlc *sdlc-address*

no sna enable-host sdlc *sdlc-address*

Syntax Description

sdlc	Required keyword for SDLC data-link control.
sdlc-address	SDLC address.

Defaults

No default SDLC address is specified.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, SDLC address C1 is enabled for use by host connections:

```
encapsulation sdlc
sdlc role secondary
sdlc address c1
sna enable-host sdlc c1
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
sna host (SDLC)	Defines a link to a Systems Network Architecture (SNA) host over an SDLC connection.

sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)

To define a link to a Systems Network Architecture (SNA) host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control connections, use the **sna host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna host *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no sna host *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	SNA host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
rmac *remote-mac*	MAC address of the remote host physical unit (PU).
rsap *remote-sap*	(Optional) Service access point (SAP) address of the remote host PU. The default is 4.
lsap *local-sap*	(Optional) local SAP (LSAP) address used by the SNA Service Point to establish connection with the remote host. The default is 12.
interface *slot/port*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with the remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between attempts to retry establishing connection with the remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Host link to be used for the focal point support.

Defaults

The default remote SAP is 4.
The default local SAP is 12.
The default window size is 7.
The default maximum I-frame size is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example defines a link to a Systems Network Architecture (SNA) host:

```
sna host CNM01 xid-snd 05d00001 rmac 4001.3745.1088 rsap 4 lsap 4 focalpoint
```

Related Commands

Command	Description
sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI)	Enables SNA on the interface.
sna rsrb enable-host	Enables an RSRB service access point (SAP) for use by the SNA Service Point feature.
sna rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by the host name through the RSRB.
sna start	Initiates a connection to a remote resource.
sna vdlc enable-host	Enables a SAP for use by the SNA Service Point feature.
sna vdlc start	Specifies that an attempt will be made to connect to the remote resource defined by the host name through virtual data-link control (VDLC).

sna host (Frame Relay)

To define a link to a Systems Network Architecture (SNA) host over a Frame Relay connection, use the **sna host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna host *host-name* **xid-snd** *xid* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no sna host *host-name* **xid-snd** *xid* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	Specified SNA host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
dlci *dlci-number*	Data-link connection identifier (DLCI) number.
rsap *remote-sap*	(Optional) Service access point (SAP) address of the remote host physical unit (PU). The default is 4.
lsap *local-sap*	(Optional) local SAP (LSAP) address used by the SNA Service Point to establish connection with the remote host. The default is 12.
interface *slot/port*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with the remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between attempts to retry establishing connection with the remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Host link to be used for the focal point support.

Defaults

The default remote SAP is 4.
The default local SAP is 12.
The default window size is 7.
The default maximum I-frame size is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example defines a link to a Systems Network Architecture (SNA) host:

```
sna host CNM01 xid-snd 05d00001 dlci 200 rsap 4 lsap 4
```

Related Commands

Command	Description
sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI)	Enables SNA on the interface.
sna start	Initiates a connection to a remote resource.

sna host (QLLC)

To define a link to a Systems Network Architecture (SNA) host over an X.25 or Qualified Logical Link Control (QLLC) connection, use the **sna host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna host *host-name* **xid-snd** *xid* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no sna host *host-name* **xid-snd** *xid* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**interface** *slot/port]* [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	SNA host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
x25 *remote-x121-addr*	Synchronous Data Link Control (SDLC) address.
qllc *local-x121-subaddr*	(Optional) Service access point (SAP) address of the remote host physical unit (PU). The default is 4.
interface *slot/port*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with the remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between attempts to retry establishing connection with the remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Host link to be used for the focal point support.

Defaults

The default remote SAP is 4.
The default window size is 7.
The default maximum I-frame size is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example defines a link to a Systems Network Architecture (SNA) host:

```
sna host MLM1 xid-snd 05d00001 x25 320108 qllc 08
```

Related Commands

Command	Description
sna enable-host (QLLC)	Enables an X.121 subaddress for use by the SNA Service Point feature on the interface.
sna start	Initiates a connection to a remote resource.

sna host (SDLC)

To define a link to a Systems Network Architecture (SNA) host over an Synchronous Data Link Control (SDLC) connection, use the **sna host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna host *host-name* **xid-snd** *xid* **sdlc** *sdlc-addr* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no sna host *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	SNA host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
sdlc *sdlc-addr*	SDLC address.
rsap *remote-sap*	(Optional) Service access point (SAP) address of the remote host physical unit (PU). The default is 4.
lsap *local-sap*	(Optional) local SAP (LSAP) address used by the SNA Service Point to establish connection with the remote host. The default is 12.
interface *slot/port*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with the remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between attempts to retry establishing connection with the remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Host link to be used for the focal point support.

Defaults

The default remote SAP is 4.
The default local SAP is 12.
The default window size is 7.
The default maximum I-frame size is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example defines a link to a Systems Network Architecture (SNA) host:

```
sna host CNM01 xid-snd 05d00001 sdlc c1 rsap 4 lsap 4 focalpoint
```

Related Commands

Command	Description
sna enable-host (SDLC)	Enables an Synchronous Data Link Control (SDLC) address for use by host connections.
sna start	Initiates a connection to a remote resource.

sna rsrb

To specify the entities that the Systems Network Architecture (SNA) feature will simulate at the remote source-route bridge (RSRB), use the **sna rsrb** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

sna rsrb *local-virtual-ring bridge-number target-virtual-ring virtual-macaddr*

no sna rsrb *local-virtual-ring bridge-number target-virtual-ring virtual-macaddr*

Syntax Description

local-virtual-ring	Local virtual ring number.
bridge-number	Virtual bridge number. The valid range is from 1 to 15.
target-virtual-ring	Target virtual ring number.
virtual-macaddr	Virtual MAC address.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can specify the bridge number no more than once in any configuration.

Examples

The following example identifies a LAN:

```
sna rsrb 88 1 99 4000.FFFF.0001
```

Related Commands

Command	Description
sna rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by the host name through the remote source-route bridging (RSRB).

sna rsrb enable-host

To enable an remote source-route bridging (RSRB) service access point (SAP) for use by the Systems Network Architecture (SNA) Service Point feature, use the **sna rsrb enable-host** command in global configuration mode. To disable the RSRB SAP, use the **no** form of this command.

sna rsrb enable-host [**lsap** *local-sap*]

no sna rsrb enable-host [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP (LSAP) address will be activated as an upstream SAP for both receiving incoming connections attempts and for starting outgoing connection attempts. The default is 12.

Defaults

The default local SAP address is 12.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the local SAP address 10 of the RSRB is enabled for use by the ibm3745 host physical unit (PU):

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

sna rsrb 88 1 99 4000.FFFF.0001
sna rsrb enable-host lsap 10

sna host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections.

sna rsrb start

To specify that an attempt will be made to connect to the remote resource defined by the host name through the remote source-route bridging (RSRB), use the **sna rsrb start** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna rsrb start *host-name*

no sna rsrb start *host-name*

Syntax Description

host-name	The name of a host defined in an **sna host** or equivalent command.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before issuing this command, you must enable the correct local service access point (SAP) with the appropriate enable command (**sna rsrb enable-host**).

Examples

In the following example, the Systems Network Architecture (SNA) Service Point will initiate a connection with the ibm3745 host physical unit (PU) across the RSRB link:

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

sna rsrb 88 1 99 4000.FFFF.0001
sna rsrb enable-host lsap 10

sna host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10
sna rsrb start ibm3745

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
sna rsrb	Specifies the entities that the SNA feature will simulate at the RSRB.

sna start

To initiate a connection to a remote resource, use the **sna start** command in interface configuration mode. To cancel the connection attempt, use the **no** form of this command.

sna start [*resource-name*]

no sna start [*resource-name*]

Syntax Description

resource-name	(Optional) Name of a host defined in an **sna host** command.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before issuing this command, you must enable the correct address using the **sna enable-host** command.

Examples

The following example initiates a connection to CNM01:

```
sna start CNM01
```

Related Commands

Command	Description
sna host (Frame Relay)	Defines a link to a Systems Network Architecture (SNA) host over a Frame Relay connection.
sna host (QLLC)	Defines a link to an SNA host over an X.25 or Qualified Logical Link Control (QLLC) connection.
sna host (SDLC)	Defines a link to an SNA host over an Synchronous Data Link Control (SDLC) connection.
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.

sna vdlc

To identify the local virtual ring and virtual MAC address that will be used to establish Systems Network Architecture (SNA) host connections over data-link switching plus (DLSw+) using virtual data-link control, use the **sna vdlc** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna vdlc *ring-group virtual-mac-address*

no sna vdlc *ring-group virtual-mac-address*

Syntax Description

ring-group	Local virtual ring number identifying the source-route bridging (SRB) ring group.
virtual-mac-address	Virtual MAC address that represents the SNA virtual data-link control.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The virtual data-link control local virtual ring must have been previously configured using the **source-bridge ring-group** command.

The virtual data-link control virtual MAC address must be unique within the DLSw+ network.

To avoid an address conflict on the virtual MAC address, use a locally administered address in the form 4000.*xxxx.xxxx*.

Examples

The following is an example of an SNA Service Point configuration that uses virtual data-link control over DLSw+:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

sna vdlc 99 4000.4500.01f0
sna vdlc enable-host lsap 12

sna host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint
sna vdlc start HOST-B

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
dlsw local-peer	Defines the parameters of the DLSw+ local peer.
dlsw remote-peer tcp	Identifies the IP address of a peer with which to exchange traffic using TCP.
sna vdlc start	Specifies that an attempt will be made to connect to the remote resource defined by the host name through virtual data-link control (VDLC).
source-bridge ring-group	Defines or removes a ring group from the configuration.

sna vdlc enable-host

To enable a service access point (SAP) for use by the Systems Network Architecture (SNA) Service Point feature, use the **sna vdlc enable-host** command in global configuration mode. To disable the SAP, use the **no** form of this command.

sna vdlc enable-host [**lsap** *local-sap*]

no sna vdlc enable-host [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP (LSAP) address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts. The default is 12.

Defaults

The default local SAP address is 12.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the local SAP address 12 is enabled for use by the host physical unit (PU) HOST-B:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

sna vdlc 99 4000.4500.01f0
sna vdlc enable-host lsap 12

sna host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint

sna vdlc start HOST-B

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.

sna vdlc start

To specify that an attempt will be made to connect to the remote resource defined by the host name through virtual data-link control (VDLC), use the **sna vdlc start** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna vdlc start *host-name*

no sna vdlc start *host-name*

Syntax Description

host-name	The name of a host defined in an **sna host** or equivalent command.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before issuing this command, you must enable the correct local service access point (SAP) with the **sna vdlc enable-host** command.

Examples

In the following example, the Systems Network Architecture (SNA) Service Point feature uses virtual data-link control to initiate a connection with the host physical unit (PU) HOST-B:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

sna vdlc 99 4000.4500.01f0
sna vdlc enable-host lsap 12

sna host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint

sna vdlc start HOST-B

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
sna vdlc	Identifies the local virtual ring and virtual MAC address that will be used to establish SNA host connections over data-link switching plus (DLSw+) using VDLC.

snasw cpname

To define a control point (CP) name for SNASw, use the **snasw cpname** command in global configuration mode. To deactivate SNASw and remove the CP definition, use the **no** form of this command.

snasw cpname {*netid.cpname* | *netid* [*hostname* | **ip-address** *interface-name*]} [**hung-pu-awareness** *timer-value*] [**hung-session-awareness** *timer-value*] [**locate-timeout** *timeout-value*] [**max-pacing-window** *max-value*] [**remove-rscvs**] [**station-segmentation**]

no snasw cpname

Syntax Description

netid.cpname	Fully qualified CP name for this node, consisting of both network ID and CP name.
netid	Partial CP name, which consists of only a network ID. If this option is selected, you must also configure the hostname or IP address operands to complete the fully qualified CP name.
hostname	(Optional) Indicates a CP name that is defined by using the hostname which is configured on the router. When configuring this operand, code a *netid* only. The last eight characters of the hostname are used to complete the CP name.
ip-address *interface-name*	(Optional) Indicates the CP name that is defined by deriving the CP name from the IP address on the interface that is indicated in the *interface-name*. When configured, this operand requires a *netid* operand. In addition, a portion of the CP name can be configured. The remaining characters of the CP name that are not configured are generated from the IP address that is indicated. The generated characters are derived from a hexadecimal format of the IP address for the interface that is specified.
hung-pu-awareness *timer-value*	(Optional) Indicates the interval at which Dependent Logical Unit Requestor (DLUR) supported physical units (PUs) are checked to see if they are hung in a pending activate PU state. If a PU is in this state for two consecutive iterations of this timer, then the PU is considered hung. No attempt is made to recover the hung PU, but for diagnostic purposes message DLUR_LOG_23 (A REQACTPU RSP has not been received. Possible hung PU problem) is written to the problem determination log. If the PU later becomes activated, message DLUR_LOG_24 (A PU previously logged as possibly hung is no longer possibly hung) is issued. The valid range is from 5 to 65535 seconds. If this keyword is not specified, the default timer-value is 300 seconds.
hung-session-awareness *timer-value*	(Optional) Indicates the length of time when a new intermediate session that is still in a non-active state is considered hung. No attempt is made to clean up the hung session, but for diagnostic purposes message SCM_LOG_16 (Slow session activation detected) is issued. The valid range is from 5 to 65535 seconds. If this keyword is not specified, the default timer-value is 180 seconds.

locate-timeout *timeout-value*	(Optional) Indicates the time when an Advanced Peer to Peer Networking (APPN) Locate Search message is considered lost and is cleaned up. This will likely result in the failure of the session for which the Locate Search message was sent. When this condition occurs message DS_LOG_18 (Locate search timed out) is issued. The valid range is from 0 to 65535 seconds. A value of 0 indicates that no timeout occurs. A value from 1 to 29 seconds is rounded up to 30 seconds. If this keyword is not specified the default timeout-value is 540 seconds.
max-pacing-window *max-value*	(Optional) Indicates the upper limit of the Receive Pacing window size for intermediate sessions. When variable pacing is used, the Receive Pacing window size will not exceed this value. It may be necessary to configure a small Receive Pacing window size (such as 7) to improve performance when both batch and interactive traffic share the same network. The valid range is from 7 to 65535. If a value is not specified, the default is 64.
remove-rscvs	(Optional) Indicates that Route Selection Control Vectors (RSCVs) will be removed from incoming BINDs that are received from an upstream node before forwarding the BINDs downstream. Removing RSCVs from BINDs enables a downstream network node (NN) that is connected over a low entry networking (LEN) link to receive the BINDs and forward them to the destination node.
station-segmentation	(Optional) Sends all segments (for example, FIS, MIS, and LIS) to a particular LU before sending segments to another LU, which prevents PU 2.0 devices (that do not support segment interleaving) from generating sense code 80070000. Use this keyword for XID0 devices.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.1	The **station-segmentation** and **max-pacing-window** keywords were added.
12.2	The **remove-rscvs** keyword was added.
12.3	The **hung-pu-awareness**, **hung-session-awareness**, and **locate-timeout** keywords were added.
12.4	Support was added to **hung-pu-awareness**, **hung-session-awareness**, and **locate-timeout** keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can also deactivate SNASw without removing the **snasw cpname** definition by using the **snasw stop** privileged EXEC command which enables you to stop and restart SNASw without losing the SNASw configuration. If you use **no snasw cpname**, all SNASw configuration commands that were entered will be lost.

Coding a CP name is required for SNASw. Only one **snasw cpname** command is allowed at a time. You cannot change the **snasw cpname** command without first deleting the previous definition by using the **no** form of the command. If SNASw is active, the **no** form deactivates it. If SNASw is inactive, using **snasw cpname** activates it.

Examples

The following are examples of how to configure the **snasw cpname** command:

```
snasw cpname NETA.BRANCH5
snasw cpname NETBANK2.DLUR0005
snasw cpname NETWORKA hostname
snasw cpname NETA.CP ip-address Loopback0
```

snasw dlcfilter

To filter the frames that arrive and leave System Network Architecture Switching Services (SNASw), use the **snasw dlcfilter** command in global configuration mode. To disable the filtering of frames, use the **no** form of this command.

snasw dlcfilter [**link** *link-name* [**session** *session-address*]] [**port** *port-name*] [**rmac** *mac-address-value* [**session** *session-address*]] [**rtp** *rtp-name* [**session** *session-address*]] [**type** [**cls**] [**hpr-cntl**] [**hpr-data**] [**isr**] [**xid**]]

no snasw dlcfilter

Syntax Description

link *link-name*	(Optional) Specifies the link name upon which the data-link control (DLC) trace is filtered (one to eight characters). All incoming and outgoing frames that match this link are traced.
session *session-address*	(Optional) Specifies the session address that needs to be filtered. The *session-address* argument must be in the 3-byte hexadecimal format (0-FFFFFFFF).
port *port-name*	(Optional) Specifies the port name upon which the port is filtered (one to eight characters). All incoming and outgoing frames that match this port are traced.
rmac *mac-address-value*	(Optional) Specifies the MAC address, in non-canonical format, upon which the DLC trace is filtered. All incoming and outgoing frames that match this MAC address are traced.
rtp *rtp-name*	(Optional) Specifies the RealTime Transport Protocol (RTP) name upon which RTP is filtered (one to eight characters). All incoming and outgoing frames that match this RTP connection name are traced.
type	(Optional) Indicates that one or more frame type filters follow.
cls	(Optional) Indicates that commands to the local DLC are traced.
hpr-cntl	(Optional) Indicates that the High-Performance Routing (HPR) format identifier 5 (FID5), which does not carry a Systems Network Architecture (SNA) data payload, is traced.
hpr-data	(Optional) Indicates that the HPR format identifier 5 (FID5), which carries an SNA data payload, is traced.
isr	(Optional) Indicates that the SNA and Advanced Peer-to-Peer Networking (APPN) format identifier 2 (FID2) is traced.
xid	(Optional) Indicates that the exchange identification (XID) frames are traced.

Command Default

This command defaults to no filtering, and all frames are traced.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **snasw dlcfilter** command is used to limit the output of the **snasw dlctrace** command to a manageable amount of trace data. Running the **snasw dlctrace** command consumes CPU and memory. Using the **snasw dlcfilter** command limits the CPU and memory consumption to only the frames that are targeted for tracing.

Up to four different types of filters can be in place at once. If the type filter is coded, the frame will pass the type filter and any of the matching filters, that are coded to be included in the trace.

Examples

The following example shows how to configure the **snasw dlcfilter** command by adding a link to the dlcfilter list, adding a remote MAC address to the dlcfilter list, and filtering the dlctrace on frames of type XID:

```
Router(config)# snasw dlcfilter link cmc1link
Router(config)# snasw dlcfilter rmac 4001.1234.1001
Router(config)# snasw dlcfilter type xid
```

Related Commands

Command	Description
debug snasw dlc	Displays real-time DLC trace data to the console.
snasw dlctrace	Traces the frames arriving and leaving SNASw.
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.
snasw start	Starts SNASw.
snasw stop	Shuts down SNASw.

snasw dlctrace

To trace frames arriving and leaving Switching Services (SNASw), use the **snasw dlctrace** command in global configuration mode. To deactivate the capture of frame data and free the storage buffer used to capture the data, use the **no** form of this command.

snasw dlctrace [**buffer-size** *buffer-size-value*] [**file** *filename* [**timestamp**]] [**frame-size** *frame-size-value* | **auto-terse**] [**format** [**brief** | **detail** | **analyzer**]] [**nostart**]

no snasw dlctrace

Syntax Description

buffer-size *buffer-size-value*	(Optional) Specifies the size (in kilobytes) of the data-link control (DLC) trace buffer requested. The minimum buffer size is 100, and the maximum is 64000.
file *filename*	(Optional) Specifies the filename for the DLC trace buffer file when this file is written to the file server. Use the following format: protocol://host/path/filename. If the output file size exceeds 32MB, the first 32MB will be in the file with the name *filename*, the next 32MB will be in the file with the name *filename*.01, and so on. Note that with formatting, the output may be of different size than the buffer-size.
timestamp	(Optional) Appends the current date and time to the end of the file when it is dumped.
frame-size *frame-size-value*	(Optional) Indicates the size of the frame that is traced within the DLC trace. All data beyond the size value is truncated and is not included in the trace. The default is that the entire frame is traced.
auto-terse	(Optional) Indicates that logical unit (LU)-LU and system services control points (SSCP)-LU session data frames should be truncated after the Systems Network Architecture (SNA) request/response (RH). Also truncates NMVTs on the SSCP-physical unit (PU) session. Control frames (for example, exchange identification [XID], BIND, Activate Physical Unit [ACTPU]) are traced in their entirety.
format	(Optional) Indicates the format the DLC trace is written to when writing to a file server. Valid values are **brief**, **detail**, and **analyzer**:
brief	(Optional) Indicates that a text file is written with a one-line-per-frame summary for each frame.
detail	(Optional) Indicates that a text file is written with a frame summary line followed by a complete hexadecimal dump of the frame.
analyzer	(Optional) Indicates a binary file is generated that is readable by several popular network analyzer products. This format uses the Network Associates Sniffer file format.
nostart	(Optional) Indicates that the specified trace is not to be started when the subsystem is started.

Defaults

Tracing is off.
If a value for the *buffer-size-value* argument is not specified, then the default is 500, creating a 500-KB buffer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.3	The maximum allowed value of the *buffer-size-value* argument was increased to 6400.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw dlctrace** command when directed by service personnel or when analysis of frame data entering and leaving SNASw is necessary.

The **snasw dlctrace** command copies frames into a memory buffer, which can degrade router performance. Therefore, care should be taken when using this command. When issued on a highly used system, the **snasw dlcfilter** command should be used in conjunction with the **snasw dlctrace** command to limit the output of the trace.

Use the **snasw dump** command to dump the trace data to a file server or the **show snasw dlctrace** command to display captured frames on the console.

When the analyzer format is used, portions of the frame are reconstructed from their actual representation on the data link. Because of this format, portions of the data in the header portion of the frame are modified. Specifically, if Routing Information Field (RIF) data was present on the actual data-link frame, that information is omitted in the dlctrace. In addition, information in the Logical Link Control (LLC) header (for example, Nr, Ns counts) is not reliably transferred to the traced frame. However, the remainder of the frame, including all Systems Network Architecture (SNA) content, is a reliable representation of the frame as it appeared on the actual upstream or downstream link.

Examples

The following are examples of how to configure the **snasw dlctrace** command:

```
snasw dlctrace
snasw dlctrace buffer-size 5000 file tftp://10.69.120.21/dlcfiles/dlc/trc
```

Related Commands

Command	Description
show snasw dlctrace	Displays the captured DLC trace information on the console.
snasw dlcfilter	Filters frames being captured.
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.

snasw dlus

To specify parameters related to Dependent Logical Unit Requestor (DLUR) or Dependent Logical Unit Server (DLUS) functionality, use the **snasw dlus** command in global configuration mode. To remove the data specified in a previous **snasw dlus** command, use the **no** form of this command.

snasw dlus *primary-dlus-name* [**backup** *backup-dlus-name*] [**prefer-active**] [**retry** *interval count*] [**once**]

no snasw dlus

Syntax Description

primary-dlus-name	Specifies the fully qualified name of the primary DLUS (3 to 17 characters).
backup *backup-dlus-name*	(Optional) Indicates configuration of a backup DLUS. A backup DLUS is used when the primary DLUS is unreachable or cannot service a specific downstream device. The fully qualified name of the backup DLUS is 3 to 17 characters in length.
prefer-active	(Optional) Indicates that if an active DLUR or DLUS connection was established, an incoming physical unit (PU) will retry exclusively on the active DLUS connection and will not attempt to connect to a different DLUS.
retry *interval count*	(Optional) Indicates that the DLUR retry parameters follow this statement. The *interval* argument indicates the time period between attempts to connect a DLUS if one is not serving a specific PU. The *count* argument indicates the number of times the current or primary DLUS is retried before an attempt is made to connect to a backup or inactive DLUS.
once	(Optional) Instructs the DLUR to attempt only one retry cycle (with primary and backup (if configured) DLUS, according to either the default retry values or to the retry values specified by the **retry** keyword) to request DLUS services. If the service requests are not answered, the downstream link will be disconnected.

Defaults

If the **prefer-active** keyword is not specified, each connected downstream station will attempt to connect to the primary DLUS or backup DLUS until the device receives DLUS services.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only one **snasw dlus** command is allowed at a time. The **snasw dlus** command cannot be changed without first deleting the previous definition using the **no** form of the command.

The **prefer-active** keyword supersedes the **once** keyword, which means that if the **prefer-active** keyword is configured and there is an active DLUS, then all DLUS services requests will be negotiated only with the active DLUS. The DLUR will not send DLUS service requests to other DLUSs. In this situation, the **once** keyword has no effect.

Examples

The following are examples of how to configure the **snasw dlus** command:

```
snasw dlus NETA.HOST1 backup NETA.HOST2
```

snasw dlus NETBANK2.CDERM34 prefer-active retry 30 3

snasw dump

To copy problem determination logs and traces from internal buffers to an external file server, use the **snasw dump** command in privileged EXEC mode.

snasw dump {**all** | **dlctrace** | **ipstrace** | **summary-ipstrace** | **pdlog**}

Syntax Description

all	Indicates that all configured trace and problem determination buffers should be transferred. The **file** keyword must be configured on the enabling configuration command for the buffers to be dumped. Traces that run but do not have the (See the "Usage Guidelines Section.) **file** keyword coded are not transferred.
dlctrace	Indicates that the data-link control (DLC) trace buffer is transferred to a file server. If **file** keyword is configured on the **snasw dlctrace** command, the URL specified is used for transferring the DLC trace file. If **file** keyword is not configured on the **snasw dlctrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and filename for the transferred file.
ipstrace	Indicates that the InterProcess Signal (IPS) trace buffer is transferred to a file server. If the **file** is configured on the **snasw ipstrace** command, the URL specified is used for transferring the ipstrace file. If **file** keyword is not configured on the **snasw ipstrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and filename for the transferred file.
summary-ipstrace	Indicates that the summary IPS trace buffer is transferred to a file server. If the **file** keyword is coded on the **snasw summary-ipstrace** command, the URL specified is used for transferring the summary ipstrace file. If the **file** keyword is not coded on the **snasw ipstrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and filename for the transferred file.
pdlog	Indicates that the problem determination log buffer is transferred to a file server. If the **file** keyword is coded on the **snasw pdlog** command, the URL specified is used for transferring the pdlog file. If the **file** keyword is not coded, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and filename for the transferred file.

Command Modes

Privileged EXEC

Defaults

No default behavior or values

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **snasw dump** command is used for gathering trace files for diagnosis by Cisco personnel or onsite trace analysis.

TFTP can handle files up to 16 Mb in size. If you are transferring a file larger than 16 Mb, do not use TFTP. Instead, use FTP or some other file transfer method. To change the transmission protocol, use the **file** keyword with the **snasw trace** or **snasw dlctrace** global configuration command.

Before you use FTP, make sure you configure the **ip ftp username** and **ip ftp password** command to a valid user and password on the system to which the file is being sent.

Examples

The following are examples of how to enter the **snasw dump** command:

```
Router# snasw dump all
Router# snasw dump dlctrace
```

Related Commands

Command	Description
snasw dlctrace	Traces frames arriving and leaving Switching Services (SNASw).
snasw ipstrace	Sets up a trace buffer and begins tracing IPS trace elements.
snasw pdlog	Controls message logging to the console and the Systems Network Architecture (SNA) problem determination log cyclic buffer.

snasw event

To indicate which normal events are logged to the console, use the **snasw event** command in global configuration mode. To return the events to their default state, use the **no** form of this command.

snasw event [**cpcp**] [**dlc**] [**implicit-ls**] [**port**]

no snasw event

Syntax Description

cpcp	(Optional) Indicates that an event is issued for control point (CP). The CP session state changes.
dlc	(Optional) Indicates data-link control (DLC) state changes.
implicit-ls	(Optional) Indicates state change on implicit links, including connection network links.
port	(Optional) Indicates that an event is issued for port state changes.

Defaults

By default, only defined links and Dependent Logical Unit Server (DLUS) events are sent to the pdlog or console.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.1(6)	The **defined-ls** keyword was deleted.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure the **snasw event** command:

```
snasw event implicit-ls
```

snasw ip-precedence

To define IP type of service (ToS) precedence settings to be mapped to Advanced Peer-to-Peer Networking (APPN) priorities, use the **snasw ip-precedence** command in global configuration mode. To remove the precedence settings, use the **no** form of this command.

snasw ip-precedence link *link-setting* **network** *network-setting* **high** *high-setting* **medium** *medium-setting* **low** *low-setting*

no snasw ip-precedence link *link-setting* **network** *network-setting* **high** *high-setting* **medium** *medium-setting* **low** *low-setting*

Syntax Description

link *link-setting*	ToS precedence setting (0–7) mapped to link control (LDLC) priority.
network *network-setting*	ToS precedence setting (0–7) mapped to network priority.
high *high-setting*	ToS precedence setting (0–7) mapped to high priority.
medium *medium-setting*	ToS precedence setting (0–7) mapped to medium priority.
low *low-setting*	ToS precedence setting (0–7) mapped to low priority.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is an example of how to configure the **snasw ip-precedence** command:

```
snasw ip-precedence link 7 network 7 high 7 medium 7 low 7
```

snasw ipsfilter

To filter interprocess signal trace elements being traced using the **snasw ipstrace** or **debug snasw ips** command, use the **snasw ipsfilter** command in global configuration mode. To remove all filtering, use the **no** form of this command.

snasw ipsfilter [**as**] [**asm**] [**bm**] [**ch**] [**cpc**] [**cs**] [**di**] [**dlc**] [**dma**] [**dr**] [**ds**] [**es**] [**ha**] [**hpr**] [**hs**] [**lm**] [**mds**] [**ms**] [**nof**] [**pc**] [**ps**] [**pu**] [**px**] [**rm**] [**rtp**] [**ru**] [**scm**] [**sco**] [**sm**] [**spc**] [**ss**] [**trs**]

no snasw ipsfilter

Syntax Description

as	(Optional) Specifies a filter on the Address Space component.
asm	(Optional) Specifies a filter on the Address Space Manager component.
bm	(Optional) Specifies a filter on the Buffer Management component.
ch	(Optional) Specifies a filter on the Channel component.
cpc	(Optional) Specifies a filter on the CPI-C component.
cs	(Optional) Specifies a filter on the Configuration Services component.
di	(Optional) Specifies a filter on the Defect Indication component.
dlc	(Optional) Specifies a filter on the Data Link Control component.
dma	(Optional) Specifies a filter on the Direct Memory Access component.
dr	(Optional) Specifies a filter on the Dependent logical unit (LU) Requester component.
ds	(Optional) Specifies a filter on the Directory Services component.
es	(Optional) Specifies a filter on the End System component.
ha	(Optional) Specifies a filter on the High Availability component.
hpr	(Optional) Specifies a filter on the High-Performance Routing component.
hs	(Optional) Specifies a filter on the Half Session component.
lm	(Optional) Specifies a filter on the LU Manager component.
mds	(Optional) Specifies a filter on the Management Data Stream component.
ms	(Optional) Specifies a filter on the Management Services component.
nof	(Optional) Specifies a filter on the Node Operator Facility component.
pc	(Optional) Specifies a filter on the Path Control component.
ps	(Optional) Specifies a filter on the Presentation Services component.
pu	(Optional) Specifies a filter on the physical unit (PU) Manager component.
px	(Optional) Specifies a filter on the PU Concentration component.
rm	(Optional) Specifies a filter on the Resource Manager component.
rtp	(Optional) Specifies a filter on the Rapid Transport Protocol component
ru	(Optional) Specifies a filter on the Request Unit Interface component.
scm	(Optional) Specifies a filter on the Session Connect Manager component.
sco	(Optional) Specifies a filter on the Session Connector component.
sm	(Optional) Specifies a filter on the Session Manager component.
spc	(Optional) Specifies a filter on the Serial Protocol Channel component.
ss	(Optional) Specifies a filter on the Session Services component.
trs	(Optional) Specifies a filter on the Topology Routing Services component.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The command defaults to no InterProcess Signal (IPS) trace filtering.

Examples

The following is an example of how to configure the **snasw ipsfilter** command:

```
snasw ipsfilter ds ss
```

Related Commands

Command	Description
show snasw ipstrace	Displays the interprocess signal trace on the router console.
snasw ipstrace	Sets up a trace buffer and begins tracing IPS trace elements.
debug snasw ips	Displays realtime ipstrace information to the console.

snasw ipstrace

To set up a trace buffer and begin tracing InterProcess Signal (IPS) trace elements, use the **snasw ipstrace** command in global configuration mode. To turn off the capture of trace elements and to free the trace buffer, use the **no** form of this command.

snasw ipstrace [**buffer-size** *buffer-size-value*] [**file** *filename* **timestamp**]

no snasw ipstrace

Syntax Description

buffer-size *buffer-size-value*	(Optional) Indicates that this trace command controls the size of the buffer used for storing ipstrace elements (in kilobytes). The default is 500 KB. The minimum buffer size is 10 KB; the maximum size is 64000 KB.
file *filename*	(Optional) Specifies the filename for the IPS trace buffer file when this file is written to the server. If the output file size exceeds 32MB, the first 32MB will be in the file with the name *filename*, the next 32MB will be in the file with the name *filename*.01, and so on. Note that with formatting, the output may be of different size than the buffer-size.
timestamp	(Optional) Appends the current date and time to the end of the file when it is dumped.

Defaults

This command defaults to no tracing with no cyclic buffer allocated.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.3	The maximum allowed value of the *buffer-size-value* argument was increased to 6400.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw ipstrace** command when directed by Switching Services (SNASw) personnel.

The **snasw ipstrace** command copies frames into a memory buffer, which can affect router performance. Therefore, care should be taken when using this command.

The ipstrace information is stored in a cyclic buffer allocated out of main processor memory. Use the **snasw dump** command to dump the binary trace information to a file server or the **show snasw ipstrace** command to display captured IPS trace information to the console. The IPS trace is a low-level internal trace.

Examples

The following is an example of how to configure the **snasw ipstrace** command:

```
snasw ipstrace buffer-size 1000 file tftp://myhost/path/file
```

Related Commands

Command	Description
show snasw ipstrace	Displays interprocess signal trace on the router console.
snasw ipsfilter	Filters interprocess signal trace elements being traced using the **snasw ipstrace** or **debug snasw ips** commands.
debug snasw ips	Displays realtime IPS trace information to the console.

snasw link

To configure upstream links, use the **snasw link** command in global configuration mode. To remove the configuration of upstream links, use the **no** form of this command.

snasw link *linkname* **port** *portname* **rmac** *mac-address* | **host-dest** *v4-or-v6-hostname* | **ip-dest** *ip-address* [**rsap** *sap-value*] [**nns**] [**tgp** [**high** | **low** | **medium** | **secure**]] [**nostart**]

no snasw link *linkname*

Syntax Description

linkname	Indicates the one-to-eight character local name for this link. This name is used to identify the link in **show** and privileged EXEC commands.
port *portname*	Specifies the Switching Services (SNASw) port from which this link will connect.
rmac *mac-address*	Specifies the 48-bit MAC address of the destination station. Either this keyword or the **ip-dest** keyword is required. remote MAC (RMAC) is required for all links associated with ports that are not High-Performance Routing (HPR) or IP ports.
host-dest *v4-or-v6-hostname*	Specifies the hostname that resolves to the IPv4 or IPv6 address of the destination station. Either the **host-dest** or **ip-dest** keyword is required for all links that are associated with HPR over IP ports. The *v4-or-v6-hostname* keyword can be between 1 and 64 characters in length.
ip-dest *ip-address*	Indicates the IP address or Domain Name System (DNS) name of the destination stations. Either this keyword or the **rmac** keyword is required. For all links associated with HPR or IP ports, the **ip-dest** keyword is required.
rsap *sap-value*	(Optional) Indicates the destination service access point (SAP) value, which defaults to 4.
nns	(Optional) Configures the adjacent Control Point (CP) as a preferred Network Node Server (NNS). You can specify the **nns** keyword on more than one link to identify multiple preferred NNSs.
tgp	(Optional) Configures a Transmission Group (TG) characteristic profile for route calculation. All SNASw TGs have the following characteristics in common: • Capacity = 16 megabits per second • Propagation delay = 384 microseconds • User parameter 1 = 128 • User parameter 2 = 128 • User parameter 3 = 128 However, you can adjust the connect cost, byte cost, and security TG characteristics. Valid values are **high**, **low**, **medium**, and **secure**.
high	(Optional) Prefers this link over links with a TG profile of **medium** or **low**. With this TG profile you can have the following TG characteristics: • Connect cost = 0 • Byte cost = 0 Security = Nonsecure

low	(Optional) Prefers this link when links with a TG profile of **high** or **medium** are not available. With this TG profile you can have the following TG characteristics: • Connect cost = 255 • Byte cost = 255 Security = Nonsecure
medium	(Optional) Prefers this link when links with a TG profile of **high** are not available. With this TG profile you can have the following TG characteristics: • Connect cost = 196 • Byte cost = 196 Security = Nonsecure
secure	(Optional) Prefers this link when a secure TG is required by the APPN class-of-service in use. With this TG profile you can have the following TG characteristics: • Connect cost = 196 • Byte cost = 196 Security = Secure public switched network
nostart	(Optional) Indicates that the link will not start automatically when defined.

Defaults

The destination SAP value defaults to 4.

The default TG characteristic profile is medium and nonsecure.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.3(14)T	The **host-dest** keyword was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw link** command to configure upstream connections to SNA data hosts, services, and DLUS nodes. Do not use this command to establish downstream connections to client workstations and devices that are serviced by the SNA switch. Configure client workstations and devices to connect into the SNA switch by configuring an outbound connection on these devices that specifies the MAC address of a port that is active on SNASw. SNASw then creates the downstream link dynamically when the workstation or device connects to SNASw.

If using the **ip-dest** keyword and using a DNS name instead of an IP address, the DNS name is resolved to an IP address at the time the definition is entered (or the time SNASw is started) and will remain resolved to that same address for the duration that SNASw is active. The DNS name is not resolved to an IP address each time the link is restarted.

If the link fails and SNASw switches to a non-preferred NNS (one without the **nns** keyword configured), SNASw will return CP-CP sessions to the preferred NNS when the NNS link becomes active again. Also, when the **nns** keyword is configured on a link, that link can be automatically restarted, even after the **snasw stop link** command is issued. See the **snasw stop link** command for details.

When using the **host-dest** keyword, the hostname must be resolved locally by either ip **ip host** or **ipv6 host** commands or by a Domain Name Server before the SNASw port is configured.

Examples

The following are examples of how to configure the **snasw link** command:

```
snasw link LINKCMC1 port TOKENO rmac 4000.333.4444 rsap 8
snasw link HOSTIP port HPRIP ip-dest 172.18.3.44
snasw link HOSTEE port HPRIP host-dest MVSOSA1
```

Related Commands

Command	Description
show snasw link	Shows the SNASw link objects.
snasw port	Specifies the DLCs used by SNASw.

snasw location

To configure the location of a resource, use the **snasw location** command in global configuration mode. To disable the location of a resource, use the **no** form of this command.

snasw location *resource-name* {**owning-cp** *cp-name* | **xid** *node-id*}

no snasw location *resource-name*

Syntax Description

resource-name	Indicates the fully qualified name of the resource for which location information is being configured. For name, 3 to 17 characters length is allowed.
owning-cp *cp-name*	Indicates the fully qualified control point (CP) name where the resource resides.
xid *node-id*	Specifies the Exchange identification (XID) of the node, where the specified resource resides. The *node-id* is specified in eight hexadecimal characters.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2	Support for wildcards was added in the *cpname* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **snasw location** command is typically used when a low-entry networking node (LEN) node link is established with a destination logical unit (LU). The **snasw location** command allows Switching Services (SNASw) to route session requests over the LEN node link to the resources named.

If the LEN node has a unique CP name configured, use the **owning-cp** keyword. Use the **xid** keyword when there is no CP name for the LEN node or conntype dyncplen is configured on the snasw port. The XID node-id of the LEN node must be unique for the location statement.

When a LEN node connects into an SNASw node, SNASw dynamically learns the CP name of the LEN and places it in its directory. In addition, SNASw dynamically learns the LU names of all LUs on the LEN that initiate independent sessions. Only define the location when an independent logical unit (ILU) on a LEN device is not sharing the node's CP name and does not initiate the first session. In all other cases, the LU's location will be learned dynamically.

The directory entry is created the next time the LEN node connects. If there is already a link to the LEN node active and you add a new SNASw location statement, it will not take effect until the next time the LEN CP connects.

Note Do not use the **snasw location** command to predefine the location of any resource that can be found dynamically using Advanced Peer-to-Peer Networking (APPN) searches (for example, resources on upstream APPN nodes or upstream or downstream ENs).

It is permissible to use the wildcard character "*" in location definitions to allow a definition to generate name associations for multiple devices. When the wildcard character is used for this purpose, the * symbol must be coded in both the *resource-name* and the *cpname* argument. If any real device attaches with a CP name that matches the non-wildcard portion of the **owning-cp** *cpname* keyword—argument pair specified, a location association will be made that replaces the wildcard characters of the CPname in the position of the *resource-name* argument. For example, if a definition **snasw location NETA.LU*01 owning-cp NETA.CP*** is coded and CP with the name NETA.CPABCD connects, then the resource name NETA.LUABCD01 will be defined to SNASw with owning-cp NETA.CPABCD.

You can also use the wildcard character "*" in location definitions to allow a specific device to connect under different CP names, but a single device cannot connect under multiple CP names at the same time. In this case, the * symbol must be used in only the *cpname* argument and not the *resource-name* argument. When the device connects with a CP name that matches the nonwildcard portion of the *cpname* argument, a corresponding location association will be made for the *resource-name* argument with that CP name.

Examples

The following example shows how to configure the location of a resource when the LEN node has CP name configured:

```
snasw location NETA.INDEPLU owning-cp NETA.LENHOSTA
```

Related Commands

Command	Description
show snasw directory	Displays the SNASw directory entries.

snasw lu62-security

To define a session-key or password with a partner logical unit (LU) or control point (CP), use the **snasw lu62-security** command in global configuration mode. To it, use the **no** form of this command.

snasw lu62-security *NETID.NAME* {**ascii** *char-string* | **hex** *hex-string*}

no snasw lu62-security *NETID.NAME*

Syntax Description

NETID.NAME	Fully qualified partner LU name.
ascii	Password/Session-key entered in ASCII string.
char-string	Character string (8 characters).
hex	Password/Session-key entered in hex string.
hex-string	Hexadecimal string (even length - 16 digits).

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

In the following example, “pvc1” within the PVC range called “range1” is deactivated:

```
Router(config)# snasw lu62-security NETA.HOSTB ascii pass1234
Router(config)# snasw lu62-security NETA.HOSTC hex 023f4bc56a
Router#show snasw session detail
1>
Partner LU nameNETA.HOSTB FMH-12 exchanged Yes
```

Related Commands

Command	Description
show snasw session detail	Displays detailed snasw session information.

snasw mode

To define a new mode and associate it with an existing Class of Service (COS), use the **snasw mode** command in global configuration mode. To delete the mode, use the **no** form of this command.

snasw mode *mode* **cos** *cos*

no snasw mode *mode* **cos** *cos*

Syntax Description

mode	Name of the new mode.
cos *cos*	Name of an existing COS, such as #INTER.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is an example of how to configure the **snasw mode** command:

```
snasw mode abcmode cos #INTER
```

snasw msgdump

To enable automatic dumping of the data-link control (DLC) trace, InterProcess Signal (IPS) trace, and problem determination log when a specified Systems Network Architecture (SNA) Switching Services (SNASw) message is displayed, use the **snasw msgdump** command in global configuration mode. To disable automatic dumping, use the **no** form of this command.

snasw msgdump *message* [**writecore**]

no snasw msgdump *message* [**writecore**]

Syntax Description

message	SNASw message to trigger the automatic dump.
writecore	(Optional) Message to trigger a write core.

Defaults

When the **writecore** keyword is used, the write core operation is attempted using Trivial File Transfer Protocol (TFTP).

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.3(15)T	The **writecore** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **snasw msgdump** command is only invoked the first time the target message is encountered. To trigger automatic dumping after this first instance of the target message, remove the configuration and configure again the command by entering the **no snasw msgdump** command followed by the **snasw msgdump** command.

When the message dump is invoked, an SNA Alert is sent to the local node’s Alert focal point. To verify the existence of an Alert focal point, use the **show snasw node** command and look at the value of the “Alert focal point” entry.

Usually, SNASw will have an Alert focal point when the router’s has an active upstream link to a network node server.

If that link is active and there is still no focal point, enter the following command in the NetView mainframe application:

```
FOCALPT CHANGE,FPCAT=ALERT,TARGET=cpname
```

where *cpname* is either the CP name of the NN server for SNASw or the CP name of SNASw itself.

The Alert ID of the SNA Alert sent is x'DAED5B0B'.

Caution Use the **writecore** keyword only under the direction of a technical support representative. Use of the **writecore** keyword puts a large load on the router and may cause momentary network disruption.

To use the **writecore** keyword successfully with the **snasw msgdump** command, you must configure the **exception dump** command to specify a destination server. By default, the write core operation is attempted using TFTP; the core file is written under the /tftpboot directory. If you want to specify the File Transfer Protocol (FTP) for exception instead, use the **ip ftp user**, the **ip ftp password**, and the **exception protocol ftp** commands to configure user name and password information.

Because the **writecore** keyword creates a large file, it is recommended that you compress this file to save server space. Use the exception core-file compress command to compress the file.

Examples

The following example shows how to use the **snasw msgdump** command:

snasw msgdump %SNASW-6-CS_LOG_60

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception dump	Configures the router to dump a core file to a particular server when the router crashes.
exception protocol	Configures the protocol used for core dumps.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

snasw pathswitch

To force an High-Performance Routing (HPR) pathswitch for an Realtime Transport Protocol (RTP) connection, use the **snasw pathswitch** command in privileged EXEC mode.

snasw pathswitch [*rtp-connection-name* | **all**]

Syntax Description

rtp-connection-name	(Optional) Specifies the RTP connection to pathswitch. This is an 8-byte string. You can obtain the value for the *rtp-connection-name* argument from the **show snasw rtp** command.
all	(Optional) Specifies that a pathswitch operation will be initiated for every RTP connection managed by the local node.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a specific connection name is coded, and no such connection is known to Switching Services (SNASw), the **snasw pathswitch** command is ignored, and a message is issued. Use the **snasw pathswitch** command to force an HPR pathswitch for sessions that use this node as an RTP endpoint.

Use the **snasw pathswitch** command if you want to force a switch back to a primary route when it recovers, and the session seems to be hung.

There is not a **no** form for this command.

Examples

The following is an example of how to execute the **snasw pathswitch** command:

```
Router# snasw pathswitch @R000006
```

Related Commands

Command	Description
show snasw rtp	Displays the SNASw RTP connections.

snasw pdlog

To control message logging to the console and the Systems Network Architecture (SNA) problem determination log cyclic buffer, use the **snasw pdlog** command in global configuration mode. To remove previous pdlog configurations, use the **no** form of this command.

snasw pdlog [**problem** | **exception** | **info**] [**buffer-size** *buffer-size-value*] [**file** *filename* [**timestamp**]]

no snasw pdlog

Syntax Description

problem	(Optional) Indicates that only problem records are sent to the console. This is the default.
exception	(Optional) Indicates that both problems and exceptions are sent to the console.
info	(Optional) Indicates that informational messages and problems and exceptions are sent to the console.
buffer-size *buffer-size-value*	(Optional) Indicates the size of the pdlog buffer requested (in kilobytes). The default is 500 KB. The minimum size is 10 KB, and the maximum size is 64000 KB.
file *filename*	(Optional) Indicates the URL for writing the pdlog file to a server. Use the following format: protocol://host/path/filename. If the output file size exceeds 32MB, the first 32MB will be in the file with the name *filename*, the next 32MB will be in the file with the name *filename*.01, and so on. Note that with formatting, the output may be of different size than the buffer-size.
timestamp	(Optional) Appends the current date and time to the end of the file when it is dumped.

Defaults

If not coded, the **snasw pdlog** command defaults to an active 500 KB cyclic buffer. Problems, exceptions, and informational messages are always sent to the buffer. By default, only problems go to the console.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.3	The maximum allowed value of the *buffer-size-value* argument was increased to 6400.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw pdlog** command to customize the type of information you prefer to see on the router console from the Switching Services (SNASw) feature.

Examples

The following is an example of how to configure the **snasw pdlog** command:

```
snasw pdlog exception buffer-size 200 file tftp://my host/files/trace.pdlog
```

Related Commands

Command	Description
show snasw pdlog	Displays entries in the cyclical problem determination log to the console.
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.

snasw port

To specify the data-link controls (DLCs) used by System Network Architecture Switching Services (SNASw), use the **snasw port** command in global configuration mode. To delete a previously configured port, use the **no** form of this command.

HPR-IP Ports

snasw port *port-name* **hpr-ip** *interface-name* [**hostname** *v4-or-v6-hostname* [**ipv4** | **ipv6**]] [**ldlc** [*liveness-time t1-retry-time t1-retry-count*]] [**maxbtu** *max-btu-size*] [**qsize** *qsize-value*] [**vnname** *virtual-node-name* [**no-limres**]] [**nostart**]

no snasw port *port-name*

VDLC and Virtual Token Ring Ports

snasw port *port-name* {**vdlc** *ring-group* **mac** *mac-address* | *virtual-TokenRing-interface-name*} [**conntype nohpr** | **len** | **dyncplen** | **dialoutlen**] [**hpr-sap** *hpr-sap-value*] [**max-links** *link-limit-value*] [**maxbtu** *max-btu-size*] [**nns-required**] [**sap** *sap-value*] [**vnname** *virtual-node-name* [**no-limres**]] [**nostart**]

no snasw port *port-name*

All Other Types of Ports

snasw port *port-name interface-name* [**conntype nohpr** | **len** | **dyncplen** | **dialoutlen**] [**hpr-sap** *hpr-sap-value*] [**max-links** *link-limit-value*] [**maxbtu** *max-btu-size*] [**sap** *sap-value*] [**vnname** *virtual-node-name* [**no-limres**]] [**nostart**]

no snasw port *port-name*

Syntax Description

hpr-ip	Indicates that the port is HPR or IP types.
port-name	The one- to- eight character name for the port. This argument is used to refer to this port in informational messages and the **show snasw port** command.
interface-name	The name of the interface over which the port communicates. Allowable interfaces are Token Ring, Ethernet, VLAN, or loopback.
hostname *v4-or-v6-hostname*	(Optional) Specifies a hostname that resolves to an IPv4 or IPv6 address associated with the interface and over which the port will communicate. The *v4-or-v6-hostname* argument can be between 1 and 64 characters in length.
ipv4	(Optional) Specifies that the preceding hostname is resolved to an IPv4 address only.
ipv6	(Optional) Specifies that the preceding hostname is resolved to an IPv6 address only.
ldlc	(Optional) Overrides the default Logical Data Link Control (LDLC) parameters for all links which use the port. This keyword allows the LDLC parameters for SNASw links to be configured to match those at the other Rapid Transport Protocol (RTP) endpoint, which is often a host z/OS or CS/390.

liveness-time	(Optional) Number of seconds for the liveness timer. This parameter matches the z/OS or CS/390 LIVTIME keyword. The allowed range is from 5 to 25 seconds. Prior to Cisco IOS Release 12.3(8)T, the default was 2 seconds. For Cisco IOS Release 12.3(8)T and later releases, the default is 10 seconds.
t1-retry-time	(Optional) Number of seconds between T1 retry attempts. This parameter matches the z/OS or CS/390 SRQTIME keyword. The allowed range is from 3 to 20 seconds. Prior to Cisco IOS Release 12.3(8)T, the default was 2 seconds. For Cisco IOS Release 12.3(8)T and later releases, the default is 15 seconds.
t1-retry-count	(Optional) Number of times to retry before the HPR-IP TG becomes inoperative. This parameter matches the z/OS or CS/390 SRQRETRY keyword. The allowed range is from 3 to 9 retries. Prior to Cisco IOS Release 12.3(8)T, the default was 10 retries. For Cisco IOS Release 12.3(8)T and later, the default is 3 retries.
maxbtu *max-btu-size*	(Optional) Indicates the maximum basic transmission unit (BTU) size for the remote end (both inbound and outbound). This value is used in XID3 negotiation. The valid range is from 1 to 17800.
qsize *qsize-value*	Number of packets allowed on the IP/ User Datagram Protocol (UDP) inbound queue. • Set the number of packets allowed to a higher value if **show ip socket detail** for one of the SNASw sockets (1200-12004) are showing drops and a highwater equal to the queue limit. • Consider adjusting the interface input hold queues and IP Selective Packet Discard (SPD) queue thresholds at the same time. The allowed range is 50 to 10000, and the default is 50. This keyword applies to HRP/IP interfaces only.
vnname *virtual-node-name*	(Optional) Indicates the network qualified virtual node name (3 to 17 characters) of the connection network being defined.
no-limres	(Optional) Indicates that sessions established on the links over this port are presented as non-limited resources.
nostart	(Optional) Indicates that the port will not open automatically when defined.
vdlc *ring-group*	Indicates that the port is virtual data-link control (VDLC). No *interface-name* argument is required. The *ring-group* argument indicates the source-bridge ring group of which this VDLC port is a member.
mac *mac-address*	Indicates the virtual source MAC address used for the VDLC port.
virtual-TokenRing-interface-name	Name of the virtual token ring interface.
conntype	(Optional) Indicates the connection type for the port. If this keyword is not configured, HPR-capable links are established.
nohpr	(Optional) Indicates that the HPR is not supported but Advanced Peer-to-Peer Networking (APPN) connections with control point (CP)-CP sessions are permitted.
len	(Optional) Indicates that APPN connections are not allowed; only low-entry networking node (LEN) node-level connectivity is negotiated.
dyncplen	(Optional) Specifies the connection type and ends CP names configured on devices that have not been configured uniquely across the XID3-capable devices.
dialoutlen	(Optional) Specifies the connection type when logical unit (LU) 6.2 communications are used.
hpr-sap *hpr-sap-value*	(Optional) Indicates the local HPR-service access point (SAP) value.

max-links *link-limit-value*	(Optional) Indicates the number of links permitted on this port.
maxbtu *max-btu-size*	(Optional) Indicates the maximum BTU size for the remote end (both inbound and outbound). This value is used in XID3 negotiation. The valid range is from 1 to 17800.
nns-required	(Optional) Enables configurations with redundant downstream MAC addresses to only allow SNASw nodes that have appropriate upstream connectivity to accept and retain connections from downstream devices.
sap *sap-value*	(Optional) Indicates the local SAP (LSAP) value.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7) T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. The **no-limres** keyword was added.
12.3	This command was integrated into Cisco IOS Release 12.3. The **dialoutlen** keyword was added.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T. The default values for the *liveness-time*, *t1-retry-time*, and *t1-retry-count* arguments were changed.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T. The **hostname** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(16)	This command was integrated into Cisco IOS Release 12.4(16). The **qsize** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M. The **ipv4** and **ipv6** keywords were added.

Usage Guidelines

More than one port can be configured (with different port names). A configured port cannot be redefined without first deleting the port using the **no** form of the **port** command.

Note Two ports cannot be defined on the same interface unless different values are configured for the **sap** and **hrp-sap** keywords on the ports.

- SNASw ports do not dynamically adjust to interface configuration changes that are made when SNASw is active. For example, if you change an interface MAC address or maximum transmission unit (MTU), SNASw may not recognize the new value. If you want to make changes to an interface and want SNASw to adjust to the new interface changes, you may need to either delete and redefine the port that is using that interface or stop and restart SNASw.

The interface must be defined before the ports that use them are defined and activated.

SNASw does not support EtherChannel interfaces (neither port-channel interfaces nor Fast Ethernet interfaces configured with the **channel-group** command). Do not try to configure a SNASw port with either of these EtherChannel interface types.

- When using the **hostname** keyword, the hostname must be defined on the interface and be resolved locally by either **ip host** or **ipv6 host** commands or by a Domain Name Server (DNS) before the SNASw port is configured.
- When using the **vnname** keyword to define a connection network, Cisco recommends that you do not define any links to this port. Configure one port for your defined links to use, without the **vnname** keyword, and another port with the **vnname** keyword. No links should use the port with the **vnname** keyword. This means you may need to also configure a loopback interface for the **vnname** port.
- When the **dyncplen** keyword is used, a unique cpname must be generated and used locally by SNASw to have a properly functioning APPN connection management and directory function.
- When LU 6.2 communications are used on this link, the **dialoutlen** keyword is needed. A unique cpname must be generated and used locally by SNASw to have a properly functioning APPN connection management and directory function. The keyword is used when link activation to a downstream device is driven by the mainframe dial command.
- When the max-links limit is reached, the port does not respond to inbound connection requests from stations attempting to connect to this port. Outbound connections are still permitted. The **max-links** can be coded only on VDLC and Virtual Token Ring port types.
- When the connection network is treated by default as limited resource, the **no-limres** keyword prevents the remote end from dropping the sessions prematurely (provided that appropriate definitions are also coded on the remote end, such as DISCNT=NO for Physical Unit (PU) or Model in VTAM).
- When a port is configured with the **nns-required** keyword, the port does not respond to downstream connection requests unless this SNASw node has active CP-CP sessions to an upstream network management system (NNS). If a connection has already been made through this SNASw node and then upstream NNS CP-CP connectivity is lost, this SNASw node deactivates all non-HPR links using this port that do not have active LU-LU or Intermediate Session Routing (ISR) sessions.

Note The **nns-required** keyword is relevant only for ports that will be accepting downstream connections from devices. It is not relevant for upstream ports. This keyword is only valid for Virtual Token Ring and VDLC ports.

Examples

The following examples show how to configure the **snasw port** command:

```
Router(config)# snasw port SRBG Virtual-TokenRing0 conntype nohpr
Router(config)# snasw port UPSTREAM TokenRing1/1
Router(config)# snasw port dlswport vdlc 30 mac 4000.33333.4444
Router(config)# snasw port HPRIP hpr-ip Loopback0
Router(config)# snasw port TRVLAN Vlan1/1 vnname NETA.CONNET
Router(config)# snasw port HOSTEE hpr-ip Loopback0 vnname NETA.CONNET hostname Loop0ip
```

Related Commands

Command	Description
show snasw port	Displays the SNASw port objects.
snasw link	Configures upstream links.

snasw rtp pathswitch-timers

To tune the RealTime Transport Protocol (RTP) pathswitch timers for an SNASwitch, use the **snasw rtp pathswitch-timers** command in global configuration mode. To restore the default settings for the RTP pathswitch timers, use the **no** form of this command.

snasw rtp pathswitch-timers *low-priority medium-priority high-priority network-priority*

no snasw rtp pathswitch-timers

Syntax Description

low-priority	Number of seconds to attempt pathswitch for low-priority RTPs. Allowed values are from 5 to 65535 seconds. The default is 480.
medium-priority	Number of seconds to attempt pathswitch for medium-priority RTPs. Allowed values are from 5 to 65535 seconds. The default is 240 seconds.
high-priority	Number of seconds to attempt pathswitch for high-priority RTPs. Allowed values are from 5 to 65535 seconds. The default is 120 seconds.
network-priority	Number of seconds to attempt pathswitch for network-priority RTPs. Allowed values are from 5 to 120 seconds. The default is 60 seconds.

Defaults

low-priority: 480 seconds
medium-priority: 240 seconds
high-priority: 120 seconds
network-priority: 60 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The arguments for this command should be tuned to match the values specified at the other end of the RTP connection. This endpoint could be another SNA switch router or any other High-Performance Routing (HPR)-capable control point, which will most often be an IBM z/OStm mainframe. In this case, you should match the settings of the HPRPST start option.

The value for each pathswitch timer value must be greater than or equal to the value for the next highest priority timer argument. In other words, the *low-priority* argument >= *medium-priority* argument >= *high-priority* argument >= *network-priority* argument.

Examples

The following example tunes the RTP pathswitch timers:

```
router(config)# snasw rtp pathswitch-timers 160 80 40 20
```

snasw start

To start Switching Services (SNASw), use the **snasw start** command in privileged EXEC mode.

snasw start

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If not enough memory exists to start SNASw, a message indicating lack of memory is issued. A control point (CP) name must be configured with the **snasw cpname** command before SNASw will start.

Examples

The following is an example of the **snasw start** command:

```
Router# snasw start
```

Related Commands

Command	Description
show snasw node	Displays details and statistics of the SNASw operation.
snasw stop	Shuts down SNASw.

snasw start cp-cp

To initiate a request to start control point (CP)-CP sessions with a partner CP, use the **snasw start cp-cp** command in privileged EXEC mode.

snasw start cp-cp *cpname*

Syntax Description

cpname	Indicates the fully qualified CP name of the adjacent node with which CP-CP sessions should be started.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw start cp-cp** command if CP-CP sessions fail permanently or temporarily, but beyond the time frame for automatic CP-CP session retry. If the current state of the node mandates that CP-CP sessions cannot be started to the partner (for example, CP-CP sessions already exist on a different upstream link) or no active adjacent CP matches the cpname named, the command fails.

Typically, Switching Services (SNASw) automatically activates CP-CP sessions as necessary and the **snasw start cp-cp** command is rarely needed. Frequent CP-CP session failure beyond the time frame for automatic session retry indicates a problem, and should be reported.

Examples

The following is an example of the **snasw start cp-cp** command:

```
Router# snasw start cp-cp NETA.CMCHOST
```

Related Commands

Command	Description
snasw stop cp-cp	Terminates CP-CP sessions with a partner CP.

snasw start link

To start an inactive defined link, use the **snasw start link** command in privileged EXEC mode.

snasw start link *linkname*

Syntax Description

linkname	Indicates the name of the link as configured or shown in **show snasw link** command.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw start link** command to initiate a connection sequence for a link that is defined but not active. Unless the **nostart** command is configured on the link definition, a link is started automatically. Use this command to start links that have **nostart** configured or links that have been stopped using the **snasw stop link** privileged EXEC command.

Examples

The following is an example of the **snasw start link** command:

```
Router# snasw start link CMCHOST1
```

Related Commands

Command	Description
show snasw link	Displays the Switching Services (SNASw) link objects.
snasw stop link	Stops an active link.

snasw start port

To start an inactive port, use the **snasw start port** command in privileged EXEC mode.

snasw start port *portname*

Syntax Description

portname	Indicates the name of the port as configured or shown in the **show snasw port** command.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw start port** command to enable a port that is defined to the configuration but is not active. Unless the **nostart** command is configured on the port definition, a port is started automatically. Use this command to start ports that have **nostart** configured or ports that have been stopped using the **snasw stop port** privileged EXEC command.

Examples

The following is an example of the **snasw start port** command:

```
Router# snasw start port TOKEN0
```

Related Commands

Command	Description
show snasw port	Displays the Switching Services (SNASw) port objects.
snasw stop port	Stops an active port.

snasw stop

To shut down Switching Services (SNASw), use the **snasw stop** command in privileged EXEC mode.

snasw stop

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw stop** command to terminate all sessions, stop all ports and links, and shut down SNASw. When you enter this command, you are prompted for confirmation.

Examples

The following is an example of the **snasw stop** command:

```
Router# snasw stop
```

Related Commands

Command	Description
snasw start	Starts SNASw.

snasw stop cp-cp

To terminate control point (CP)-CP sessions with a partner CP, use the **snasw stop cp-cp** command in privileged EXEC mode.

snasw stop cp-cp *cpname*

Syntax Description

cpname	Indicates the fully qualified CP name of the adjacent node with which CP-CP sessions should be stopped.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the primary National Number (NN) server (uplink) fails, CP-CP sessions are established with a backup, if one is available. When the link to the primary recovers, Switching Services (SNASw) retains the CP-CP sessions established with the backup and does not automatically switch back to the primary. To force SNASw to switch back to the primary, use the **snasw stop cp-cp** command. (If the link to the backup fails, SNASw does switch back to the primary automatically.)

You can also use the **snasw stop cp-cp** command to clear some fault scenarios, such as hung or nonresponsive CP sessions, allowing the Systems Network Architecture (SNA) switch to potentially restart sessions with the same or alternate destination logical unit (LU).

Examples

The following is an example of the **snasw stop cp-cp** command:

```
Router# snasw stop cp-cp NETA.CMCHOST
```

Related Commands

Command	Description
snasw start cp-cp	Initiates a request to start CP-CP sessions with a partner CP.

snasw stop link

To stop an active link, use the **snasw stop link** command in privileged EXEC mode.

snasw stop link *linkname*

Syntax Description

linkname	Indicates the name of the link as configured or shown in the **show snasw link** command.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw stop link** command to deactivate a link to a specified partner control point (CP). All High-Performance Routing (HPR) sessions established using the link are disconnected. HPR sessions are disrupted only if no alternate route is available.

Normally a link stopped with the **snasw stop link** command must be restarted by issuing the **snasw start link** command. However, it will be automatically restarted under the following conditions:

- The **nns** keyword is specified on the **snasw link** command, and
- The SNASw CP did not already re-establish CP-CP sessions with a network node server over another upstream link.

Examples

The following is an example of the **snasw stop link** command:

```
Router# snasw stop link CMCHOST1
```

Related Commands

Command	Description
show snasw link	Displays the Switching Services (SNASw) link objects.

snasw stop port

To stop an active port, use the **snasw stop port** command in privileged EXEC mode.

snasw stop port *portname*

Syntax Description

portname	Indicates the name of the port as configured or shown in the **show snasw port** command.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **snasw stop port** command to disable a specified port without removing it from the configuration. All High-Performance Routing (HPR) sessions established using the port and all links are shut down on the port. HPR sessions are disrupted only if no alternate route is available.

Examples

The following is an example of the **snasw stop port** command:

```
Router# snasw stop port TOKEN0
```

Related Commands

Command	Description
snasw start port	Starts an inactive port.

snasw stop session

To terminate an active session, use the **snasw stop session** command in privileged EXEC mode.

snasw stop session *pcid*

Syntax Description

pcid	Procedure correlator ID in 16-digit hexadecimal form.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **snasw stop session** command is used to clear sessions that are active but in an indeterminate or hung state or if the session partner is not responsive.

You can also use the **snasw stop session** command to free a small amount of memory if the session is no longer being used to transport data and you do not expect to use the session later.

Examples

The following is an example of the **snasw stop session** command:

```
Router# snasw stop session C3BBD36EA9CBA1AF
```

Related Commands

Command	Description
show snasw session	Displays the Switching Services (SNASw) session objects.

source-bridge

To configure an interface for source-route bridging (SRB), use the **source-bridge** command in interface configuration mode. To disable source-route bridging on an interface, use the **no** form of this command.

source-bridge *source-ring-number bridge-number target-ring-number* [**conserve-ring**]

no source-bridge *source-ring-number bridge-number target-ring-number* [**conserve-ring**]

Syntax Description

source-ring-number	Ring number for the interface's Token Ring or FDDI ring. It must be a decimal number in the range from 1 to 4095 that uniquely identifies a network segment or ring within the bridged Token Ring or FDDI network
bridge-number	Number that uniquely identifies the bridge connecting the source and target rings. It must be a decimal number in the range from 1 to 15.
target-ring-number	Ring number of the destination ring on this router. It must be unique within the bridged Token Ring or FDDI network. The target ring can also be a ring group. Must be a decimal number.
conserve-ring	(Optional) Keyword to enable SRB over Frame Relay. When this option is configured, the SRB software does not add the ring number associated with the Frame Relay PVC (the partner's virtual ring) to outbound explorer frames. This option is permitted for Frame Relay subinterfaces only.

Defaults

SRB is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was revised to enable SRB over Frame Relay.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The parser automatically displays the word "active" in the **source-bridge** command in configurations that have SRB enabled. You need not enter the **source-bridge** command with the **active** keyword.

Examples

In the following example, Token Rings 129 and 130 are connected via a router:

```
interface tokenring 0
```

```
 source-bridge 129 1 130
!
interface tokenring 1
 source-bridge active 130 1 129
```

In the following example, an FDDI ring on one router is connected to a Token Ring on a second router across a data-link switching plus (DLSw+) link:

```
dlsw local-peer peer-id 132.11.11.2
dlsw remote-peer 0 tcp 132.11.11.3
!
interface fddi 0
 no ip address
 multiring all
 source-bridge active 26 1 10
!
dlsw local-peer peer-id 132.11.11.3
dlsw remote-peer 0 tcp 132.11.11.2
!
interface tokenring 0
 no ip address
 multiring all
 source-bridge active 25 1 10
```

In the following example, a router forwards frames from a locally attached Token Ring over the Frame Relay using SRB:

```
source-bridge ring-group 200
!
interface Serial0
 encapsulation frame-relay
!
interface Serial0.30 point-to-point
 frame-relay interface-dlci 30 ietf
 source-bridge 100 1 200 conserve-ring
 source-bridge spanning
!
interface TokenRing0
 source-bridge 600 1 200
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
source-bridge ring-group	Defines or removes a ring group from the configuration.
source-bridge transparent	Establishes bridging between transparent bridging and SRB.

source-bridge connection-timeout

To establish the interval of time between first attempt to open a connection until a timeout is declared, use the **source-bridge connection-timeout** command in global configuration mode. To disable this feature, use the **no** form of this command.

source-bridge connection-timeout *seconds*

no source-bridge connection-timeout *seconds*

Syntax Description

seconds	Interval of time, in seconds, before a connection attempt to a remote peer is aborted. The default is 10 seconds.

Defaults

The default connection-timeout interval is 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **source-bridge connection-timeout** command is used for setting timeout intervals in a complex topology such as a large multihop WAN with virtual rings or satellite links. The timeout interval is used when a connection to a remote peer is attempted. If the timeout interval expires before a response is received, the connection attempt is aborted.

Examples

The following example sets the connection timeout interval to 60 seconds:

```
source-bridge connection-timeout 60
```

Related Commands

Command	Description
source-bridge ring-group	Defines or removes a ring group from the configuration.

source-bridge cos-enable

To force the Cisco IOS software to read the contents of the format identification (FID) frames to prioritize traffic when using TCP, use the **source-bridge cos-enable** command in global configuration mode. To disable prioritizing, use the **no** form of this command.

source-bridge cos-enable

no source-bridge cos-enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to prioritize your Systems Network Architecture (SNA) traffic across the backbone network. All your important front-end processor (FEP) traffic can flow on high-priority queues. This is useful only between FEP-to-FEP (physical unit [PU] 4-to-PU 4) communications (across the non-SNA backbone).

Note Logical Link Control, type 2 (LLC2) local acknowledgment must be turned on for the Class of Service (CoS) feature to take effect, and the **source-bridge remote-peer tcp** command with the **priority** keyword must be issued.

Examples

The following example enables CoS for prioritization of SNA traffic across a network:

```
source-bridge cos-enable
```

Related Commands

Command	Description
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

source-bridge enable-80d5

To change the router's Token Ring to Ethernet translation behavior, use the **source-bridge enable-80d5** command in global configuration mode. To disable this function, use the **no** form of this command.

source-bridge enable-80d5

no source-bridge enable-80d5

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software supports two types of Token Ring LLC2 to Ethernet conversion:

- Token Ring LLC2 to Ethernet 802.3 LLC2
- Token Ring LLC2 to Ethernet 0x80d5

Use this global configuration command to change the translation behavior. By default, the Cisco IOS software translates Token Ring LLC2 to Ethernet 802.3 LLC2. This command allows you to configure the software to translate Token Ring LLC2 frames into Ethernet 0x80d5 format frames.

This command is useful when you have a non-IBM device attached to an IBM network with devices that are using the nonstandard Token Ring LLC2 to Ethernet 80d5 translation. If you do not configure your router to enable 80d5 processing, the non-IBM and IBM devices will not be able to communicate.

The parameters specifying the current parameters for the processing of 0x80d5 frames are given at the end of the output of the **show span** command.

Note The 80d5 frame processing option is available only with source-route translational bridging (SR/TLB). It is not available when source-route transparent bridging (SRT) is used.

Use the **show span** command to verify that 80d5 processing is enabled. If it is, the following line is displayed in the output:

```
Translation between LLC2 and Ethernet Type II 80d5 is enabled
```

Examples

The following example enables 0x80d5 processing, removes the translation for service access point (SAP) 08, and adds the translation for SAP 1c:

```
source-bridge enable-80d5
no source-bridge sap-80d5 08
source-bridge sap-80d5 1c
```

Related Commands

Command	Description
show span	Displays the spanning-tree topology known to the router.
source-bridge sap-80d5	Allows non-IBM hosts (attached to a router with 80d5 processing enabled) to use the standard Token Ring to Ethernet LLC2 translation instead of the nonstandard Token Ring to Ethernet 80d5 translation, and allows the translation to be set on a per-DSAP basis.

source-bridge explorer-dup-ARE-filter

To filter out duplicate explorers in networks with redundant topologies, use the **source-bridge explorer-dup-ARE-filter** command in global configuration mode. To disable this feature, use the **no** form of this command.

source-bridge explorer-dup-ARE-filter

no source-bridge explorer-dup-ARE-filter

Syntax Description

This command has no arguments or keywords.

Defaults

Duplicate explorer filtering is disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables duplicate explorer filtering:

```
source-bridge explorer-dup-ARE-filter
```

source-bridge explorer-fastswitch

To enable explorer fast switching, use the **source-bridge explorer-fastswitch** command in global configuration mode. To disable explorer fast switching, use the **no** form of this command.

source-bridge explorer-fastswitch

no source-bridge explorer-fastswitch

Syntax Description

This command has no arguments or keywords.

Defaults

Fast switching is enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **no** form of this command in conjunction with the **source-bridge explorerq-depth** and the **source-bridge explorer-maxrate** commands to optimize explorer processing.

Examples

The following example enables explorer fast switching after it has been previously disabled:

```
source-bridge explorer-fastswitch
```

Related Commands

Command	Description
source-bridge explorer-maxrate	Sets the maximum byte rate of explorers per ring.
source-bridge explorerq-depth	Sets the maximum explorer queue depth.

source-bridge explorer-maxrate

To set the maximum byte rate of explorers per ring, use the **source-bridge explorer-maxrate** command in global configuration mode. To reset the default rate, use the **no** form of this command.

source-bridge explorer-maxrate *maxrate*

no source-bridge explorer-maxrate *maxrate*

Syntax Description

maxrate	Number in the range from 100 to 1000000000 (in bytes per second). The default maximum byte rate is 38400 bytes per second.

Defaults

The default maximum byte rate is 38400 bytes per second.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Given the number of different explorer packet types and sizes and the bandwidth limits of the various interfaces, the bus data rate (as opposed to the packet rate) is the common denominator used to decide when to flush incoming explorers. The packets are dropped by the interface before any other processing.

Examples

The following command sets the maximum byte rate of explorers on a ring:

```
source-bridge explorer-maxrate 100000
```

source-bridge explorerq-depth

To set the maximum explorer queue depth, use the **source-bridge explorerq-depth** command in global configuration mode. To reset the default value, use the **no** form of this command.

source-bridge explorerq-depth *depth*

no source-bridge explorerq-depth *depth*

Syntax Description

depth	The maximum number of incoming packets. The valid range is from 1 to 500. The default is 30 packets.

Defaults

The default maximum depth is 30.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In this implementation, the maximum depth is set on a per-interface basis (default maximum depth is 30) therefore, each interface can have up to the maximum outstanding packets on the queue before explorers from that particular interface are dropped.

The **source-bridge explorerq-depth** command is used in a Token Ring and source-route bridging environment.

Examples

The following example sets the maximum explorer queue depth:

```
source-bridge explorerq-depth 100
```

Related Commands

Command	Description
dlsw explorerq-depth	Establishes queue depth for multiple queues that handle various types of explorer traffic.

source-bridge fst-peername

To set up a Fast-Sequenced Transport (FST) peer name, use the **source-bridge fst-peername** command in global configuration mode. To disable the IP address assignment, use the **no** form of this command.

source-bridge fst-peername *local-interface-address*

no source-bridge fst-peername *local-interface-address*

Syntax Description

local-interface-address	IP address to assign to the local router.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is the first step to configuring a remote source-route bridge to use FST.

Examples

The following example sets up an FST peer name:

```
source-bridge fst-peername 10.136.64.98
```

Related Commands

Command	Description
source-bridge remote-peer fst	Specifies an FST encapsulation connection.

source-bridge input-address-list

To apply an access list to an interface configured for source-route bridging, use the **source-bridge input-address-list** command in interface configuration mode. To remove the application of the access list, use the **no** form of this command.

source-bridge input-address-list *access-list-number*

no source-bridge input-address-list *access-list-number*

Syntax Description

access-list-number	Number of the access list. The value must be in the range from 700 to 799.

Defaults

No access list is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command filters source-routed packets received from the router interface based upon the source MAC address.

Examples

The following example assigns access list 700 to Token Ring 0:

```
access-list 700 deny 1000.5A00.0000  8000.00FF.FFFF
access-list 700 permit 0000.0000.0000  FFFF.FFFF.FFFF
!
interface tokenring 0
 source-bridge input-address-list 700
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
source-bridge output-address-list	Applies an access list to an interface configured for SRB, and filters source-routed packets sent to the router interface based on the destination MAC address.

source-bridge input-lsap-list

To filter, on input, FDDI and IEEE 802-encapsulated packets that include the destination service access point (DSAP) and source service access point (SSAP) fields in their frame formats, use the **source-bridge input-lsap-list** command in interface configuration mode. To restore the default value, use the **no** form of this command.

source-bridge input-lsap-list *access-list-number*

no source-bridge input-lsap-list *access-list-number*

Syntax Description

access-list-number	Number of the access list. This access list is applied to all IEEE 802 or FDDI frames received on that interface prior to the source-routing process. Specify zero (0) to disable the filter. The value must be in the range from 200 to 299.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The access list specifying the type codes to be filtered is given by this variation of the **source-bridge** command in interface configuration mode.

Examples

The following example specifies access list 203:

```
interface tokenring 0
 source-bridge input-lsap-list 203
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
source-bridge output-lsap-list	Filters, on output, FDDI and IEEE 802-encapsulated packets that have DSAP and SSAP fields in their frame formats.

source-bridge input-type-list

To filter Subnetwork Access Protocol (SNAP)-encapsulated packets on input, use the **source-bridge input-type-list** command in interface configuration mode.

source-bridge input-type-list *access-list-number*

no source-bridge input-type-list *access-list-number*

Syntax Description

access-list-number	Number of the access list. This access list is applied to all SNAP frames received on that interface prior to the source-routing process. Specify zero (0) to disable the application of the access list on the bridge group. The value must be in the range from 200 to 299.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **access list** command to specify type code when using the **source-bridge input-type-list** command.

Examples

The following example specifies access list 202:

```
access-list 202 deny 0x6000 0x0007
access-list 202 permit 0x0000 0xFFFF
!
interface tokenring 0
 source-bridge input-type-list 202
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
source-bridge output-type-list	Filters SNAP-encapsulated frames by type code on output.

source-bridge keepalive

To assign the keepalive interval of the remote source-bridging peer, use the **source-bridge keepalive** command in interface configuration mode. To cancel previous assignments, use the **no** form of this command.

source-bridge keepalive *seconds*

no source-bridge keepalive

Syntax Description

seconds	Keepalive interval in seconds. The valid range is from 10 to 300. The default value is 30 seconds.

Defaults

30 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the keepalive interval to 60 seconds:

```
source-bridge keepalive 60
```

Related Commands

Command	Description
show interfaces	Displays statistics for the interfaces configured on a router or access server.
source-bridge	Configures an interface for source-route bridging (SRB).
source-bridge remote-peer fst	Specifies an FST encapsulation connection.
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

source-bridge largest-frame

To configure the largest frame size that is used to communicate with any peers in the ring group, use the **source-bridge largest-frame** command in global configuration mode. To cancel previous assignments, use the **no** form of this command.

source-bridge largest-frame *ring-group size*

no source-bridge largest-frame *ring-group*

Syntax Description

ring-group	Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.
size	Maximum frame size. The default is that no frame size is assigned. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

Defaults

No frame size is assigned.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Cisco IOS software negotiates all transit routes down to the specified size or lower. Use the *size* argument with this command to prevent timeouts in end hosts by reducing the amount of data they must send in a fixed interval. For example, in some networks containing slow links, it would be impossible to send an 8-KB frame and receive a response within a few seconds. These are standard defaults for an application on a 16-Mb Token Ring. If the frame size is lowered to 516 bytes, then only 516 bytes must be sent and a response received in 2 seconds. This feature is most effective in a network with slow links. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

Examples

The following example sets the largest frame that can be sent through a ring group to 1500 bytes:

```
source-bridge largest-frame 8 1500
```

Related Commands

Command	Description
source-bridge ring-group	Defines or removes a ring group from the configuration.

source-bridge max-hops

To control the forwarding or blocking of all-route explorer frames received on an interface, use the **source-bridge max-hops** command in interface configuration mode. To reset the count to the maximum value, use the **no** form of this command.

source-bridge max-hops *count*

no source-bridge max-hops

Syntax Description

count	Determines the number of bridges an explorer packet can traverse. Typically, the maximum number of bridges for interoperability with IBM equipment is seven.

Defaults

The maximum number of bridge hops is seven.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Frames are forwarded only if the number of hops in the routing information field of the input frame plus hops appended by the router is fewer than or equal to the specified count. If the interface is connected to a destination interface, the router appends one hop. If the interface is tied to a virtual ring, the router appends two hops. This applies only to all-routes explorer frames on input to this interface.

Examples

The following example limits the maximum number of source-route bridge hops to five:

```
source-bridge max-hops 5
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.
source-bridge max-in-hops	Controls the forwarding or blocking of spanning-tree explorer frames received on an interface.
source-bridge max-out-hops	Controls the forwarding or blocking of spanning-tree explorer frames sent from this interface.

source-bridge max-in-hops

To control the forwarding or blocking of spanning-tree explorer frames received on an interface, use the **source-bridge max-in-hops** command in interface configuration mode. To reset the count to the maximum value, use the **no** form of this command.

source-bridge max-in-hops *count*

no source-bridge max-in-hops

Syntax Description

count	Determines the number of bridges an explorer packet can traverse. Typically, the maximum number of bridges for interoperability with IBM equipment is seven.

Defaults

The maximum number of bridge hops is seven.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Frames are forwarded only if the number of hops in the routing information field of the input frame is fewer than or equal to the specified count. This applies only to spanning-tree explorer frames input to the specified interface.

Examples

The following example limits the maximum number of source-route bridge hops to three:

```
source-bridge max-in-hops 3
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.
source-bridge max-hops	Controls the forwarding or blocking of all-route explorer frames received on an interface.
source-bridge max-out-hops	Controls the forwarding or blocking of spanning-tree explorer frames sent from this interface.

source-bridge max-out-hops

To control the forwarding or blocking of spanning-tree explorer frames sent from this interface, use the **source-bridge max-out-hops** command in interface configuration mode. To reset the count to the maximum value, use the **no** form of this command.

source-bridge max-out-hops *count*

no source-bridge max-out-hops

Syntax Description

count	Determines the number of bridges an explorer packet can traverse. Typically, the maximum number of bridges for interoperability with IBM equipment is seven.

Defaults

The maximum number of bridge hops is seven.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Frames are forwarded only if the number of hops in the routing information field of the frame (including the hops appended by the router) is fewer than or equal to the specified count. This applies only to spanning-tree explorer frames output from the specified interface.

Examples

The following example limits the maximum number of source-route bridge hops to five:

```
source-bridge max-out-hops 5
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.
source-bridge max-hops	Controls the forwarding or blocking of all-route explorer frames received on an interface.
source-bridge max-in-hops	Controls the forwarding or blocking of spanning-tree explorer frames received on an interface.

source-bridge output-address-list

To apply an access list to an interface configured for source-route bridging, use the **source-bridge output-address-list** command in interface configuration mode. To remove the application of the access list, use the **no** form of this command.

source-bridge output-address-list *access-list-number*

no source-bridge output-address-list *access-list-number*

Syntax Description

access-list-number	Number of the access list. The value must be in the range from 700 to 799.

Defaults

No access list is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command filters source-routed packets sent to the router interface based upon the destination MAC address.

Examples

To disallow the bridging of Token Ring packets of all IBM workstations on Token Ring 1, use this sample configuration. The software assumes that all such hosts have Token Ring addresses with the vendor code 1000.5A00.0000. The vendor portion of the MAC address is the first three bytes (left to right) of the address. The first line of the access list denies access to all IBM workstations, and the second line permits access to all other devices on the network. Then, the access list can be assigned to the input side of Token Ring 1.

```
access-list 700 deny 1000.5A00.0000   8000.00FF.FFFF
access-list 700 permit 0000.0000.0000   FFFF.FFFF.FFFF
interface tokenring 1
 source-bridge output-address-list 700
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
source-bridge input-address-list	Applies an access list to an interface configured for source-route bridging, and filters source-routed packets received from the router interface based on the source MAC address.

source-bridge output-lsap-list

To filter, on output, FDDI and IEEE 802-encapsulated packets that have destination service access point (DSAP) and source service access point (SSAP) fields in their frame formats, use the **source-bridge output-lsap-list** command in interface configuration mode.

source-bridge output-lsap-list *access-list-number*

no source-bridge output-lsap-list *access-list-number*

Syntax Description

access-list-number	Number of the access list. This access list is applied just before sending out a frame to an interface. Specify zero (0) to disable the filter. The value must be in the range from 200 to 299.

Defaults

No filters are applied.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The access list specifying the type codes to be filtered is given by this command.

Examples

The following example specifies access list 251:

```
access-list 251 permit 0xE0E0 0x0101
access-list 251 deny 0x0000 0xFFFF
!
interface tokenring 0
 source-bridge output-lsap-list 251
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
source-bridge input-lsap-list	Filters, on input, FDDI and IEEE 802-encapsulated packets that include the DSAP and SSAP fields in their frame formats. The access list specifying the type codes to be filtered is given by this variation of the **source-bridge** command in interface configuration mode.

source-bridge output-type-list

To filter Subnetwork Access Protocol (SNAP)-encapsulated frames by type code on output, use the **source-bridge output-type-list** command in interface configuration mode. To restore the default value, use the **no** form of this command.

source-bridge output-type-list *access-list-numbers*

no source-bridge output-type-list *access-list-numbers*

Syntax Description

access-list-number	Number of the access list. This access list is applied just before sending out a frame to an interface. Specify zero (0) to disable the application of the access list on the bridge group. The value must be in the range from 200 to 299.

Defaults

No filters are applied.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Input and output type code filtering on the same interface reduces performance and is not recommended.

Access lists for Token Ring- and IEEE 802-encapsulated packets affect only source-route bridging functions. Such access lists do not interfere with protocols that are being routed.

Use the access list specifying the types codes in this command.

Examples

The following example filters SNAP-encapsulated frames on output:

```
access-list 202 deny 0x6000 0x0007
access-list 202 permit 0x0000 0xFFFF
!
! apply interface configuration commands to interface tokenring 0
interface tokenring 0
! filter SNAP-encapsulated frames on output using access list 202
 source-bridge output-type-list 202
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
source-bridge input-type-list	Filters SNAP-encapsulated packets on input.

source-bridge passthrough

To configure some sessions on a few rings to be locally acknowledged and the remaining to pass through, use the **source-bridge passthrough** command in global configuration mode. To disable passthrough on all the rings and allow the session to be locally acknowledged, use the **no** form of this command.

source-bridge passthrough *ring-group*

no source-bridge passthrough *ring-group*

Syntax Description

ring-group	Ring group number. This ring is either the start ring or destination ring of the two IBM end machines for which the pass through feature is to be configured. This ring group number must match the number you specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in conjunction with the **source-bridge remote-peer tcp** command that has the **local-ack** keyword specified, which causes every new Logical Link Control, type 2 (LLC2) session to be locally terminated. If a machine on the Token Ring attempts to start an LLC2 session to an end host that exists on the *ring-group* value specified in the **source-bridge passthrough** command, the session will “pass through” and not use local acknowledgment for LLC2.

If you specify pass through for a ring, LLC2 sessions will never be locally acknowledged on that ring. This is true even if a remote peer accessing the ring has set th**e local-ack** keyword in the **source-bridge remote-peer tcp** command. The **source-bridge passthrough** command overrides any setting in the **source-bridge remote-peer tcp** command.

You can define more than one **source-bridge passthrough** command in a configuration.

Examples

The following example configures the router to use local acknowledgment on remote peer at 10.1.1.2 but pass through on rings 9 and 4:

```
source-bridge ring-group 100
source-bridge remote-peer 100 tcp 10.1.1.1
source-bridge remote-peer 100 tcp 10.1.1.2 local-ack
source-bridge passthrough 9
source-bridge passthrough 4
```

Related Commands

Command	Description
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.
source-bridge ring-group	Defines or removes a ring group from the configuration.

source-bridge proxy-explorer

To configure the interface to respond to any explorer packets from a source node that meet the conditions described below, use the **source-bridge proxy-explorer** command in interface configuration mode. To cancel responding to explorer packets with proxy explorers, use the **no** form of this command.

source-bridge proxy-explorer

no source-bridge proxy-explorer

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The proxy explorer function allows the source-route bridge interface to respond to a source node on behalf of a particular destination node. The interface responds with proxy explorers. The following conditions must be met in order for the interface to respond to a source node with proxy explorers on behalf of a destination node:

- The destination node must be in the Routing Information Field (RIF) cache.
- The destination node must not be on the same ring as the source node.
- The explorer packet must be an IEEE 802.2 XID or TEST packet.
- The packet cannot be from the IBM Token Ring LAN Network Manager source service access point (SAP).

If all of the conditions are met, the source-route bridge interface will turn the packet around, append the appropriate RIF, and reply to the source node.

Use proxy explorers to limit the amount of explorer traffic propagating through the source-bridge network, especially across low-bandwidth serial lines. The proxy explorer is most useful for multiple connections to a single node.

Examples

The following example configures the router to use proxy explorers on Token Ring 0:

```
interface tokenring 0
 source-bridge proxy-explorer
```

source-bridge proxy-netbios-only

To enable proxy explorers for the NetBIOS name-caching function, use the **source-bridge proxy-netbios-only** command in global configuration mode. To disable the NetBIOS name-caching function, use the **no** form of this command.

source-bridge proxy-netbios-only

no source-bridge proxy-netbios-only

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the router to use proxy explorers:

```
source-bridge proxy-netbios-only
```

source-bridge qllc-local-ack

To enable or disable Qualified Logical Link Control (QLLC) local acknowledgment for all QLLC conversion connections, use the **source-bridge qllc-local-ack** command in global configuration mode. To disable this capability, use the **no** form of this command.

source-bridge qllc-local-ack

no source-bridge qllc-local-ack

Syntax Description

This command has no arguments or keywords.

Defaults

QLLC local acknowledgment is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In a remote source-route bridged topology, QLLC local acknowledgment is used to configure the QLLC conversion router (connecting the remote X.25 devices) to exchange local acknowledgment information with the Token Ring router (on the Token Ring side of the cloud). This Token Ring device has been configured for Logical Link Control, type 2 (LLC2) local acknowledgment using the **source-bridge remote-peer tcp local-ack** command.

You must issue the **source-bridge qllc-local-ack** command only on the QLLC conversion router. When this command is issued, all of the QLLC conversion sessions are locally acknowledged at the Token Ring interface of the Token Ring router with which it is communicating using QLLC conversion.

Examples

The following configuration indicates that the local router (10.108.2.2) QLLC conversion sessions will be locally acknowledged at the remote router:

```
source-bridge ring-group 100
source-bridge remote-peer 100 tcp 10.108.1.1 local-ack
source-bridge remote-peer 100 tcp 10.108.2.2
source-bridge qllc-local-ack
```

Related Commands

Command	Description
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.
source-bridge sdllc-local-ack	Activates local acknowledgment for SDLLC sessions on a particular interface.

source-bridge remote-peer frame-relay

To specify a point-to-point direct encapsulation connection, use the **source-bridge remote-peer frame-relay** command in global configuration mode. To disable previous interface assignments, use the **no** form of this command.

source-bridge remote-peer *ring-group* **frame-relay interface** *name number* [*mac-address*] [*dlci-number*] [**lf** *size*]

no source-bridge remote-peer *ring-group* **frame-relay interface** *name number*

Syntax Description

ring-group	Ring group number. This ring group number must match the number you specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.
interface *name number*	Name and number of the interface over which to send source-route bridged traffic.
mac-address	(Optional) MAC address for the interface on the other side of the virtual ring. This argument is required for nonserial interfaces. You can obtain the value of this MAC address by using the **show interface** command, and then scanning the display for the interface specified by the *name* argument.
dlci-number	(Optional) Data-link connection identifier (DLCI) number for Frame Relay encapsulation.
lf *size*	(Optional) Maximum-sized frame to be sent to this remote peer, in bytes. The Cisco IOS software negotiates all transit routes down to this size or lower. Use the size argument to prevent timeouts in end hosts by reducing the amount of data they must send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800.

Defaults

No point-to-point direct encapsulation connection is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to identify the interface over which to send source-route bridged traffic to another router in the ring group. A serial interface does not require that you include a MAC-level address; all other types of interfaces do require MAC addresses.

You must specify one **source-bridge remote-peer** command for each peer router that is part of the virtual ring. You must also specify one **source-bridge remote-peer** command to identify the IP address of the local router.

It is possible to mix all types of transport methods within the same ring group.

Note The two peers using the serial-transport method will function correctly only if there are routers at the end of the serial line that have been configured to use the serial transport. The peers must also belong to the same ring group.

Examples

The following example sends source-route bridged traffic over serial interface 0 and Ethernet interface 0:

```
! send source-route bridged traffic over serial 0
source-bridge remote-peer 5 frame-relay interface serial 0
! specify MAC address for source-route bridged traffic on Ethernet 0
source-bridge remote-peer 5 interface Ethernet 0 0000.0c00.1234
```

Related Commands

Command	Description
show interfaces	Displays statistics for the interfaces configured on a router or access server.
source-bridge	Configures an interface for source-route bridging (SRB).
source-bridge remote-peer fst	Specifies an FST encapsulation connection.
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

source-bridge remote-peer fst

To specify a Fast-Sequenced Transport (FST) encapsulation connection, use the **source-bridge remote-peer fst** command in global configuration mode. To disable the previous assignments, use the **no** form of this command.

source-bridge remote-peer *ring-group* **fst** *ip-address* [**lf** *size*]

no source-bridge remote-peer *ring-group* **fst** *ip-address*

Syntax Description

ring-group	Ring group number. This ring group number must match the number you specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.
ip-address	IP address of the remote peer with which the router will communicate.
lf *size*	(Optional) Maximum-sized frame to be sent to this remote peer, in bytes. The Cisco IOS software negotiates all transit routes down to this size or lower. Use the size argument to prevent timeouts in end hosts by reducing the amount of data they must send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800.

Defaults

No FST encapsulation connection is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The two peers using the serial-transport method will function correctly only if there are routers at the end of the serial line that have been configured to use the serial transport. The peers must also belong to the same ring group.

You must specify one **source-bridge remote-peer** command for each peer router that is part of the virtual ring. You must also specify one **source-bridge remote-peer** command to identify the IP address of the local router.

Examples

In the following example, the **source-bridge-fst-peername** command specifies an IP address of 10.136.64.98 for the local router. The **source-bridge ring-group** command assigns the device to a ring group. The **source-bridge remote-peer fst** command specifies ring group number 100 for the remote peer at IP address 10.136.64.97.

```
source-bridge fst-peername 10.136.64.98
source-bridge ring-group 100
source-bridge remote-peer 100 fst 10.136.64.97
```

source-bridge remote-peer interface

When specifying a point-to-point direct encapsulation connection, use the **source-bridge remote-peer interface** command in global configuration mode. To disable previous interface assignments, use the **no** form of this command.

source-bridge remote-peer *ring-group* **interface** *name number* [*mac-address*] [**lf** *size*]

no source-bridge remote-peer *ring-group* **interface** *name number*

Syntax Description

ring-group	Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.
interface *name number*	Name of the serial interface over which to send source-route bridged traffic.
mac-address	(Optional) MAC address for the interface you specify using the *name* argument. This argument is required for nonserial interfaces. You can obtain the value of this MAC address by using the **show interfaces** command, and then scanning the display for the interface specified by the *name* argument.
lf *size*	(Optional) Maximum size frame to be sent to this remote peer in bytes. The Cisco IOS software negotiates all transit routes down to this size or lower. The size argument is useful in preventing timeouts in end hosts by reducing the amount of data they must send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800.

Defaults

No point-to-point direct encapsulation connection is specified.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to identify the interface over which to send source-route bridged traffic to another router or bridge in the ring group. A serial interface does not require that you include a MAC-level address; all other types of interfaces do require MAC addresses.

It is possible to mix all types of transport methods within the same ring group.

Note The two peers using the serial-transport method will function correctly only if there are routers at the end of the serial line that have been configured to use the serial transport. The peers must also belong to the same ring group.

Examples

The following example shows how to send source-route bridged traffic over serial interface 0 and Ethernet interface 0:

```
! send source-route bridged traffic over serial 0
source-bridge remote-peer 5 interface serial 0
! specify MAC address for source-route bridged traffic on Ethernet 0
source-bridge remote-peer 5 interface ethernet 0 0000.0c00.1234
```

Related Commands

Command	Description
show interfaces	Displays statistics for the interfaces configured on a router or access server.
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

source-bridge remote-peer tcp

To identify the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP, use th**e source-bridge remote-peer tcp** command in global configuration mode. To remove a remote peer for the specified ring group, use the **no** form of this command.

source-bridge remote-peer *ring-group* **tcp** *ip-address* [**lf** *size*] [**tcp-receive-window** *wsize*] [**local-ack**] [**priority**]

no source-bridge remote-peer *ring-group* **tcp** *ip-address*

Syntax Description

ring-group	Ring group number. This ring group number must match the number you specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.
ip-address	IP address of the remote peer with which the router will communicate. The default is that no IP address is identified.
lf *size*	(Optional) Maximum size frame to be sent to this remote peer in bytes. The Cisco IOS software negotiates all transit routes down to this size or lower. The size argument is useful in preventing timeouts in end hosts by reducing the amount of data they must send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800.
tcp-receive-window *wsize*	(Optional) The TCP receive window size in bytes. The range is from 10240 to 65535 bytes. The default window size is 10240 bytes.
local-ack	(Optional) Logical Link Control, type 2 (LLC2) sessions destined for a specific remote peer are locally terminated and acknowledged. Use local acknowledgment for LLC2 sessions going to this remote peer.
priority	(Optional) Enables prioritization over a TCP network. You must specify the **local-ack** keyword earlier in the same **source-bridge remote-peer** command. The **priority** keyword is a prerequisite for features such as System Network Architecture (SNA) Class of Service (COS) and Systems Network Architecture (SNA) logical unit (LU) address prioritization over a TCP network.

Defaults

No IP address is identified.

The default window size is 10240 bytes.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **tcp-receive-window** keyword was added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you change the default TCP receive window size on one peer, you must also change the receive window size on the other peer. Both sides of the connection should have the same window size.

If you configure one peer for LLC2 local acknowledgment, you need to configure both peers for LLC2 local acknowledgment. If only one peer is so configured, unpredictable results occur.

You must specify one **source-bridge remote-peer** command for each peer router that is part of the virtual ring. You must also specify one **source-bridge remote-peer** command to identify the IP address of the local router.

The two peers using the serial-transport method will function correctly only if there are routers at the end of the serial line that have been configured to use the serial transport. The peers must also belong to the same ring group.

Examples

In the following example, the remote peer with IP address 10.108.2.291 belongs to ring group 5. It also uses LLC2 local acknowledgment, priority, and remote source-route bridging (RSRB) protocol version 2:

```
! identify the ring group as 5
source-bridge ring-group 5
! remote peer at IP address 10.108.2.291 belongs to ring group 5, uses
! tcp as the transport, is set up for local acknowledgment, and uses priority
source-bridge remote-peer 5 tcp 10.108.2.291 local-ack priority
```

The following example shows how to locally administer and acknowledge LLC2 sessions destined for a specific remote peer:

```
! identify the ring group as 100
source-bridge ring-group 100
! remote peer at IP address 10.1.1.1 does not use local acknowledgment
source-bridge remote-peer 100 tcp 10.1.1.1
! remote peer at IP address 10.1.1.2 uses local acknowledgment
source-bridge remote-peer 100 tcp 10.1.1.2 local-ack
!
interface tokenring 0
 source-bridge 1 1 100
```

Sessions between a device on Token Ring 0 that must go through remote peer 10.1.1.2 use local acknowledgment for LLC2, but sessions that go through remote peer 10.1.1.1 do *not* use local acknowledgment (that is, they “pass through”).

Related Commands

Command	Description
source-bridge	Configures an interface for source-route bridging (SRB).
source-bridge remote-peer fst	Specifies an FST encapsulation connection.
source-bridge remote-peer frame-relay	Specifies a point-to-point direct encapsulation connection.

source-bridge ring-group

To define or remove a ring group from the configuration, use the **source-bridge ring-group** command in global configuration mode. To cancel previous assignments, use the **no** form of this command.

source-bridge ring-group *ring-group* [*virtual-mac-address*]

no source-bridge ring-group *ring-group* [*virtual-mac-address*]

Syntax Description

ring-group	Ring group number. The valid range is from 1 to 4095.
virtual-mac-address	(Optional) 12-digit hexadecimal string written as a dotted triple of four-digit hexadecimal numbers (for example, 0010.0a00.20a6).

Defaults

No ring group is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To configure a source-route bridge with more than two network interfaces, the *ring group* arrangement is used. A ring group is a collection of Token Ring interfaces in one or more routers that are collectively treated as a virtual ring. The ring group is denoted by a ring number that must be unique for the network. The ring group's number is used just like a physical ring number, showing up in any route descriptors contained in packets being bridged.

To configure a specific interface as part of a ring group, set its target ring number parameter to the ring group number specified in this command. Do not use the number 0; it is reserved to represent the local ring.

To avoid an address conflict on the virtual MAC address, use a locally administered address in the form 4000.*xxxx.xxxx*.

Examples

In the following example, multiple Token Rings are source-route bridged to one another through a single router. These Token Rings are all part of ring group seven.

```
! all token rings attached to this bridge/router are part of ring group 7
source-bridge ring-group 7
!
interface tokenring 0
 source-bridge 1000 1 7
!
interface tokenring 1
 source-bridge 1001 1 7
!
interface tokenring 2
 source-bridge 1002 1 7
!
interface tokenring 3
 source-bridge 1003 1 7
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.

source-bridge route-cache

To enable fast switching, use the **source-bridge route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

source-bridge route-cache

no source-bridge route-cache

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, fast-switching software is enabled in the source-route bridging software. Fast switching allows for faster implementations of local source-route bridging between 4 to 16 MB Token Ring cards in the same router. This feature also allows for faster implementations of local source-route bridging between two routers using the 4 to 16 MB Token Ring cards and the direct interface encapsulation.

Examples

The following example disables use of fast switching between two 4 to 16 MB Token Ring interfaces:

```
interface token 0
 source-bridge 1 1 2
 no source-bridge route-cache
!
interface token 1
 source-bridge 2 1 1
 no source-bridge route-cache
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.

source-bridge route-cache cbus

To enable autonomous switching, use the **source-bridge route-cache cbus** command in interface configuration mode. To disable autonomous switching, use the **no** form of this command.

source-bridge route-cache cbus

no source-bridge route-cache cbus

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Autonomous switching in source-route bridging software is available for local source-route bridging between ciscoBus Token Ring cards in the same router. Autonomous switching provides higher switching rates than does fast switching between 4 to 16 MB Token Ring cards. Autonomous switching works for both two-port bridges and multiport bridges that use ciscoBus Token Ring cards.

In a virtual ring that includes both ciscoBus Token Ring and 4 to 16 MB Token Ring interfaces, frames that flow from one ciscoBus Token Ring interface to another are autonomously switched, and the remainder of the frames are fast switched. The switching that occurs on the ciscoBus Token Ring interface takes advantage of the high-speed ciscoBus controller processor.

Note Using either NetBIOS byte offset access lists or the access-expression capability to logically combine the access filters disables the autonomous or fast switching of source-route bridging (SRB) frames.

Examples

The following example enables use of autonomous switching between two ciscoBus Token Ring interfaces:

```
interface token 0
 source-bridge 1 1 2
 source-bridge route-cache cbus
 !
interface token 1
 source-bridge 2 1 1
```

```
source-bridge route-cache cbus
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.

source-bridge route-cache sse

To enable the Cisco silicon switching engine (SSE) switching function, use the **source-bridge route-cache sse** command in interface configuration mode. To disable SSE switching, use the **no** form of this command.

source-bridge route-cache sse

no source-bridge route-cache sse

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables use of SSE switching between two 4 to 16 MB Token Ring interfaces:

```
interface token 0
 source-bridge 1 1 2
 source-bridge route-cache sse
!
interface token 1
 source-bridge 2 1 1
 source-bridge route-cache sse
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.

source-bridge sap-80d5

To allow non-IBM hosts (attached to a router with 80d5 processing enabled) to use the standard Token Ring to Ethernet LLC2 translation instead of the nonstandard Token Ring to Ethernet 80d5 translation, use the **source-bridge sap-80d5** command in global configuration mode. To disable this feature, use the **no** form of this command.

source-bridge sap-80d5 *dsap*

no source-bridge sap-80d5 *dsap*

Syntax Description

dsap	Destination service access point (DSAP).

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command allows you to set the translation on a per-destination service access point (DSAP) basis.

By default, the following DSAPs are enabled for 0x80d5 translation by specifying the **source-bridge enable-80d5** command:

- For Systems Network Architecture (SNA)—04, 08, 0C, 00
- For NetBIOS—F0

Any of these DSAPs can be disabled with the **no** form of this command.

The parameters specifying the current parameters for the processing of 0x80d5 frames are given at the end of the output of the **show span** command.

Note The 80d5 frame processing option is available only with source-route translational bridging (SR/TLB). It is not available when source-route transparent bridging (SRT) is used.

Use the **show span** to verify that 80d5 processing is enabled for a particular DSAP. The following line is displayed in the output if 80d5 processing is enabled, listing each DSAP for which it is enabled:

```
Translation is enabled for the following DSAPs:
 04 0C 1C F0
```

Examples

The following example enables 0x80d5 processing, removes the translation for SAP 08, and adds the translation for SAP 1c:

```
source-bridge enable-80d5
no source-bridge sap-80d5 08
source-bridge sap-80d5 1c
```

Related Commands

Command	Description
show span	Displays the spanning-tree topology known to the router.
source-bridge enable-80d5	Changes the Token Ring of the router to Ethernet translation behavior.

source-bridge sdllc-local-ack

To activate local acknowledgment for SDLC Logical Link Control. Cisco (SDLLC) sessions on a particular interface, use th**e source-bridge sdllc-local-ack** command in global configuration mode. To deactivate local acknowledgment for SDLLC sessions, use the **no** form of this command.

source-bridge sdllc-local-ack

no source-bridge sdllc-local-ack

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command must be issued only on a router with a serial interface. Once the command is issued, *all* SDLLC sessions between the two devices will be locally acknowledged. You cannot selectively choose which SDLLC sessions are to be locally acknowledged and which are not. Also, local acknowledgment is not supported when the Logical Link Control, type 2 (LLC2) station is attached to Ethernet rather than to Token Ring.

Note You must use the TCP encapsulation option if you use local acknowledgment for SDLLC.

Examples

The following example activates local acknowledgment for SDLLC sessions:

```
source-bridge ring-group 100
source-bridge remote-peer 100 tcp 10.108.1.1 local-ack
source-bridge remote-peer 100 tcp 10.108.2.2
source-bridge sdllc-local-ack
```

source-bridge spanning (automatic)

To enable the automatic spanning-tree function for a specified group of bridged interfaces, use the automatic version of the **source-bridge spanning** command in interface configuration mode. To return to the default disabled state, use the **no** form of this command.

source-bridge spanning *bridge-group* [**path-cost** *path-cost*]

no source-bridge spanning *bridge-group* [**path-cost** *path-cost*]

Syntax Description

bridge-group	Number in the range from 1 to 9 that you choose to refer to a particular group of bridged interfaces. This must be the same number as assigned in the **bridge protocol ibm** command.
path-cost	(Optional) Assign a path cost for a specified interface.
path-cost	(Optional) Path cost for the interface. The valid range is from 0 to 65535.

Defaults

The automatic spanning-tree function is disabled. The default path cost is 16.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To return an assigned path cost to the default path cost of 16, use the **no source-bridge spanning path-cost** command.

Examples

The following example adds Token Ring 0 to bridge group 1 and assigns a path cost of 12 to Token Ring 0:

```
interface tokenring 0
 source-bridge spanning 1 path-cost 12
```

Related Commands

Command	Description
bridge protocol ibm	Creates a bridge group that runs the automatic spanning-tree function.
show source-bridge	Displays the current source bridge configuration and miscellaneous statistics.

source-bridge spanning (manual)

To enable use of spanning explorers, use the **source-bridge spanning** command in interface configuration mode. To disable the use of spanning explorers, use the **no** form of this command.

source-bridge spanning

no source-bridge spanning

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only spanning explorers will be blocked; everything else will be forwarded. Use of the **source-bridge spanning** command is recommended. This command puts the interface into a forwarding or active state with respect to the spanning tree. Two types of explorer packets are used to collect Routing Information Field (RIF) information:

- All-rings, all-routes explorer packets follow all possible paths to a destination ring. In a worst-case scenario, the number of all-rings explorers generated may be exponentially large.
- Spanning or limited-route explorer packets follow a spanning tree when looking for paths, greatly reducing the number of explorer packets required. There is no dynamic spanning-tree algorithm to establish that spanning tree; it must be manually configured.

Examples

The following example enables use of spanning explorers:

```
! Global configuration command establishing the ring group for the interface
! configuration commands
source-bridge ring-group 48
!
! commands that follow apply to interface token 0
interface tokenring 0
! configure interface tokenring 0 to use spanning explorers
 source-bridge spanning
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.

source-bridge tcp-queue-max

To modify the size of the backup queue for remote source-route bridging, use the **source-bridge tcp-queue-max** command in global configuration mode. To return to the default value, use the **no** form of this command.

source-bridge tcp-queue-max *number*

no source-bridge tcp-queue-max

Syntax Description

number	Number of packets to hold in any single outgoing TCP queue to a remote router. The default is 100 packets.

Defaults

The default number of packets is 100.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This backup queue determines the number of packets that can wait for transmission to a remote ring before packets start being thrown away.

Examples

If, for example, your network experiences temporary bursts of traffic using the default packet queue length, the following command raises the limit from 100 to 150 packets:

```
source-bridge tcp-queue-max 150
```

source-bridge transparent

To establish bridging between transparent bridging and source-route bridging (SRB), use the **source-bridge transparent** command in global configuration mode. To disable a previously established link between a source-bridge ring group and a transparent-bridge group, use the **no** form of this command.

source-bridge transparent *ring-group pseudoring bridge-number tb-group* [*oui*]

no source-bridge transparent *ring-group pseudoring bridge-number tb-group*

Syntax Description

ring-group	Virtual ring group created by the **source-bridge ring-group** command. This is the source-bridge virtual ring to associate with the transparent-bridge group. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.
pseudoring	Ring number used to represent the transparent bridging domain to the source-route bridged domain. This number must be a unique number, not used by any other ring in your source-route bridged network.
bridge-number	Bridge number of the bridge that leads to the transparent bridging domain.
tb-group	Number of the transparent bridge group that you want to tie into your source-route bridged domain. The **no** form of this command disables this feature.
oui	(Optional) Organizational unique identifier. Values are the following: • **90-compatible** • **standard** • **cisco**

Defaults

Not established

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before using this command, you must have completely configured your router using multiport source-bridging and transparent bridging.

Specify the **90-compatible** keyword oui when talking to Cisco routers. This OUI provides the most flexibility. Specify the **standard** keyword oui when talking to IBM 8209 bridges and other vendor equipment. This oui does not provide for as much flexibility as the other two choices. The **cisco** keyword oui is provided for compatibility with future equipment.

Do not use the **standard** keyword oui unless you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity. Use the **standard** keyword only when you are transferring data between IBM 8209 Ethernet/Token Ring bridges and routers running the source-route translational bridging (SR/TLB) software (to create a Token Ring backbone to connect Ethernets). Use of the **standard** keyword causes the OUI code in Token Ring frames to always be 0x000000. In the context of the **standard** keyword, an OUI of 0x000000 identifies the frame as an Ethernet Type II frame. If the OUI in Token Ring frame is 0x000000 SR/TLB will output an Ethernet Type II frame.

When 8209 compatibility is enabled with the **ethernet transit-oui standard** command, the SR/TLB chooses to translate all Token Ring Subnetwork Access Protocol (SNAP) frames into Ethernet Type II frames as described earlier in this chapter.

Examples

The following example establishes bridging between a transparent-bridge network and a source-route network:

```
source-bridge ring-group 9
source-bridge transparent 9 6 2 2
!
interface tokenring 0
 source-bridge 5 2 9
!
interface token ring 1
 source bridge 4 2 9
!
interface ethernet 0
 bridge-group 2
!
interface ethernet 1
 bridge-group 2

bridge 2 protocol ieee
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
ethernet transit-oui standard	Chooses Organizational Unique Identifier (OUI) code to encapsulate Ethernet Type II frames across Token Ring backbone networks.
source-bridge	Configures an interface for SRB.
source-bridge ring-group	Defines or removes a ring group from the configuration.

source-bridge transparent fastswitch

To enable fast switching of packets between the source-route bridging (SRB) and transparent domains, use the **source-bridge transparent fastswitch** command in global configuration mode. To disable fast switching of packets, use the **no** form of this command.

source-bridge transparent *ring-group* **fastswitch**

no source-bridge transparent *ring-group* **fastswitch**

Syntax Description

ring-group	Virtual ring group created by the **source-bridge ring-group** command. This is the source-bridge virtual ring to associate with the transparent-bridge group. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.
fastswitch	Fast-switched source-route translational bridging (SR/TLB) enables the Cisco IOS software to process packets at the interrupt level.

Defaults

Fast-switched SR/TLB is enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Because fast-switched SR/TLB is enabled by default when the router is configured for SR/TLB, there are no user-specified changes to the operation of the router, and the enabling command does not appear in the configuration.

The **no source-bridge transparent** *ring-group* **fastswitch** command is provided to disable fast-switched SR/TLB, causing the router to handle packets by process switching. When fast-switched SR/TLB is disabled, the **no** form of the command appears on a separate line of the configuration, immediately following the parent **source-bridge transparent** command.

If fast-switched SR/TLB has been disabled, it can be enabled using the **source-bridge transparent** *ring-group* **fastswitch** command, but the enabling form of the command will not appear in the configuration.

Examples

The following example disables fast-switched SR/TLB between a transparent-bridge network and a source-route network:

```
source-bridge ring-group 9
source-bridge transparent 9 6 2 2
no source-bridge transparent 9 fastswitch
!
interface tokenring 0
 source-bridge 5 2 9
!
interface token ring 1
 source bridge 4 2 9
!
interface ethernet 0
 bridge-group 2
!
interface ethernet 1
 bridge-group 2

bridge 2 protocol ieee
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
source-bridge	Configures an interface for SRB.
source-bridge ring-group	Defines or removes a ring group from the configuration.

state-tracks-signal

To allow the channel interface state to track the state of the physical interface signal on a Channel Port Adapter (CPA), use the **state-tracks-signal** command in interface configuration mode. To disable tracking of the physical interface signal on a CPA interface, use the **no** form of this command.

state-tracks-signal

no state-tracks-signal

Syntax Description

This command has no arguments or keywords.

Defaults

The physical interface signal is not tracked.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(4.1)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **state-tracks-signal** command is useful in environments where you are using Hot Standby Router Protocol (HSRP) or Simple Network Management Protocol (SNMP) alerts to monitor channel interface status.

The **state-tracks-signal** command is valid only on channel interfaces which combine the functions of both a physical and virtual interface. The ESCON Channel Port Adapter (ECPA) and Parallel Channel Port Adapter (PCPA) are examples of this type of channel interface. The command is not valid for the Channel Interface Processor (CIP), which has a separate channel interface for the virtual channel functions.

When the **state-tracks-signal** command is used on an interface that has been started by the **no shutdown** command, then the state of the channel interface is reported according to the status of the physical channel interface signal. If the physical channel interface signal is not present, then the channel interface status is DOWN/DOWN.

When the **no state-tracks-signal** command is enabled on the channel interface (the default), and the interface has been started by the **no shutdown** command, the channel interface status is always reported as UP/UP, even when there is no signal present on the physical connection. This configuration is useful for TN3270 server environments that are operating in a mode without any physical channel interface connections.

Examples

The following example specifies that the channel interface state tracks the physical channel interface signal and reports the channel interface state according to the presence or absence of the physical interface signal when the interface has been started by the **no shutdown** command:

```
interface channel 5/0
 state-tracks-signal
```

stun group

To place each serial tunnel (STUN)-enabled interface on a router in a previously defined STUN group, use the **stun group** command in interface configuration mode. To remove an interface from a group, use the **no** form of this command.

stun group *group-number*

no stun group *group-number*

Syntax Description

group-number	Integer in the range from 1 to 255.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before using this command, perform the following steps:

- Enable STUN on a global basis with the **stun peer-name** command.
- Define the protocol group in which you want to place this interface using the **stun protocol-group** command.
- Enable STUN on the interface using the **encapsulation stun** command.

  Packets only travel between STUN-enabled interfaces that are in the same group. Once a given serial link is configured for the STUN function, it is no longer a shared multiprotocol link. All traffic that arrives on the link is transported to the corresponding peer as determined by the current STUN configuration.

Examples

The following example places serial interface 0 in STUN group 2, which is defined to run the Synchronous Data Link Control (SDLC) transport:

```
! sample stun peer-name global command
stun peer-name 10.108.254.6
! sample protocol-group command telling group 2 to use the SDLC protocol
stun protocol-group 2 sdlc
!
interface serial 0
! sample ip address subcommand
 no ip address
! sample encapsulation stun subcommand
 encapsulation stun
! place interface serial0 in previously defined STUN group 2
 stun group 2
! enter stun route command
 stun route 7 tcp 10.108.254.7
```

Related Commands

Command	Description
encapsulation stun	Enables STUN encapsulation on a specified serial interface.
priority-list protocol stun address	Establishes STUN queueing priorities based on the address of the serial link.
stun peer-name	Enables STUN for an IP address.
stun protocol-group	Creates a protocol group.

stun keepalive-count

To define the number of times to attempt a peer connection before declaring the peer connection to be down, use the **stun keepalive-count** command in global configuration mode. To cancel the definition, use the **no** form of this command.

stun keepalive-count *count*

no stun keepalive-count

Syntax Description

count	Number of connection attempts. The range is from from 2 to 10 retries.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the number of times to retry a connection to a peer to 4:

```
stun keepalive-count 4
```

Related Commands

Command	Description
stun remote-peer-keepalive	Enables detection of the loss of a peer.

stun peer-name

To enable serial tunnel (STUN) for an IP address, use the **stun peer-name** command in global configuration mode. To disable STUN for an IP address, use the **no** form of this command.

stun peer-name *ip-address* **cls**

no stun peer-name *ip-address* **cls**

Syntax Description

ip-address	IP address by which this STUN peer is known to other STUN peers.
cls	Use Cisco Link Services (CLS) to access the Frame Relay network.

Defaults

STUN is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enable any further STUN features. After using this command, perform the following steps:

- Define the protocol group in which you want to place this interface with the **stun protocol-group** command.
- Enable STUN on the interface using the **encapsulation stun** command.
- Place the interface in a STUN group using with the **stun group** command.

Examples

The following example assigns IP address 10.108.254.6 as the STUN peer:

```
stun peer-name 10.108.254.6 cls
```

Related Commands

Command	Description
encapsulation stun	Enables STUN encapsulation on a specified serial interface.
stun group	Places each STUN-enabled interface on a router in a previously defined STUN group.
stun protocol-group	Creates a protocol group.

stun protocol-group

To create a protocol group, use the **stun protocol-group** command in global configuration mode. To remove an interface from the group, use the **no** form of this command.

stun protocol-group *group-number* {**basic** | **sdlc** [**sdlc-tg**] | **schema**}

no stun protocol-group

Syntax Description

group-number	Integer in the range from 1 to 255.
basic	Indicates a non-Synchronous Data Link Control (SDLC) protocol.
sdlc	Indicates an Synchronous Data Link Control (SDLC) protocol.
sdlc-tg	(Optional) Identifies the group as part of an Systems Network Architecture (SNA) Transmission Group (TG).
schema	Indicates a custom protocol.

Defaults

No protocol group established.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **sdlc** keyword to specify an SDLC protocol. You must specify either the **sdlc** or the **sdlc-tg** keyword before you can enable SDLC local acknowledgment. SDLC local acknowledgment is established with the **stun route address tcp** command.

Use the **basic** keyword to specify a non-SDLC protocol, such as high-level data link control (HDLC).

Use the **schema** keyword to specify a custom protocol. The custom protocol must have been previously created with the **stun schema** command.

Use the optional **sdlc-tg** keyword, in conjunction with the **sdlc** keyword, to establish an SNA TG. A TG is a set of protocol groups providing parallel links to the same pair of IBM establishment controllers. This provides redundancy of paths. In case one or more links go down, an alternate path will be used. All serial tunnel (STUN) connections in a TG must connect to the same IP address. SDLC local acknowledgment must be enabled.

Note If you specify the **sdlc** keyword in the **stun protocol group** command string, you cannot specify the **stun route all** command on that interface.

Examples

The following example specifies that group 7 will use the Synchronous Data Link Control (SDLC) STUN protocol to route frames within that group:

```
stun protocol-group 7 sdlc
```

The following example specifies that group 5 use the basic protocol, wherein the serial addressing is unimportant and you have a point-to-point link:

```
stun protocol-group 5 basic
```

Related Commands

Command	Description
encapsulation stun	Enables STUN encapsulation on a specified serial interface.
stun route address interface serial	Forwards all HDLC traffic on a serial interface.
stun route address tcp	Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for STUN.
stun schema offset length format	Defines a protocol other than SDLC for use with STUN.

stun quick-response

To enable serial tunnel (STUN) quick-response, which can be used with local acknowledgment, use the **stun quick-response** command in global configuration mode. To disable STUN quick-response, use the **no** form of this command.

stun quick-response

no stun quick-response

Syntax Description

This command has no arguments or keywords.

Defaults

STUN quick-response is disabled.

Command Modes

Global configuration

Command History

Release	Modification
10.3(5)	This command was introduced.\
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is used with local acknowledgment (local ack).

When STUN quick-response is enabled, the router responds to an exchange identification (XID) or a Set Normal Response Mode (SNRM) request with a Disconnect Mode (DM) response when the device is not in the CONNECT state. The request is then passed to the remote router and, if the device responds, the reply is cached. The next time the device is sent an XID or SNRM, the router replies with the cached DM response.

Note Using STUN quick-response avoids an AS/400 line reset problem by eliminating the Non-Productive Receive Timer (NPR) expiration in the AS/400. With quick-response enabled, the AS/400 receives a response from the polled device, even when the device is down. If the device does not respond to the forwarded request, the router continues to respond with the cached DM response.

Examples

The following example enables STUN quick-response:

```
stun quick-response
```

Related Commands

Command	Description
stun route address interface dlci	Configures direct Frame Relay encapsulation between STUN peers with Synchronous Data Link Control (SDLC) local acknowledgment.
stun route address interface serial	Forwards all high-level data link control (HDLC) traffic on a serial interface.
stun route address tcp	Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for STUN.
stun route all interface serial	Encapsulates and forwards all STUN traffic using HDLC encapsulation on a serial interface.
stun route all tcp	Used with TCP encapsulation, forwards all STUN traffic on an interface regardless of which address is contained in the serial frame.

stun remote-peer-keepalive

To enable detection of the loss of a peer, use the **stun remote-peer-keepalive** command in global configuration mode. To disable detection, use the **no** form of this command.

stun remote-peer-keepalive *seconds*

no stun remote-peer-keepalive

Syntax Description

seconds	Keepalive interval, in seconds. The range is from 1 to 300 seconds. The default is 30 seconds.

Defaults

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the remote peer keepalive interval is set to 60 seconds:

```
stun remote-peer-keepalive 60
```

Related Commands

Command	Description
stun keepalive-count	Defines the number of times to attempt a peer connection before declaring the peer connection to be down.

stun route address interface dlci

To configure direct Frame Relay encapsulation between serial tunnel (STUN) peers with Synchronous Data Link Control (SDLC) local acknowledgment, use the **stun route address interface dlci** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

stun route address *sdlc-addr* **interface** *frame-relay-port* **dlci** *number localsap* **local-ack cls**

no stun route address *sdlc-addr* **interface** *frame-relay-port* **dlci** *number localsap* **local-ack cls**

Syntax Description

sdlc-addr	Address of the serial interface.
frame-relay-port	Port number.
number	Data-link connection identifier (DLCI) number.
localsap	Local connecting service access point (SAP).
local-ack	Enable local acknowledgment.
cls	Use Cisco Link Services (CLS) to access the Frame Relay network.

Defaults

The configuration is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following command enables Frame Relay encapsulation between STUN peers with SDLC local acknowledgment:

```
stun route address c1 interface serial1 dlci 22 04 local-ack
```

Related Commands

Command	Description
stun route all interface serial	Encapsulates and forwards all STUN traffic using high-level data link control (HDLC) encapsulation on a serial interface.

stun route address interface serial

To forward all high-level data link control (HDLC) traffic on a serial interface, use the **stun route address interface serial** command in interface configuration mode. To disable this method of HDLC encapsulation, use the **no** form of this command.

stun route address *address-number* **interface serial** *number* [**direct**]

no stun route address *address-number* **interface serial** *number*

Syntax Description

address-number	Address of the serial interface.
number	Number assigned to the serial interface.
direct	(Optional) Forwards all HDLC traffic on a direct serial tunnel (STUN) link.

Defaults

The configuration is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, serial frames with a STUN route address of 4 are forwarded through serial interface 0 using HDLC encapsulation:

```
stun route address 4 interface serial 0
```

In the following example, serial frames with STUN route address 4 are propagated through serial interface 0 using STUN encapsulation:

```
stun route address 4 interface serial 0 direct
```

Related Commands

Command	Description
stun route all interface serial	Encapsulates and forwards all STUN traffic using HDLC encapsulation on a serial interface.

stun route address tcp

To specify TCP encapsulation and optionally establish Synchronous Data Link Control (SDLC) local acknowledgment (SDLC transport) for serial tunnel (STUN), use the **stun route address tcp** command in interface configuration mode. To disable this method of TCP encapsulation, use the **no** form of this command.

stun route address *address-number* **tcp** *ip-address* [**local-ack**] [**priority**] [**tcp-queue-max**] [**passive**]

no stun route address *address-number* **tcp** *ip-address* [**local-ack**] [**priority**] [**tcp-queue-max**] [**passive**]

Syntax Description

address-number	Number that conforms to SDLC addressing conventions.
ip-address	IP address by which this STUN peer is known to other STUN peers that are using the TCP as the STUN encapsulation.
local-ack	(Optional) Enables local acknowledgment for STUN.
priority	(Optional) Establishes the four levels used in priority queueing: low, medium, normal, and high.
tcp-queue-max	(Optional) Sets the maximum size of the outbound TCP queue for the SDLC link. The default is 100.
passive	(Optional) Prevents the STUN peer from initiating a TCP connection. Normally, the STUN peer connects to the SDLC primary device and initiates a TCP connection to another STUN peer. If the STUN peers connect to non-SDLC devices, such as voice equipment, both STUN peers might try to start a TCP connection at the same time, which can delay the TCP connection setup. The **passive** keyword, used in STUN basic mode, enables this STUN peer to wait for the other STUN peer to initiate the TCP connection.

Defaults

TCP encapsulation is not established; TCP queue size default is 100.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **tcp-queue-max** keyword was added.
12.0	The **passive** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SDLC transport participates in SDLC windowing and resending through support of local acknowledgment. SDLC sessions require that end nodes send acknowledgments for a set amount of data frames received before allowing further data to be sent. Local acknowledgment provides local termination of the SDLC session, so that control frames no longer travel the WAN backbone networks. This means that end nodes do not time out, and a loss of sessions does not occur.

Examples

In the following example, a frame with a source-route address of 10 is propagated using TCP encapsulation to a device with an IP address of 10.108.8.1:

```
stun route address 10 tcp 10.108.8.1
```

Related Commands

Command	Description
sdlc address ff ack-mode	Configures the IBM reserved address FF as a valid local address.
stun route all tcp	Used with TCP encapsulation, forwards all STUN traffic on an interface regardless of which address is contained in the serial frame.

stun route all interface serial

To encapsulate and forward all serial tunnel (STUN) traffic using high-level data link control (HDLC) encapsulation on a serial interface, use the **stun route all interface serial** command in interface configuration mode. To disable this method of encapsulation, use the **no** form of this command.

stun route all interface serial *number* [**direct**]

no stun route all interface serial *number* [**direct**]

Syntax Description

number	Number assigned to the serial interface.
direct	(Optional) Indicates that the specified interface is also a direct STUN link, rather than a serial connection to another peer.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An appropriately configured router must exist on the other end of the designated serial line. The outgoing serial link still can be used for other kinds of traffic (the frame is not TCP encapsulated). This mode is used when TCP/IP encapsulation is not needed or when higher performance is required. Enter the serial line number connected to the router for the *number* argument.

Examples

In the following example, all traffic on serial interface 0 is propagated using STUN encapsulation:

```
stun route all interface serial 0
```

In the following example, serial interface 1 is a direct STUN link, not a serial connection to another peer:

```
stun route all interface serial 1 direct
```

Related Commands

Command	Description
stun route address interface serial	Forwards all HDLC traffic on a serial interface.

stun route all tcp

To forward all serial tunnel (STUN) traffic on an interface regardless of which address is contained in the serial frame, use the **stun route all tcp** command in interface configuration mode with TCP encapsulation. To disable traffic from being forwarded with this method of encapsulation, use the **no** form of this command.

stun route all tcp *ip-address* [**passive**]

no stun route all tcp *ip-address* [**passive**]

Syntax Description

ip-address	IP address by which this remote STUN peer is known to other STUN peers. Use the address that identifies the remote STUN peer that is connected to the remote serial link.
passive	(Optional) Prevents the STUN peer from initiating a TCP connection. Normally, the STUN peer connects to the Synchronous Data Link Control (SDLC) primary device and initiates a TCP connection to another STUN peer. If the STUN peers connect to non-SDLC devices, such as voice equipment, both STUN peers might start a TCP connection at the same time. The **passive** keyword enables a delay when setting up a TCP connection.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0	The **passive** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

TCP/IP encapsulation allows movement of serial frames across arbitrary media types and topologies. This is particularly useful for building shared, multiprotocol enterprise network backbones.

Examples

In the following example, all STUN traffic received will be propagated through the bridge:

```
stun route all tcp 10.108.10.1
```

stun schema offset length format

To define a protocol other than Synchronous Data Link Control (SDLC) for use with serial tunnel (STUN), use the **stun schema offset length format** command in global configuration mode. To disable the new protocol, use the **no** form of this command.

stun schema *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*

no stun schema *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*

Syntax Description

name	Name that defines your protocol. It can be up to 20 characters in length.
constant-offset	Constant offset, in bytes, for the address to be found in the frame.
address-length	Length in one of the following formats: decimal (4 bytes), hexadecimal (8 bytes), or octal (4 bytes).
format-keyword	Identifies the format to be used to specify and display addresses for routes on interfaces that use this STUN protocol. Valid format keyword values and their ranges are: • **decimal**—0 to 9 • **hexadecimal**—0 to F • **octal**—0 to 7

Defaults

No protocol is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command before defining the protocol group (**stun protocol-group** command). The serial protocol you define must meet the following criteria:

- The protocol uses full-duplex conventions (Request To Send [RTS]/Clear To Send [CTS] always high).
- The protocol uses standard high-level data link control (HDLC) checksum and framing (beginning and end of frames, data between frames).
- Addresses are contained in a constant location (offset) within the frame.
- Addresses are found on a byte boundary.

Examples

In the following example, a protocol named new-sdlc is created. In the protocol frame structure, the constant offset is 0, the address length is 1 byte, and the address format is hexadecimal.

```
stun schema new-sdlc offset 0 length 1 format hexadecimal
```

Related Commands

Command	Description
priority-list protocol stun address	Establishes STUN queueing priorities based on the address of the serial link.
stun protocol-group	Creates a protocol group.

stun sdlc-role primary

To assign the router the role of Synchronous Data Link Control (SDLC) primary node, use the **stun sdlc-role primary** command in interface configuration mode. To disable the primary node role assignment, use the **no** form of this command.

stun sdlc-role primary

no stun sdlc-role

Syntax Description

This command has no arguments or keywords.

Defaults

No role is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Primary nodes poll secondary nodes in a predetermined order.

If the router is connected to a cluster controller, for example a 3x74, it should appear as a front-end processor (FEP) such as a 37x5, and must be assigned the role of a primary node.

Examples

The following example assigns the router the role of SDLC primary node:

```
stun sdlc-role primary
```

Related Commands

Command	Description
encapsulation stun	Enables serial tunnel (STUN) encapsulation on a specified serial interface.
stun sdlc-role secondary	Assigns the router the role of SDLC secondary node. Secondary nodes respond to polls sent by the SDLC primary by sending any outgoing data they may have.

stun sdlc-role secondary

To assign the router the role of Synchronous Data Link Control (SDLC) secondary node, use the **stun sdlc-role secondary** command in interface configuration mode. To disable the assignment, use the **no** form of this command.

stun sdlc-role secondary

no stun sdlc-role

Syntax Description

This command has no arguments or keywords.

Defaults

No secondary role is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Secondary nodes respond to polls sent by the SDLC primary by sending any outgoing data they may have.

If the router is connected to a front-end processor (FEP), for example a 37x5, it should appear as a cluster controller such as a 3x74, and must be assigned the role of a secondary node.

Examples

The following example assigns the router the role of SDLC secondary node:

```
stun sdlc-role secondary
```

Related Commands

Command	Description
encapsulation stun	Enables serial tunnel (STUN) encapsulation on a specified serial interface.
stun sdlc-role primary	Assigns the router the role of SDLC primary node. Primary nodes poll secondary nodes in a predetermined order.

subscriber-policy

To define or modify the forward and filter decisions of the subscriber policy, use the **subscriber-policy** command in global configuration mode.

subscriber-policy *policy* [[**no** | **default**] *packet* [**permit** | **deny**]]

Syntax Description

policy	Subscriber policy number in the range from 1 to 100.
no	(Optional) Turn off the permit for the packet (this is an equivalent of the **deny** keyword).
default	(Optional) Deny forwarding of the packet (this is an equivalent of the **deny** keyword).
packet	(Optional) One of the following packets: • **arp** • **broadcast** • **cdp** • **multicast** • **st** • **unknown unicast**
permit	(Optional) Permit forwarding of the packet.
deny	(Optional) Deny forwarding of the packet.

Defaults

Table 99 shows the default values that are applied if no forward or filter decisions have been specified for the subscriber policy:

Table 99 Packet Default Values

Packet	Upstream
ARP	Permit
Broadcast	Deny
CDP	Deny/Disable
Multicast	Permit
Spanning Tree Protocol	Deny/Disable
Unknown Unicast	Deny

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

As an alternative to the command syntax described, you can enter the **subscriber-policy** *policy* command, followed by the specific forward or filter decisions for each packet.

There is not a **no** form for this command.

Examples

The following example changes the Address Resolution Protocol (ARP) behavior and the multicast behavior from permit to deny:

```
subscriber-policy 3 arp deny
subscriber-policy 3 multicast deny
```

The following example changes the ARP behavior and the multicast behavior from permit to deny, using the alternative syntax shown in the usage guidelines section:

```
subscriber-policy 3
arp deny
multicast deny
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.
bridge subscriber-policy	Binds a bridge group with a subscriber policy.
show subscriber-policy	Displays the details of a subscriber policy.

tcp-port

To override the default TCP port setting of 23, use the **tcp-port** command in TN3270 server, Dependent Logical Unit Requestor (DLUR) physical unit (PU), or PU configuration mode. To restore the default, use the **no** form of this command.

tcp-port *port-number*

no tcp-port

Syntax Description

port-number	A valid TCP port number in the range from 0 to 65534. The default is 23, which is the Internet Engineering Task Force (IETF) standard. The value 65535 is reserved by the TN3270 server.

Defaults

TN3270 server configuration mode: 23.

PU configuration mode: the value configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration

DLUR PU configuration

PU configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **tcp-port** command is valid only on the virtual channel interface, and it can be entered in either TN3270 server, DLUR PU or PU configuration mode. A value entered in TN3270 mode applies to all PUs for that TN3270 server, except as overridden by values entered in PU configuration mode. The **tcp-port** command affects only future TN3270 sessions.

The **tcp-port** command entered in DLUR PU configuration mode applies to all PUs defined under DLUR configuration mode.

The **no tcp-port** command entered in PU configuration mode removes the override. In this mode, the **tcp-port** command applies only to the specified PU.

Examples

The following example entered in TN3270 server configuration mode returns the TCP port value to 23:

```
no tcp-port
```

Related Commands

Command	Description
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.

tg (CMPC)

Note Effective with release 12.3(4)T, the **tg (CMPC)** command is no longer available in Cisco IOS software.

To define Logical Link Control (LLC) connection parameters for the Cisco Multipath Channel (CMPC) transmission group, use the **tg** command in interface configuration mode. To remove the specified transmission group from the configuration, which also deactivates the transmission group, use the **no** form of this command.

tg *tg-name* **llc** *token-adapter adapter-number lsap* [**rmac** *rmac*] [**rsap** *rsap*]

no tg *tg-name* **llc**

Syntax Description

tg-name	Name of the CMPC Transmission Group (TG). The maximum length of the name is eight characters. This must match the name specified by the **cmpc** commands.
llc	Specifies that this TG is connected to the LLC stack on the Cisco Mainframe Channel Connection (CMCC) adapter card.
token-adapter	Internal adapter type on the CMCC adapter card. The supported type is token-adapter.
adapter-number	Internal adapter number on the CMCC adapter card, which is the same value specified in the **adapter** internal LAN configuration command.
lsap	Local service access point (SAP) number, 04 to FC, in hexadecimal. The value must be an even number and should be a multiple of four. It must be unique within the internal adapter in that no other IEEE 802.2 clients of that adapter, in the router or in a host, can use the same SAP. The default value is 04.
rmac *rmac*	(Optional) Remote MAC address of the form *xxxx.xxxx.xxxx* in hexadecimal. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.
rsap *rsap*	(Optional) Remote SAP address, 04 to FC in hexadecimal. The value for the *rsap* argument must be an even number and should be a multiple of 4, but this requirement is not enforced. The default value for the *rsap* argument is 04.

Defaults

The *lsap* and *rsap* values default to 04.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.3(4)T	This command was removed and is no longer available in Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **tg** (CMPC) command is valid only on the virtual channel interface. This command defines an LLC connection with a complete addressing 4-tuple. The *lsap*, *rmac*, and *rsap* arguments are specified explicitly by parameters. The *lmac* argument is the local MAC address of the adapter referred to by the *type* and *adapter-number* arguments.

To change any parameter of the **tg** (CMPC) command, first remove the existing TG by using the **no tg** command.

The **no tg** command removes the CMPC TG from the configuration. If the TG is used for a High-Performance Routing (HPR) connection, all sessions using the TG will be terminated immediately. If the TG is an HPR connection, all sessions using the TG will be terminated if no other HPR connection is available to the host.

Examples

The following example configures a TG name and includes values for the *rmac* and *rsap* arguments:

```
tg LAGUNAA llc token-adapter 1 18 rmac 4000.0000.beef rsap 14
```

Related Commands

Command	Description
adapter	Configures internal adapters.
lan	Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode.

tg (CMPC+)

To define IP connection parameters for the Cisco Multipath Channel (CMPC+) transmission group, use the **tg** command in interface configuration mode. To remove the specified transmission group from the configuration and deactivate the transmission group, use the **no** form of this command.

tg *tg-name* {**ip** | **hsas-ip**} *host-ip-addr local-ip-addr* [**broadcast**]

no tg *tg-name* {**ip** | **hsas-ip**}

Syntax Description

tg-name	Name of the CMPC+ Transmission Group (TG). The maximum length of the name is eight characters. This name must match the name specified on the **cmpc** statements.
ip	Specifies that this TG is connected to the TCP/IP stack.
hsas-ip	Specifies that this TG is connected to the High Speed Access Services (HSAS) IP stack.
host-ip-addr	Specifies the IP address of the channel-attached host using this TG. A host may have more than one IP stack, therefore this is the IP address of the host IP stack as indicated by the HOME statement in the host TCP/IP profile. For HSAS, this address is the host address as indicated by the *source-IP-address* argument of the **oeifconfig** command.
local-ip-addr	This address must match an IP address configured on the virtual interface. Specifies the IP address of the router to be used for this TG. This is the IP address of the router as indicated by the DEFAULTNET statement in the host TCP/IP profile. For HSAS, this address is the router IP address as indicated by the *destination-IP-address* argument of the **oeifconfig** command.
broadcast	(Optional) Enables the sending of routing updates to the host.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **tg** (CMPC+) command is valid only on the Channel Interface Processor's (CIP) virtual channel interface and the Channel Port Adapter's (CPA) physical channel interface. This command defines either an IP connection or an HSAS IP connection.

To change any parameter of the **tg** (CMPC+) command, first remove the existing TG must be removed first by using **no tg** *name* command. At a minimum, *tg-name* must be specified to avoid ambiguity.

The **no tg** command removes the CMPC+ TG from the configuration. All sessions using the TG are terminated immediately.

Examples

The following example configures a TG name for an HSAS stack configured with CMPC+:

```
interface Channel0/2
 ip address 10.12.165.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip route-cache same-interface
 no ip mroute-cache
 no keepalive
 tg TG00 hsas-ip 10.12.165.2 10.12.165.1
```

The following example configures a TG name for an IP stack configured with CMPC+:

```
interface Channel0/2
 ip address 10.12.165.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip route-cache same-interface
 no ip mroute-cache
 no keepalive
 tg TG00 ip 10.12.165.2 10.12.165.1
```

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.

tg delay

To configure the duration of time the router is to wait before ending an Multi-Path Channel (MPC) block and sending it to the host, use the **tg delay** command in interface configuration mode. To restore the default duration of time, use the **no** form of this command.

tg *tg-name* **delay** *delay*

no tg *tg-name* **delay**

Syntax Description

tg-name	Name of the Cisco Multipath Channel (CMPC+) Transmission Group (TG). The maximum length of the name is eight characters. This name must match the name specified by the **cmpc** commands.
delay	Duration of delay in milliseconds. Allowed values are from 0 to 20. The default is 10 milliseconds.

Defaults

10 milliseconds

Command Modes

Interface configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

By default, the **tg delay** command does not appear in the running configuration. It is displayed in the configuration only when configured for a value that is not default.

Examples

The following example configures a TG delay of 20 milliseconds:

```
router(config)# interface channel 0/2
router(config-if)# tg TG00 delay 20
```

The following example resets the TG delay to the default of 10 milliseconds:

```
router(config-if)# no tg TG00 delay
```

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.

timing-mark

To select whether a WILL TIMING-MARK is sent when the host application needs a Systems Network Architecture (SNA) response (definite or pacing response), use the **timing-mark** command in TN3270 server configuration mode. To turn off WILL TIMING-MARK transmission except as used by the keepalive function, use the **no** form of this command.

timing-mark

no timing-mark

Syntax Description

This command has no arguments or keywords.

Defaults

No WILL TIMING-MARKS are sent except by keepalive.

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **timing-mark** command is configured, the TN3270 server will send WILL TIMING-MARK as necessary to achieve an end-to-end response protocol. Specifically, TIMING-MARK will be sent if either of the following conditions is true:

- The host application has requested a pacing response.
- The host application has requested a Definite Response, and either the client is not using TN3270E, or the request is not Begin Chain.

The use of the **timing-mark** command can degrade performance. Some clients do not support the **timing-mark** command used in this way. Therefore, the **timing-mark** command should be configured only when both of the following conditions are true:

- All clients support this usage.
- The application benefits from end-to-end acknowledgment.

Examples

The following example enables the sending of the TIMING-MARK:

```
timing-mark
```

Related Commands

Command	Description
idle-time	Specifies how many seconds of logical unit (LU) inactivity, from both host and client, before the TN3270 session is disconnected.
keepalive (TN3270)	Specifies how many seconds of inactivity elapse before transmission of a DO TIMING-MARK or Telnet no operation (nop) to the TN3270 client.

tn3270-server

To start the TN3270 server on a Cisco Mainframe Channel Connection (CMCC) adapter or to enter TN3270 server configuration mode, use the **tn3270-server** command in interface configuration mode. To remove the existing TN3270 server configuration, use the **no** form of this command.

tn3270-server

no tn3270-server

Syntax Description

This command has no arguments or keywords.

Defaults

No TN3270 server function is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **tn3270-server** command is valid only on the virtual channel interface. Only one TN3270 server can run on a CMCC adapter. It will always be configured on a virtual channel interface.

The **no tn3270-server** command shuts down TN3270 server immediately. All active sessions will be disconnected and all Dependent Logical Unit Requestor (DLUR) and physical unit (PU) definitions deleted from the router configuration. To restart a TN3270 server, you must reconfigure all parameters.

Examples

The following example starts the TN3270 server and enters TN3270 server configuration mode:

```
tn3270-server
```

unbind-action

To select what action to take when the TN3270 server receives an UNBIND request, use the **unbind-action** command in TN3270 server configuration mode. To restore the default, use the **no** form of this command.

unbind-action {**keep** | **disconnect**}

no unbind-action

Syntax Description

keep	No automatic disconnect will be made by the server on receipt of an UNBIND.
disconnect	Session will be disconnected upon receipt of an UNBIND.

Defaults

In TN3270 server configuration mode, the default is **disconnect**.
In physical unit (PU) configuration mode the default is the value configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **unbind-action** command is valid only on the virtual channel interface. The **unbind-action** command affects active and future TN3270 sessions.

In TN3270 server configuration mode, the **unbind-action** command applies to all PUs for that TN3270 server, except as overridden by values entered in PU configuration mode.

In listen-point configuration mode, the **unbind-action** command applies to all PUs defined at the listen point.

In DLUR PU configuration mode, the **unbind-action** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **unbind-action** command applies only to the specified PU. The **no unbind-action** command entered in PU configuration mode removes the override.

Examples

The following example prevents automatic disconnect:

```
unbind-action keep
```

vrn

To tell the Systems Network Architecture (SNA) session switch the connection network to which the internal adapter interface on the Cisco Mainframe Channel Connection (CMCC) adapter belongs, use the **vrn** Dependent Logical Unit Requestor (DLUR) service access point (SAP) configuration command. To remove a network name, use the **no** form of this command.

vrn *vrn-name*

no vrn

Syntax Description

vrn-name	Fully qualified name of the connection network.

Defaults

The adapter is not considered to be part of a connection network.

Command Modes

DLUR SAP configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **vrn** command is valid only on the virtual channel interface. This command is used to discover routes without having to configure all possible links.

A connection network is also known as a shared-access transport facility (SATF), which means, at the MAC level, that all nodes in the network can reach each other using the same addressing scheme and without requiring the services of SNA session routing. A bridged LAN (whether source-route or transparent) is an example. Such a network is represented in the Advanced Peer-to-Peer Networking (APPN) topology as a kind of node, termed a virtual routing node (VRN).

To make use of this function, all APPN nodes must use the same VRN name for the SATF.

Refer to the virtual telecommunications access method (VTAM) operating system documentation for your host system for additional information regarding the VTAM VNGROUP and VNNAME parameters on the PORT statement of an XCA major node.

Several parameters in the DLUR configuration mode consist of fully qualified names, as defined by the APPN architecture. Fully qualified names consist of two case-insensitive alphanumeric strings, separated by a period. However, for compatibility with existing APPN products, including VTAM, the characters “#” (pound), “@” (at), and “$” (dollar) are allowed in the fully qualified name strings. Each string is from one to eight characters long; for example, RA12.NODM1PP. The portion of the name before the period is the network entity title (NET) ID and is shared between entities in the same logical network.

Examples

The following example sets a VRN name:

```
vrn SYD.BLAN25
```

Related Commands

Command	Description
client pool	Nails clients to pools.
adapter	Configures internal adapters.
lan	Configures an internal LAN on a CMCC adapter interface and enters the internal LAN configuration mode.
lsap	Creates a service access point (SAP) in the SNA session switch and enters DLUR SAP configuration mode.

x25 map qllc

To specify the X.121 address of the remote X.25 device with which you plan to communicate using Qualified Logical Link Control (QLLC) conversion, use the **x25 map qllc** command in interface configuration mode. To disable QLLC conversion to this X.121 address, use the **no** form of this command.

x25 map qllc *virtual-mac-addr x121-addr* [**cud** *cud-value*] [*x25-map-options*]

no x25 map qllc *virtual-mac-addr x121-addr* [**cud** *cud-value*] [*x25-map-options*]

Syntax Description

virtual-mac-addr	Virtual MAC address.
x121-addr	X.121 address of the remote X.25 device you are associating with this virtual MAC address. It can be from 1 to 15 digits long.
cud cud-value	(Optional) Override of the standard Call User Data (CUD) value for outbound switched virtual circuits (SVCs). The value can range from 1 to 4 hex bytes.
x25-map-options	(Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in Table 100.

Defaults

No association is made.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The central notion that binds the QLLC conversion interface to the X.25 and source-route bridging (SRB) facilities is the X.25 address map. For each remote client an X.121 address is associated with a virtual MAC address. The rest of the configuration is specified by using the virtual Token Ring address to refer to the connection.

When a Token Ring device wants to open communications with another device, it will send the request to the address it knows, which is the MAC address. The Cisco IOS software accepts this connection request and must transform it into a known X.121 address. The **x25 map qllc** command matches the MAC address with the X.121 address.

You must enter a mapping for each X.25 device with which the router will exchange traffic.

All QLLC conversion commands use the *virtual-mac-addr* argument that you define with the **x25 map qllc** command to refer to the connection.

You use the **x25 map qllc** command in conjunction with the **qllc srb** command.

Table 100 shows the possible values for the *x25-map-options* argument.

Table 100 x.25 map qllc Options

Option	Description
compress	Specifies that X.25 payload compression be used for mapping the traffic to this host. Each virtual circuit established for compressed traffic uses a substantial amount of memory (for a table of learned data patterns) and for computation (for compression and decompression of all data). Cisco recommends that compression be used with careful consideration to its impact on overall performance.
method {**cisco** | **ietf** | **snap** | **multi**}	Specifies the encapsulation method. The choices are as follows: • **cisco**—Cisco's proprietary encapsulation; not available if more than one protocol is to be carried. • **ietf**—Default RFC 1356 operation: Protocol identification of single-protocol virtual circuits and protocol identification within multiprotocol virtual circuits uses the standard encoding, which is compatible with RFC 877. Multiprotocol virtual circuits are used only if needed. • **snap**—RFC 1356 operation where IP is identified with Subnetwork Access Protocol (SNAP) rather than the standard Internet Engineering Task Force (IETF) method (the standard method is compatible with RFC 877). • **multi**—Forces a map that specifies a single protocol to set up a multiprotocol virtual circuit when a call is originated; also forces a single-protocol permanent virtual circuit (PVC) to use multiprotocol data identification methods for all datagrams sent and received.
no-incoming	Use the map only to originate calls.
no-outgoing	Do not originate calls when using the map.
idle *minutes*	Specifies an idle timeout for calls other than the interface default; 0 minutes disables the idle timeout.
reverse	Specifies reverse charging for outgoing calls.
accept-reverse	Causes the Cisco IOS software to accept incoming reverse-charged calls. If this option is not present, the Cisco IOS software clears reverse-charged calls unless the interface accepts all reverse-charged calls.
broadcast	Causes the Cisco IOS software to direct any broadcasts sent through this interface to the specified X.121 address. This option also simplifies the configuration of OSPF; see the "Usage Guidelines" section for more detail.
cug *group-number*	Specifies a closed user group number (from 1 to 99) for the mapping in an outgoing call.
nvc *count*	Sets the maximum number of virtual circuits for this map or host. The default *count* is the **x25 nvc** setting of the interface. A maximum number of eight virtual circuits can be configured for each map. Compressed TCP may use only one virtual circuit.

Table 100 x.25 map qllc Options (continued)

Option	Description
packetsize *in-size out-size*	Proposes maximum input packet size (*in-size*) and maximum output packet size (*out-size*) for an outgoing call. Both values typically are the same and must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096.
windowsize *in-size out-size*	Proposes the packet count for input window (*in-size*) and output window (*out-size*) for an outgoing call. Both values typically are the same, must be in the range from 1 to 127, and must be lower than the value set by the **x25 modulo** command.
throughput *in out*	Sets the requested throughput class values for input (*in*) and output (*out*) throughput across the network for an outgoing call. Values for *in* and *out* are in bits per second (bps) and range from 75 to 48000 bps.
transit-delay *milliseconds*	Specifies the transit delay value in milliseconds (0 to 65534) for an outgoing call, for networks that support transit delay.
nuid *username password*	Specifies that a network user ID (NUID) facility be sent in the outgoing call with the specified Terminal Access Controller Access Control System (TACACS) username and password (in a format defined by Cisco). This option should be used only when connecting to another Cisco router. The combined length of the username and password must not exceed 127 characters.
nudata *string*	Specifies the network user identification in a format determined by the network administrator (as allowed by the standards). This option is provided for connecting to non-Cisco equipment that requires an NUID facility. The string must not exceed 130 characters and must be enclosed in quotation marks (“ ”) if any spaces are present.
roa *name*	Specifies the name defined by the **x25 roa** command for a list of transit Recognized Operating Agencies (ROAs) to use in outgoing Call Request packets.
passive	Specifies that the X.25 interface should send compressed outgoing TCP datagrams only if they were already compressed when they were received. This option is available only for compressed TCP maps.

Examples

In the following example, the **x25 map qllc** command is used to associate the remote X.25 device at X.121 address 31104150101 with the virtual MAC address 0100.000.0001:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
```

Related Commands

Command	Description
qllc accept-all-calls	Enables the router to accept a call from any remote X.25 device.
qllc srb	Enables Qualified Logical Link Control (QLLC) conversion on a serial interface configured for X.25 communication.

x25 pvc qllc

To associate a virtual MAC address with a permanent virtual circuit (PVC) for communication using Qualified Logical Link Control (QLLC) conversion, use the **x25 pvc qllc** command in interface configuration mode. To remove the association, use the **no** form of this command.

x25 pvc *circuit* **qllc** *x121-address* [*x25-map-options*]

no x25 pvc *circuit* **qllc** *x121-address* [*x25-map-options*]

Syntax Description

circuit	PVC you are associating with the virtual MAC address. This must be lower than any number assigned to switched virtual circuits.
x121-address	X.121 address.
x25-map-options	(Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in Table 100.

Defaults

No association is made.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a Token Ring device wants to communicate with another device, it will send the request to the address it knows, which is the MAC address. The Cisco IOS software accepts this connection request and transforms it into the known X.121 address and virtual circuit. You must use the **x25 map qllc** command to specify the required protocol-to-X.121 address mapping before you use the **x25 pvc qllc** command. The **x25 map qllc** command associates the MAC address with the X.121 address, and the **x25 pvc qllc** command further associates that address with a known PVC.

You use the **x25 pvc** command in conjunction with the **x25 map qllc** and **qllc srb** commands.

Examples

In the following example, the **x25 pvc qllc** command associates the virtual MAC address 0100.0000.0001, as defined in the previous **x25 map qllc** command entry, with PVC 3:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 x25 pvc 3 qllc 0100.0000.0001
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.

Appendix: Ethernet Type Codes

Table 101 lists known Ethernet type codes. You can use these type codes in transparent bridging and source-route bridging access lists for filtering frames by protocol type. For configuration information on filtering by protocol type, refer to the following two sections of the *Cisco IOS Bridging and IBM Networking Configuration Guide*:

- "Filtering Transparently Bridged Packets" in the "Configuring Transparent Bridging" chapter
- "Securing the SRB Network" in the "Configuring Source-Route Bridging" chapter

Table 101 Ethernet Type Codes

Hexadecimal	Description (Notes)
0000-05DC	IEEE 802.3 Length Field
0101-01FF	Experimental; for development (conflicts with 802.3 length fields)
0200	Xerox PARC Universal Protocol (PUP) (conflicts with IEEE 802.3 length fields)
0201	Xerox PUP Address Translation (conflicts with IEEE 802.3 length fields)
0400	Nixdorf Computers (Germany)
0600	Xerox XNS IDP
0660-0661	DLOG (Germany)
0800	DOD Internet Protocol (IP) *[1] #[2]
0801	X.75 Internet
0802	NBS Internet
0803	ECMA Internet
0804	CHAOSnet
0805	X.25 Level 3
0806	Address Resolution Protocol (for IP and CHAOS)
0807	XNS Compatibility
081C	Symbolics Private
0888-088A	Xyplex
0900	Ungermann-Bass (UB) Network Debugger
0A00	Xerox IEEE 802.3 PUP
0A01	Xerox IEEE 802.3 PUP Address Translation

Table 101 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
0BAD	Banyan VINES IP
0BAE	Banyan VINES Loopback
0BAF	Banyan VINES Echo
1000	Berkeley trailer negotiation
1001-100F	Berkeley trailer encapsulation for IP
1600	VALID system protocol
4242	PCS Basic Block Protocol
5208	BBN Simnet Private
6000	DEC unassigned
6001	DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
6002	DEC MOP Remote Console
6003	DEC DECnet Phase IV Route
6004	DEC Local Area Transport (LAT)
6005	DEC DECnet Diagnostics
6006	DEC Customer Protocol
6007	DEC Local-Area VAX Cluster (LAVC), SCA
6008	DEC unassigned
6009	DEC unassigned
6010-6014	3Com Corporation
7000	Ungermann-Bass (UB) Download
7001	UB diagnostic/loopback
7002	UB diagnostic/loopback
7020-7029	LRT (England)
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe protocol
8006	Nestar
8008	AT&T
8010	Excelan
8013	Silicon Graphics diagnostic (obsolete)
8014	Silicon Graphics network games (obsolete)
8015	Silicon Graphics reserved type (obsolete)
8016	Silicon Graphics XNS NameServer, bounce server (obsolete)

Table 101 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
8019	Apollo Computers
802E	Tymshare
802F	Tigan, Inc.
8035	Reverse Address Resolution Protocol (RARP) (Stanford)
8036	Aeonic Systems
8038	DEC LANBridge Management
8039-803C	DEC unassigned
803D	DEC Ethernet CSMA/CD Encryption Protocol
803E	DEC unassigned
803F	DEC LAN Traffic Monitor Protocol
8040-8042	DEC unassigned
8044	Planning Research Corporation
8046-8047	AT&T
8049	ExperData (France)
805B	*Versatile Message Translation Protocol*, RFC 1045 (Stanford)
805C	Stanford V Kernel, production
805D	Evans & Sutherland
8060	Little Machines
8062	Counterpoint Computers
8065-8066	University of Massachusetts at Amherst
8067	Veeco Integrated Automation
8068	General Dynamics
8069	AT&T
806A	Autophon (Switzerland)
806C	ComDesign
806D	Compugraphic Corporation
806E-8077	Landmark Graphics Corporation
807A	Matra (France)
807B	Dansk Data Elektronik A/S
807C	University of Michigan
807D-807F	Vitalink Communications
8080	Vitalink TransLAN III Management
8081-8083	Counterpoint Computers
809B	Kinetics EtherTalk (AppleTalk over Ethernet)
809C-809E	Datability
809F	Spider Systems, Ltd.

Table 101 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
80A3	Nixdorf Computers (Germany)
80A4-80B3	Siemens Gammasonics, Inc.
80C0-80C3	Digital Communications Association (DCA), Inc.
80C1	DCA Data Exchange Cluster
80C4	Banyan VINES IP
80C5	Banyan VINES Echo
80C6	Pacer Software
80C7	Applitek Corporation
80C8-80CC	Intergraph Corporation
80CD-80CE	Harris Corporation
80CF-80D2	Taylor Instrument
80D3-80D4	Rosemount Corporation
80D5	IBM SNA Services over Ethernet
80DD	Varian Associates
80DE	Integrated Solutions Transparent Remote File System (TRFS)
80DF	Integrated Solutions
80E0-80E3	Allen-Bradley
80E4-80F0	Datability
80F2	Retix
80F3	Kinetics AppleTalk Address Resolution Protocol (AARP)
80F4-80F5	Kinetics
80F7	Apollo Computer
80FF-8103	Wellfleet Communications
8107-8109	Symbolics Private
8130	Hayes Microcomputer Products, Ltd. (formerly Waterloo Microsystems, Inc.)
8131	VG Laboratory Systems
8132-8136	Bridge Communications, Inc.
8137	Novell NetWare IPX (old)
8137-8138	Novell, Inc.
8139-813D	KTI
8148	Logicraft, Inc.
8149	Network Computing Devices
814A	Alpha Micro
814C	SNMP
814D-814E	BIIN
814F	Technically Elite Concepts, Inc.

Table 101 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
8150	Rational Corporation
8151-8153	Qualcomm, Inc.
815C-815E	Computer Protocol Pty, Ltd.
8164-8166	Charles River Data Systems, Inc.
817D-818C	Protocol Engines, Inc.
818D	Motorola Computer X
819A-81A3	Qualcomm, Inc.
81A4	ARAI Bunkichi
81A5-81AE	RAD Network Devices
81B7-81B9	Xyplex
81CC-81D5	Apricot Computers
81D6-81DD	Artisoft, Inc.
81DE-81E0	Hewlett Packard
81E6-81EF	Polygon, Inc.
81F0-81F2	Comsat Laboratories
81F3-81F5	Science Applications International Corporation (SAIC)
81F6-81F8	VG Analytical, Ltd.
8203-8205	Quantum Software Systems, Ltd.
8221-8222	Ascom Banking Systems, Ltd.
823E-8240	Advanced Encryption Systems, Inc.
827F-8282	Athena Programming, Inc.
8263-826A	Charles River Data Systems
829A-829B	Institute for Industrial Information Technology, Ltd.
829C-82AB	Taurus Controls, Inc.
82AC-838F	Walker Richer & Quinn, Inc.
8390	LANSoft, Inc.
8391-8693	Walker Richer & Quinn, Inc.
8694-869D	Idea Courier
869E-86A1	Computer Network Technology Corporation
86A3-86AC	Gateway Communications, Inc.
86DB	SECTRA - Secure Transmission AB
86DE	Delta Controls, Inc.
86DF	USC-ISI
86E0-86EF	Landis & Gyr Powers, Inc.
8700-8710	Motorola, Inc.
8711-8720	Cray Communications

Table 101 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
8725-8728	Phoenix Microsystems
8739-873C	Control Technology, Inc.
8755-8759	LANSoft, Inc.
875A-875C	Norland
875D-8766	University of Utah Dept./Computer Science
8780-8785	Symbol Technologies, Inc.
8A96-8A97	Invisible Software
9000	Loopback (Configuration Test Protocol)
9001	3Com (Bridge) XNS Systems Management
9002	3Com (Bridge) TCP/IP Systems Management
9003	3Com (Bridge) loop detect
FF00	BBN VITAL LANBridge cache wakeups
FF00-FF0F	ISC-Bunker Ramo

1. An asterisk (*) indicates the current connection in various informational displays.
2. A pound sign (#) is a delimiting character for configuration commands that contain arbitrary text strings.