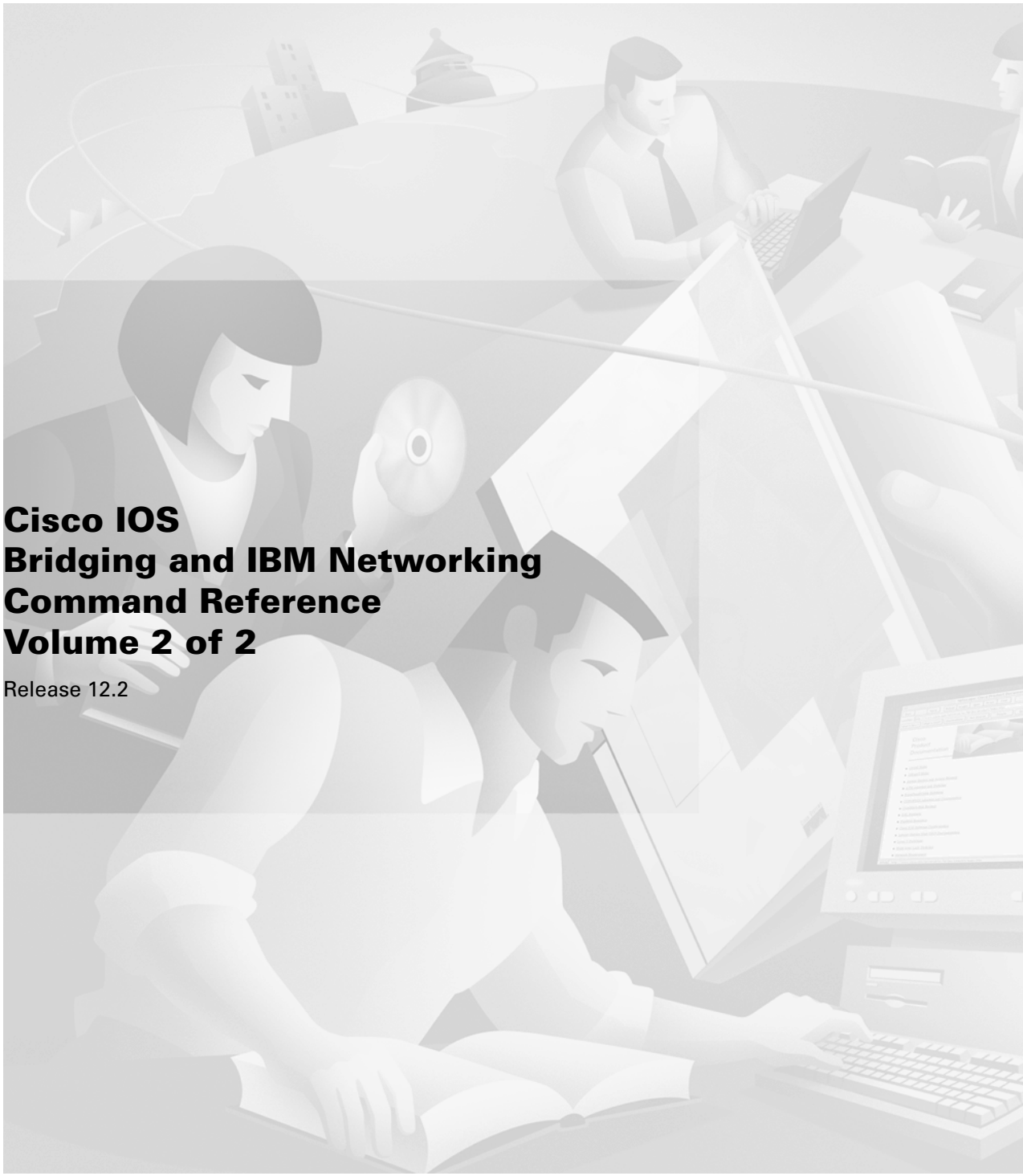


Cisco IOS Bridging and IBM Networking Command Reference Volume 2 of 2

Release 12.2

Corporate 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: 408 526-4100

Customer Order Number: DOC-7811736=
Text Part Number: 78-11736-02

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.

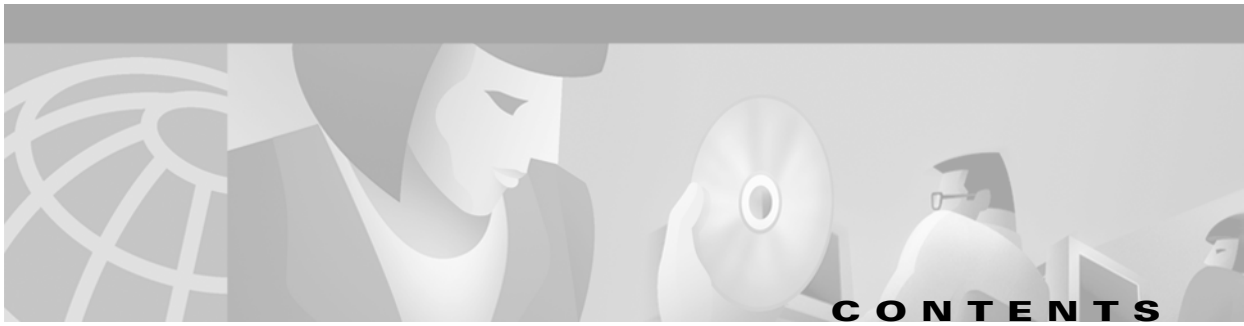
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Net*Works* logo, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or 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. (0102R)

Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2
Copyright © 2001–2006 Cisco Systems, Inc.
All rights reserved.



CONTENTS

About Cisco IOS Software Documentation v

Using Cisco IOS Software xiii

IBM Networking

DSPU and SNA Service Point Commands B2R-3

SNA Switching Services Commands B2R-77

Cisco Transaction Connection Commands B2R-153

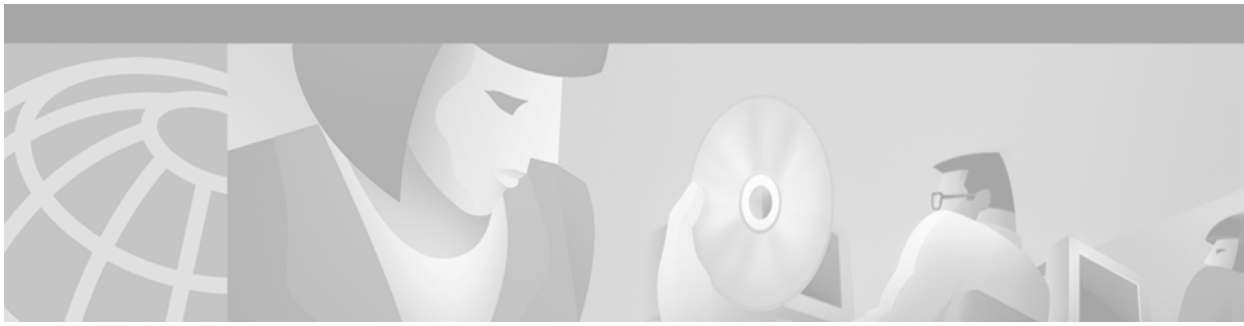
Cisco Mainframe Channel Connection Commands B2R-205

CLAW and TCP/IP Offload Commands B2R-265

CMPC, CMPC+ and CSNA Commands B2R-287

TN3270 Server Commands B2R-315

Index



About Cisco IOS Software Documentation

This chapter discusses the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation from Cisco Systems.

Documentation Objectives

Cisco IOS software documentation describes the tasks and commands necessary to configure and maintain Cisco networking devices.

Audience

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

Documentation Organization

The Cisco IOS software documentation set consists of documentation modules and master indexes. In addition to the main documentation set, there are supporting documents and resources.

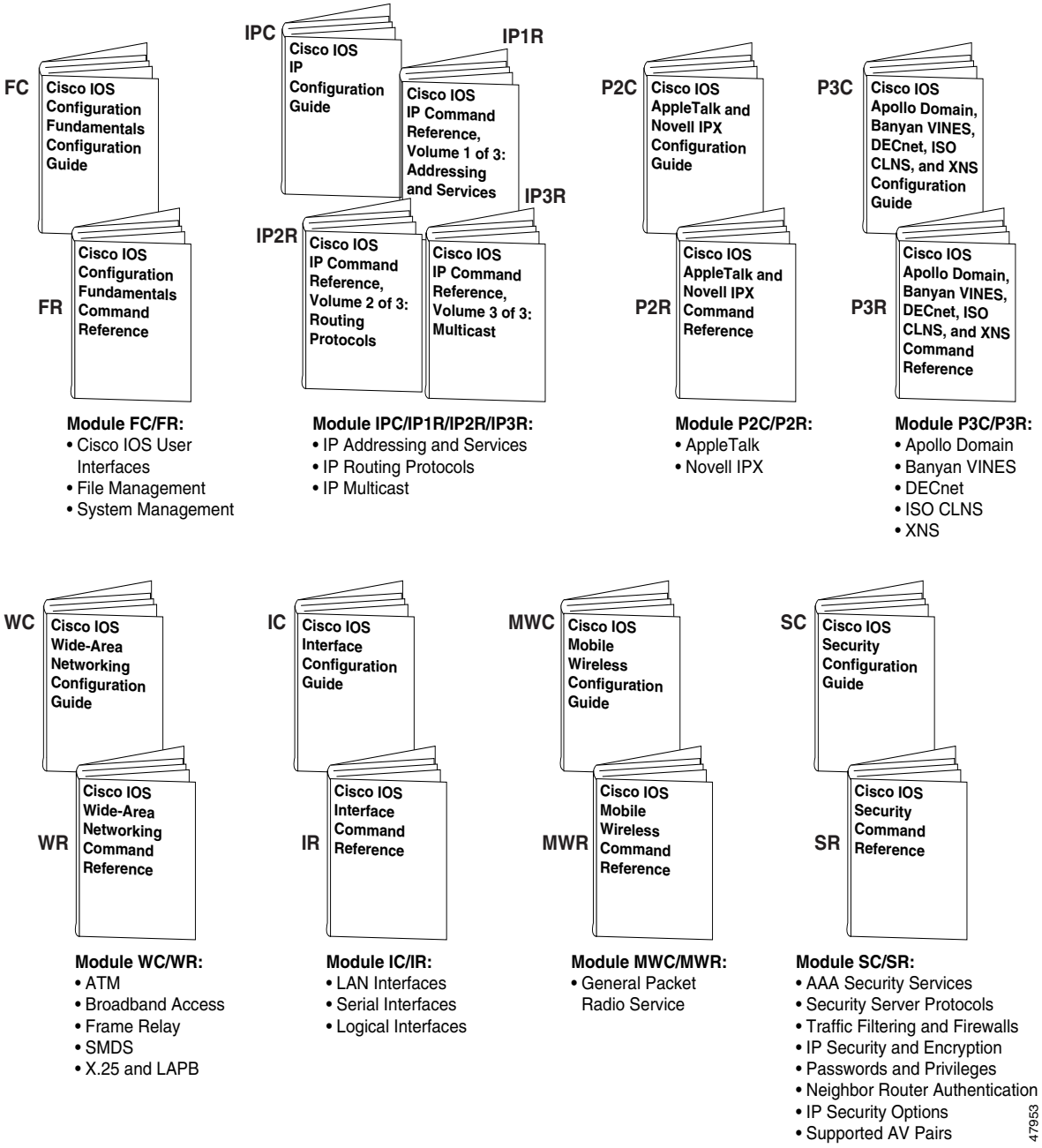
Documentation Modules

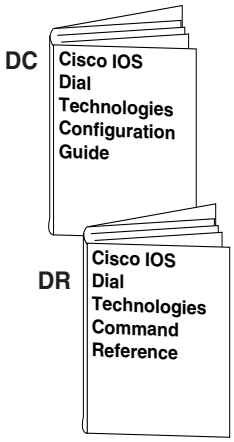
The Cisco IOS documentation modules consist of configuration guides and corresponding command reference publications. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality and contain comprehensive configuration examples. Chapters in a command reference publication provide complete Cisco IOS command syntax information. Use each configuration guide in conjunction with its corresponding command reference publication.

Figure 1Figure 1 shows the Cisco IOS software documentation modules.

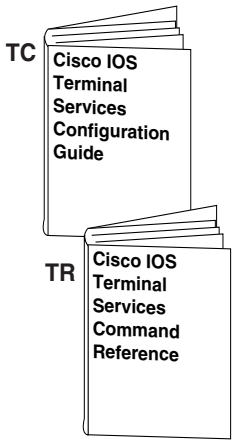
Note The abbreviations (for example, FC and FR) next to the book icons are page designators, which are defined in a key in the index of each document to help you with navigation. The bullets under each module list the major technology areas discussed in the corresponding books.

Figure 1 Cisco IOS Software Documentation Modules

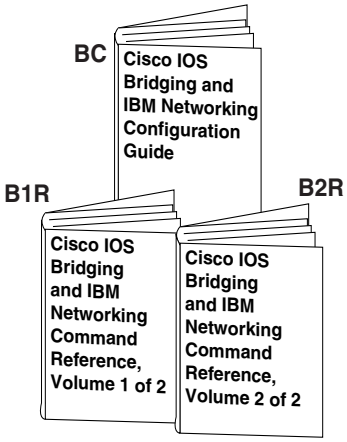




Module DC/DR:
- Preparing for Dial Access
- Modem and Dial Shelf Configuration and Management
- ISDN Configuration
- Signalling Configuration
- Dial-on-Demand Routing Configuration
- Dial-Backup Configuration
- Dial-Related Addressing Services
- Virtual Templates, Profiles, and Networks
- PPP Configuration
- Callback and Bandwidth Allocation Configuration
- Dial Access Specialized Features
- Dial Access Scenarios

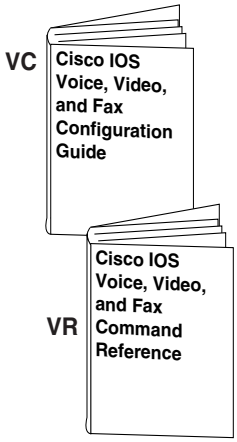


Module TC/TR:
- ARA
- LAT
- NASI
- Telnet
- TN3270
- XRemote
- X.28 PAD
- Protocol Translation

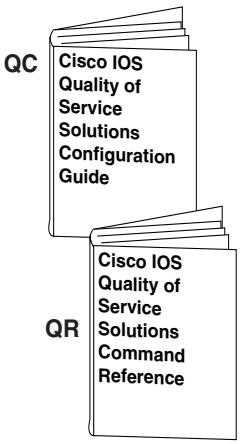


Module BC/B1R:
- Transparent Bridging
- SRB
- Token Ring Inter-Switch Link
- Token Ring Route Switch Module
- RSRB
- DLSw+
- Serial Tunnel and Block Serial Tunnel
- LLC2 and SDLC
- IBM Network Media Translation
- SNA Frame Relay Access
- NCIA Client/Server
- Airline Product Set

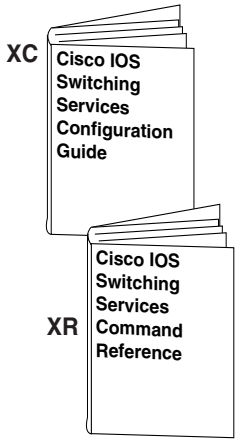
Module BC/B2R:
- DSPU and SNA Service Point
- SNA Switching Services
- Cisco Transaction Connection
- Cisco Mainframe Channel Connection
- CLAW and TCP/IP Offload
- CSNA, CMPC, and CMPC+
- TN3270 Server



Module VC/VR:
- Voice over IP
- Call Control Signalling
- Voice over Frame Relay
- Voice over ATM
- Telephony Applications
- Trunk Management
- Fax, Video, and Modem Support



Module QC/QR:
- Packet Classification
- Congestion Management
- Congestion Avoidance
- Policing and Shaping
- Signalling
- Link Efficiency Mechanisms



Module XC/XR:
- Cisco IOS Switching Paths
- NetFlow Switching
- Multiprotocol Label Switching
- Multilayer Switching
- Multicast Distributed Switching
- Virtual LANs
- LAN Emulation

47954

Master Indexes

Two master indexes provide indexing information for the Cisco IOS software documentation set: an index for the configuration guides and an index for the command references. Individual books also contain a book-specific index.

The master indexes provide a quick way for you to find a command when you know the command name but not which module contains the command. When you use the online master indexes, you can click the page number for an index entry and go to that page in the online document.

Supporting Documents and Resources

The following documents and resources support the Cisco IOS software documentation set:

- *Cisco IOS Command Summary* (two volumes)—This publication explains the function and syntax of the Cisco IOS software commands. For more information about defaults and usage guidelines, refer to the Cisco IOS command reference publications.
- *Cisco IOS System Error Messages*—This publication lists and describes Cisco IOS system error messages. Not all system error messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
- *Cisco IOS Debug Command Reference*—This publication contains an alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, usage guidelines, and sample output.
- *Dictionary of Internetworking Terms and Acronyms*—This Cisco publication compiles and defines the terms and acronyms used in the internetworking industry.
- New feature documentation—The Cisco IOS software documentation set documents the mainline release of Cisco IOS software (for example, Cisco IOS Release 12.2). New software features are introduced in early deployment releases (for example, the Cisco IOS "T" release train for 12.2, 12.2(x)T). Documentation for these new features can be found in standalone documents called "feature modules." Feature module documentation describes new Cisco IOS software and hardware networking functionality and is available on Cisco.com and the Documentation CD-ROM.
- Release notes—This documentation describes system requirements, provides information about new and changed features, and includes other useful information about specific software releases. See the section "Using Software Release Notes" in the chapter "Using Cisco IOS Software" for more information.
- Caveats documentation—This documentation provides information about Cisco IOS software defects in specific software releases.
- RFCs—RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained on the World Wide Web at http://www.rfc-editor.org/.
- MIBs—MIBs are used for network monitoring. For lists of supported MIBs by platform and release, and to download MIB files, see the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means 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 an SNMP community string to public, do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
boldface	Boldface text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.

Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y | z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
`screen`	Examples of information displayed on the screen are set in Courier font.
`boldface screen`	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:

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

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

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

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at the following website:

http://www.cisco.com

Translated documentation is available at the following website:

http://www.cisco.com/public/countries_languages.html

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation can be ordered in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

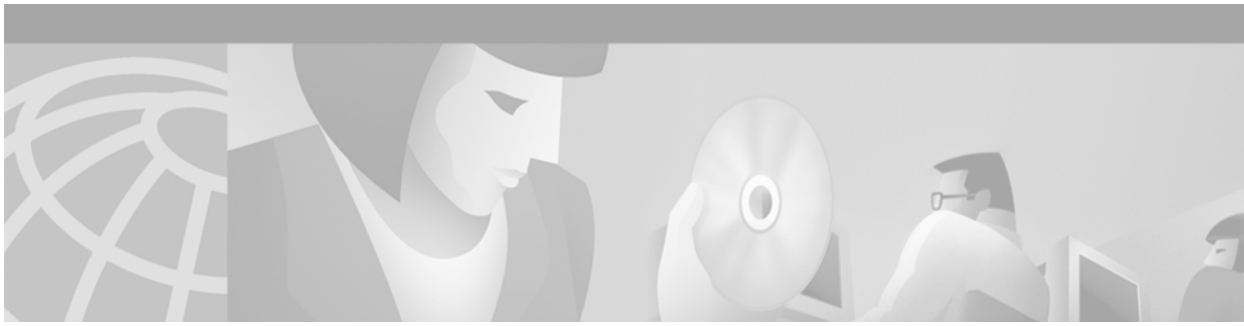
Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



Using Cisco IOS Software

This chapter provides helpful tips for understanding and configuring Cisco IOS software using the command-line interface (CLI). It contains the following sections:

- Understanding Command Modes, page xiii
- Getting Help, page xiv
- Using the no and default Forms of Commands, page xvii
- Saving Configuration Changes, page xviii
- Filtering Output from the show and more Commands, page xviii
- Identifying Supported Platforms, page xix

For an overview of Cisco IOS software configuration, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information on the conventions used in the Cisco IOS software documentation set, see the chapter "About Cisco IOS Software Documentation" located at the beginning of this book.

Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode you are currently in. Entering a question mark (**?**) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to the CLI, you are in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode, normally by using a password. From privileged EXEC mode you can issue any EXEC command—user or privileged mode—or you can enter global configuration mode. Most EXEC commands are one-time commands. For example, **show** commands show important status information, and **clear** commands clear counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS 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.

Table 1 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

Table 1 Accessing and Exiting Command Modes

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	`Router>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** EXEC command.	`Router#`	To return to user EXEC mode, use the **disable** command.
Global configuration	From privileged EXEC mode, use the **configure terminal** privileged EXEC command.	`Router(config)#`	To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command, or press **Ctrl-Z**.
Interface configuration	From global configuration mode, specify an interface using an **interface** command.	`Router(config-if)#`	To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command, or press **Ctrl-Z**.
ROM monitor	From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting.	`>`	To exit ROM monitor mode, use the **continue** command.

For more information on command modes, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Getting Help

Entering a question mark (**?**) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
help	Provides a brief description of the help system in any command mode.
*abbreviated-command-entry***?**	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
abbreviated-command-entry<**Tab**>	Completes a partial command name.
?	Lists all commands available for a particular command mode.
command **?**	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for "carriage return." On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

Table 2 shows examples of how you can use the question mark (**?**) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface on a Cisco 7206 router that is running Cisco IOS Release 12.0(3).

Table 2 How to Find Command Options

Command	Comment

`Router> enable`
`Password: <password>`
`Router#`
	Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to `Router#`.

`Router# configure terminal`
`Enter configuration commands, one per line. End with CNTL/Z.`
`Router(config)#`
	Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router(config)#`.

`Router(config)# interface serial ?`
`  <0-6>  Serial interface number`
`Router(config)# interface serial 4 ?`
`  /`
`Router(config)# interface serial 4/ ?`
`  <0-3>  Serial interface number`
`Router(config)# interface serial 4/0`
`Router(config-if)#`
	Enter interface configuration mode by specifying the serial interface that you want to configure using the **interface serial** global configuration command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.
	You are in interface configuration mode when the prompt changes to `Router(config-if)#`.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ?`
`Interface configuration commands:`
`  .`
`  .`
`  .`
`  ip  Interface Internet Protocol config commands`
`  keepalive  Enable keepalive`
`  lan-name  LAN Name command`
`  llc2  LLC2 Interface Subcommands`
`  load-interval  Specify interval for load calculation for an interface`
`  locaddr-priority  Assign a priority group`
`  logging  Configure logging for interface`
`  loopback  Configure internal loopback on an interface`
`  mac-address  Manually set interface MAC address`
`  mls  mls router sub/interface commands`
`  mpoa  MPOA interface configuration commands`
`  mtu  Set the interface Maximum Transmission Unit (MTU)`
`  netbios  Use a defined NETBIOS access list or enable name-caching`
`  no  Negate a command or set its defaults`
`  nrzi-encoding  Enable use of NRZI encoding`
`  ntp  Configure NTP`
`  .`
`  .`
`  .`
`Router(config-if)#`
	Enter **?** to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.

`Router(config-if)# ip ?`
`Interface IP configuration subcommands:`
`  access-group  Specify access control for packets`
`  accounting  Enable IP accounting on this interface`
`  address  Set the IP address of an interface`
`  authentication  authentication subcommands`
`  bandwidth-percent  Set EIGRP bandwidth limit`
`  broadcast-address  Set the broadcast address of an interface`
`  cgmp  Enable/disable CGMP`
`  directed-broadcast  Enable forwarding of directed broadcasts`
`  dvmrp  DVMRP interface commands`
`  hello-interval  Configures IP-EIGRP hello interval`
`  helper-address  Specify a destination address for UDP broadcasts`
`  hold-time  Configures IP-EIGRP hold time`
`  .`
`  .`
`  .`
`Router(config-if)# ip`
	Enter the command that you want to configure for the interface. This example uses the **ip** command.
	Enter **?** to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.

Table 2 How to Find Command Options (continued)

Command	Comment

`Router(config-if)# ip address ?`
`  A.B.C.D  IP address`
`  negotiated  IP Address negotiated over PPP`
`Router(config-if)# ip address`
	Enter the command that you want to configure for the interface. This example uses the **ip address** command.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP address or the **negotiated** keyword.
	A carriage return (<cr>) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

`Router(config-if)# ip address 172.16.0.1 ?`
`  A.B.C.D  IP subnet mask`
`Router(config-if)# ip address 172.16.0.1`
	Enter the keyword or argument you want to use. This example uses the 172.16.0.1 IP address.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.
	A <cr> is not displayed; therefore, you must enter additional keywords or arguments to complete the command.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?`
`  secondary  Make this IP address a secondary address`
`  <cr>`
`Router(config-if)# ip address 172.16.0.1 255.255.255.0`
	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.
	Enter **?** to display what you must enter next on the command line. In this example, you can enter the **secondary** keyword, or you can press **Enter**.
	A <cr> is displayed; you can press **Enter** to complete the command, or you can enter another keyword.

`Router(config-if)# ip address 172.16.0.1 255.255.255.0` `Router(config-if)#`	In this example, Enter is pressed to complete the command.

Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands also can have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and

have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

Saving Configuration Changes

Use the **copy system:running-config nvram:startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A Flash file system platforms, this task saves the configuration to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Filtering Output from the show and more Commands

In Cisco IOS Release 12.0(1)T and later releases, you can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

command **|** {**begin | include | exclude**} *regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression "protocol" appears:

```
Router# show interface | include protocol

Fast Ethernet0/0 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
```

For more information on the search and filter functionality, refer to the "Using the Command-Line Interface" chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Identifying Supported Platforms

Cisco IOS software is packaged in feature sets consisting of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. To identify the set of software images available in a specific release or to find out if a feature is available in a given Cisco IOS software image, see the following sections:

- Using Feature Navigator, page xix
- Using Software Release Notes, page xix

Using Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

http://www.cisco.com/go/fn

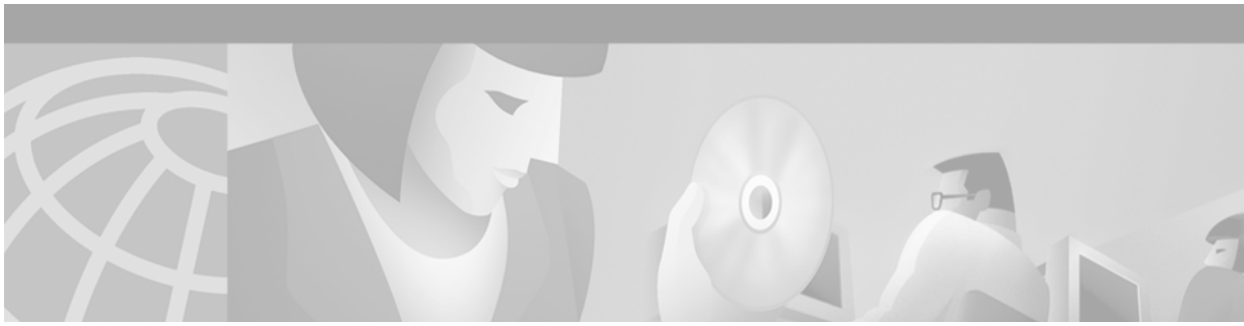
Using Software Release Notes

Cisco IOS software releases include release notes that provide the following information:

- Platform support information
- Memory recommendations
- Microcode support information
- Feature set tables
- Feature descriptions
- Open and resolved severity 1 and 2 caveats for all platforms

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases.

IBM Networking



DSPU and SNA Service Point Commands

This chapter describes the commands you use to configure the downstream physical unit (DSPU) feature, which provides a gateway facility for downstream Systems Network Architecture (SNA) physical units (PUs), and SNA Service Point support. For DSPU and SNA Service Point configuration tasks and examples, refer to the "Configuring DSPU and SNA Service Point Support" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

dspu activation-window

To define the number of activation request units (RUs) and response messages (such as ACTLUs or DDDLU NMVTs) that can be sent without waiting for responses from the remote PU, use the **dspu activation-window** global configuration command. 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 5.

Defaults

The default window size is 5 outstanding unacknowledged activation RUs.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

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 DSPU activation window allows more LUs 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/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 PU attempts to connect, but does not match any of the explicit PU definitions, use the **dspu default-pu** global configuration command. 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 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 64 bytes to 18,432 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.

Usage Guidelines

If the 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 SNA transmission header (TH), request header (RH), and request unit (RU), but does not include the DLC header. The DSPU feature segments 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 smaller of the two values is used.

Examples

In the following example, the default PU feature is enabled with a window size of 5 and a maximum I-frame size of 128. Each default PU can have up to 3 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 SAP on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts, use the **dspu enable-host** interface configuration command. 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.

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, RSRB, or VDLC connections.

dspu enable-host (QLLC)

To enable an X.121 subaddress for use by upstream host connections via QLLC, use the **dspu enable-host** interface configuration command. 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	Required keyword for 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.

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 SDLC address for use by upstream host connections, use the **dspu enable-host** interface configuration command. 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	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.

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 downstream PU connections, use the **dspu enable-pu** interface configuration command. 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 SAP address used by the 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.

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, RSRB, VDLC, or NCIA connections.

dspu enable-pu (QLLC)

To enable an X.121 subaddress for use by downstream PU connections via QLLC, use the **dspu enable-pu** interface configuration command. 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 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.

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 SDLC address for use by downstream PU connections, use the **dspu enable-pu** interface configuration command. 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.

Examples

The following example enables a 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 (Frame Relay)

To define a DSPU host over a Frame Relay connection, use the **dspu host** global configuration command. 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*	XID that will be sent to the host during connection establishment. The XID value is 8 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 1 to 127.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 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 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 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.

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 smaller of the two values is used.

Alerts from downstream PUs will be forwarded to the focalpoint 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 DSPU host over an X.25/QLLC connection, use the **dspu host** global configuration command. 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*	XID that will be sent to the host during connection establishment. The XID value is 8 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 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 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 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 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.

Usage Guidelines

The X.121 subaddress must be enabled by a **dspu enable-host (QLLC)** command.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the smaller of the two values is used.

Alerts from downstream PUs will be forwarded to the focalpoint 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 DSPU host over an SDLC connection, use the **dspu host** global configuration command. 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*	XID that will be sent to the host during connection establishment. The XID value is 8 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 1 to 127. The default window size is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is 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 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 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.

Usage Guidelines

The SDLC address must be enabled by a **dspu enable-host (SDLC)** command.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the smaller of the two values is used.

Alerts from downstream PUs will be forwarded to the focalpoint 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 host (Token Ring, Ethernet, FDDI, RSRB, VDLC)

To define a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections, use the **dspu host** global configuration command. 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*	XID that will be sent to the host during connection establishment. The XID value is 8 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 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.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is 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 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 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 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.

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 smaller of the two values is used.

Alerts from downstream PUs will be forwarded to the focalpoint 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 LUs 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 lu

To define a dedicated LU or a range of LUs for an upstream host and a downstream PU, use the **dspu lu** global configuration command. 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*. The range of host LUs starts with the address *host-lu-start*.
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.

Usage Guidelines

The **dspu lu** command is applied to that PU, and the **pu** keyword and *pu-name* argument are not required if the **dspu lu** command immediately follows one of these commands: **dspu default-pu** or **dspu pu**.

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 parameters 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 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 NCIA server as the underlying transport, use the **dspu ncia** global configuration command. 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.

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 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 SAP on the NCIA server for use by downstream connections, use the **dspu ncia enable-pu** global configuration command. 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.

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 DSPU notifications to send to SNMP and SNA network management, use the **dspu notification-level** global configuration command. 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 DSPU.
low	Sends PU and 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.

Usage Guidelines

This command applies to both SNMP traps and unsolicited SNA messages to operator. The upstream PU and LU notification events and the LU state change notification events are not sent as unsolicited SNA messages to operator. These events are sent as SNMP traps only.

Examples

The following example sets the notification level to enable 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 LUs in an LU pool, use the **dspu pool** global configuration command. 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 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.

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 PU, or it can include LUs from different host PUs. The LUs from host *host-name* starting at *lu-start* and ending with *lu-end*, 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, RSRB, or VDLC connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu pu (Frame Relay)

To define a DSPU host over a Frame Relay connection, use the **dspu pu** global configuration command. 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 PU.
dlci *dlci-number*	Frame Relay data-link connection identifier (DLCI) number. This number is a decimal.
rsap *remote-sap*	(Optional) 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 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 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum I-frame that can be sent or received across the link. The range is 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 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 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.

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 PU over an X.25 connection, use the **dspu pu** global configuration command. 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 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 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum I-frame that can be sent or received across the link. The range is 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 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 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.

Examples

The following example defines a downstream PU:

```
dspu pu testpu xid-rcv 05d00001 x25 32012 qllc 12
```

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 DSPU host over an SDLC connection, use the **dspu pu** global configuration command. 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 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 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum I-frame that can be sent or received across the link. The range is 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 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 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.

Examples

The following example defines a downstream PU:

```
dspu pu testpu sdlc c1 interface serial 0
```

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 pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)

To define an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, virtual data-link control, or NCIA connections, use the **dspu pu** global configuration command. 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) 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 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 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum I-frame that can be sent or received across the link. The range is 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 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 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.

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 SNA TH and 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 smaller 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 **rmac**, **rsap**, **xid-rcv** 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/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 smaller of the two values is used.

For Cisco IOS Release 11.3 and later, 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 only be accepted if the remote MAC/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 xid-rcv 05d00001 rmac 1000.5AED.1F53 rsap 20
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 VDLC downstream connections.

dspu rsrb

To define the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the DSPU feature will simulate at the RSRB, use the **dspu rsrb** global configuration command. 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 1 to 15.
target-virtual-ring	RSRB target virtual ring number. The RSRB target virtual ring corresponds to the ring-number parameter 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.

Usage Guidelines

The bridge number parameter 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** parameter 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 150.10.13.1
source-bridge remote-peer 99 tcp 150.10.13.2
```

```
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 150.10.13.1 255.255.255.0
```

The following example defines 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 150.10.13.1
source-bridge remote-peer 99 tcp 150.10.13.2 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 150.10.13.1 255.255.255.0
```

The following example defines 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 150.10.13.1
source-bridge remote-peer 99 tcp 150.10.13.2

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 150.10.13.1 255.255.255.0
```

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 RSRB SAP for use by DSPU host connections, use the **dspu rsrb enable-host** global configuration command. 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.

Examples

In the following example, the local SAP address 10 of the RSRB is enabled for use by the ibm3745 host PU:

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 150.10.13.1
source-bridge remote-peer 99 tcp 150.10.13.2

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 150.10.13.1 255.255.255.0
```

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 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 RSRB SAP for use by DSPU downstream connections, use the **dspu rsrb enable-pu** global configuration command. 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.

Defaults

The default local SAP is 8.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

In the following example, the local SAP address 20 of the RSRB is enabled for use by the ciscopu DSPU downstream PU:

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 150.10.13.1
source-bridge remote-peer 99 tcp 150.10.13.2

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 PU name through the RSRB, use the **dspu rsrb start** global configuration command. 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, 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.

Usage Guidelines

Before issuing this command, you must enable the correct local 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 only valid if the target MAC address has been defined in the resource. For a host resource, this 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 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 150.10.13.1
source-bridge remote-peer 99 tcp 150.10.13.2

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 150.10.13.1 255.255.255.0
```

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 PU name, use the **dspu start** interface configuration command. 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.

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 only valid if the target address (RMAC SDLC, 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 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 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 DSPU host and downstream connections over DLSw+ using virtual data-link control, use the **dspu vdlc** global configuration command. 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.

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 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 150.10.16.2
dlsw remote-peer 0 tcp 150.10.16.1

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 150.10.16.2 255.255.255.0
 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 SAP for use by DSPU host connections, use the **dspu vdlc enable-host** global configuration command. 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.

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 150.10.16.2
dlsw remote-peer 0 tcp 150.10.16.1

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 150.10.16.2 255.255.255.0
 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 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 SAP for use by DSPU virtual data-link control downstream connections, use the **dspu vdlc enable-pu** global configuration command. 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.

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 150.10.16.2
dlsw remote-peer 0 tcp 150.10.16.1

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 150.10.16.2 255.255.255.0
 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 PU name through virtual data-link control, use the **dspu vdlc start** global configuration command. 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.

Usage Guidelines

Before issuing this command, you must enable the correct local 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 only valid 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, DSPU attempts to initiate connections with host PU HOST-B, host PU HOST3k-A, and downstream PU PU3k-A over DLSw+ using virtual data-link control:

```
source-bridge ring-group 99
dlsw local-peer peer-id 150.10.16.2
dlsw remote-peer 0 tcp 150.10.16.1

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 150.10.16.2 255.255.255.0
 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.

lan-name

To specify a name for the LAN that is attached to the interface, use the **lan-name** interface configuration command. This name is included in any Alert sent to the 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.

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.

show dspu

To display the status of the DSPU feature, use the **show dspu** privileged EXEC command.

show dspu [**pool** *pool-name* | [**pu** {*host-name* | *pu-name*} [**all**]]

Syntax Description

pool *pool-name*	(Optional) Name of a pool of LUs (as defined by the **dspu pool** command).
pu	(Optional) Name of defined 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.

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 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 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 sna

To display the status of the SNA Service Point feature, use the **show sna** privileged EXEC command.

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.

Examples

The following is sample output from the **show sna** command. It shows a summary of the 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 LUs under the PU, this has no significance for the Service Point host.

sna enable-host (QLLC)

To enable an X.121 subaddress for use by the SNA Service Point feature on the interface, use the **sna enable-host** interface configuration command. 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 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.

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 an SDLC address for use by host connections, use the **sna enable-host** interface configuration command. 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.

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 an SNA host over an SDLC connection.

sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI)

To enable SNA on the interface, use the **sna enable-host** interface configuration command. 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 SAP as an upstream SAP, for both receiving ConnectIn attempts and for starting ConnectOut attempts.
lsap-address	(Optional) Local SAP. 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.

Examples

The following example enables SNA on the interface and specifies that the local SAP 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, RSRB, or VDLC connections.

sna host (Frame Relay)

To define a link to an SNA host over a Frame Relay connection, use this form of the **sna host** global configuration command. 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*	XID that will be sent to the host during connection establishment. The XID value is 8 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*	DLCI number.
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 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 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 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with remote host PU. The range is 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 remote host PU. The range is 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.

Examples The following example defines a link to an 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 an SNA host over an X.25/QLLC connection, use this form of the **sna host** global configuration command. 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*	XID that will be sent to the host during connection establishment. The XID value is 8 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*	SDLC address.
qllc *local-x121-subaddr*	(Optional) Specifies the SAP address of the remote host 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 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 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with remote host PU. The range is 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 remote host PU. The range is 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.

Examples

The following example defines a link to an 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 an SNA host over an SDLC connection, use this form of the **sna host** global configuration command. 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*	XID that will be sent to the host during connection establishment. The XID value is 8 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) SAP address of the remote host PU. The default is 4.
lsap *local-sap*	(Optional) Local SAP 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 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 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with remote host PU. The range is 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 remote host PU. The range is 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.

Examples

The following example defines a link to an 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 SDLC address for use by host connections.
sna start	Initiates a connection to a remote resource.

sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)

To define a link to an SNA host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control connections, use the **sna host** global configuration command. 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** s*lot/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*	XID that will be sent to the host during connection establishment. The XID value is 8 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 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 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 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 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with remote host PU. The range is 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 remote host PU. The range is 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.

Examples The following example defines a link to an 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 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 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 host name through VDLC.

sna rsrb

To specify the entities that the SNA feature will simulate at the remote source-route bridge (RSRB), use the **sna rsrb** interface configuration command. 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 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.

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 host name through the RSRB.

sna rsrb enable-host

To enable an RSRB SAP for use by SNA Service Point feature, use the **sna rsrb enable-host** global configuration command. 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 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.

Examples

In the following example, the local SAP address 10 of the RSRB is enabled for use by the ibm3745 host PU:

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 150.10.13.1
source-bridge remote-peer 99 tcp 150.10.13.2

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 150.10.13.1 255.255.255.0
```

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 start

To specify that an attempt will be made to connect to the remote resource defined by host name through the RSRB, use the **sna rsrb start** global configuration command. 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.

Usage Guidelines

Before issuing this command, you must enable the correct local SAP with the appropriate enable command (**sna rsrb enable-host**).

Examples

In the following example, the SNA Service Point will initiate a connection with the ibm3745 host PU across the RSRB link:

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 150.10.13.1
source-bridge remote-peer 99 tcp 150.10.13.2

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 150.10.13.1 255.255.255.0
```

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** interface configuration command. 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.

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 an SNA host over a Frame Relay connection.
sna host (QLLC)	Defines a link to an SNA host over an X.25/QLLC connection.
sna host (SDLC)	Defines a link to an SNA host over an SDLC connection.
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 vdlc

To identify the local virtual ring and virtual MAC address that will be used to establish SNA host connections over DLSw+ using virtual data-link control, use the **sna vdlc** global configuration command. 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 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.

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 150.10.16.2
dlsw remote-peer 0 tcp 150.10.16.1

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 150.10.16.2 255.255.255.0
 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 host name through VDLC.
source-bridge ring-group	Defines or removes a ring group from the configuration.

sna vdlc enable-host

To enable a SAP for use by SNA Service Point feature, use the **sna vdlc enable-host** global configuration command. 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 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.

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 150.10.16.2
dlsw remote-peer 0 tcp 150.10.16.1

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 150.10.16.2 255.255.255.0
 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, RSRB, or VDLC connections.

sna vdlc start

To specify that an attempt will be made to connect to the remote resource defined by host name through virtual data-link control (VDLC), use the **sna vdlc start** global configuration command. 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.

Usage Guidelines

Before issuing this command, you must enable the correct local SAP with the **sna vdlc enable-host** command.

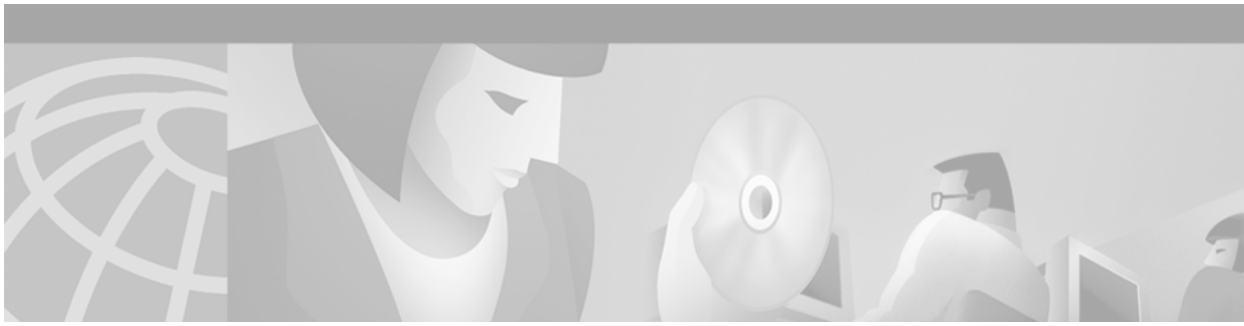
Examples

In the following example, SNA Service Point uses virtual data-link control to initiate a connection with the host PU HOST-B:

```
source-bridge ring-group 99
dlsw local-peer peer-id 150.10.16.2
dlsw remote-peer 0 tcp 150.10.16.1

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 150.10.16.2 255.255.255.0
 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 DLSw+ using VDLC.



SNA Switching Services Commands

Use the commands in this chapter to configure and monitor the SNA Switching Services (SNASw) feature. For SNASw configuration tasks and examples, refer to the "Configuring SNA Switching Services" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

ping sna

To initiate an APPC session with a named destination LU to run the APING transaction program to check network integrity and timing characteristics, use the **ping sna** privileged EXEC command.

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.
-i *number-iterations*	(Optional) Specifies number of iterations.
-m *mode*	(Optional) Specifies APPC mode to use.
-n	(Optional) Skips any security (SECURITY=NONE).
-r	(Optional) Displays route taken by APPC PING.
-s *size*	(Optional) Specifies the size of the of the data block to be sent.
-t *tpname*	(Optional) Specifies TP to start on the server.
-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 1 to 8 characters.
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, **ping sna** will send the quantity of data represented by **-s** *size*, **-i** *number-iterations*, and **-c** *consecutive blocks*. 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 T.

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:

```
ping sna NETA.CP001
```

Related Commands

Command	Description
show snasw session	Displays the SNASw session objects.

show snasw class-of-service

To display the COS definitions predefined to SNASw, use the **show snasw class-of-service** command.

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 TG rows.
detail	(Optional) Indicates a detailed, multiline display of all fields returned for COS display.

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.

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.

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.

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.

Examples

The following is an example of 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 SNASw link objects.

show snasw directory

To display the SNASw directory entries, use the **show snasw directory** command.

show snasw directory [**name** *resourcenamefilter*] [**brief** | **detail**]

Syntax Description

name *resourcenamefilter*	(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 CP name, network node server name, and entry type.
detail	(Optional) Indicates a detailed, multiline display of all fields returned for the directory display.

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.

Examples

The following is an example of the **show snasw directory** command:

```
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 DLC trace information to the console, use the **show snasw dlctrace** command.

show snasw dlctrace [**all** | **last** *number-records* | **next** *number-records*] [**brief** | **detail**] [**filter** *filter-string*] [**id** *recordid*]

Syntax Description

all	(Optional) Indicates that all records in the dlctrace buffer are displayed.
last *number-records*	(Optional) Indicates the last *n* 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 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 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 are filtered. Only frames that contain the filter-string are displayed.
id *recordid*	(Optional) Indicates the 1 to 999,999 trace record identifier. Only the frame ID that matches the record specified is displayed.

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.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples

The following is an example of 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 SNASw 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 PUs on the DLUS.
detail	(Optional) Indicates the detailed, multiline display that shows all fields returned for DLUS displayed.

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.

Examples

The following is an example of 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 trace on the router console, use the **show snasw ipstrace** command.

show snasw ipstrace [**all** | **next** *number-records* | **last** *number-records*] [**filter** *filter-string*] [**id** *recordid*]

Syntax Description

all	(Optional) Specifies all records are displayed
next *number-records*	(Optional) Displays records from beginning or following record IS.
last *number-records*	(Optional) Indicates that the last *n* 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.
id *recordid*	(Optional) Indicates the 1 to 999,999 trace record identifier. Only the frame ID that matches the record specified are displayed.

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.

Examples

The following is an example of 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 SNASw link objects, use the **show snasw link** command.

show snasw link [**brief** | **detail**] [**cpname** *cpnamefilter*] [**name** *linknamefilter*] [**port** *portnamefilter*] [**rmac** *macfilter*] [**xid** *xidfilter*]

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 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 displayed.
cpname *cpnamefilter*	(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 *portnamefilter*	(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 *macfilter*	(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 *xidfilter*	(Optional) Indicates a 4-byte XID (idnum/idblk) specified in hexadecimal form. Only links matching the configured XID are displayed.

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.

Examples

The following is an example of 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.

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 3 describes the significant fields shown in the output.

Table 3 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 SNASw modes, use the **show snasw mode** command.

show snasw mode

Syntax Description

This command has no arguments or keywords.

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.

Examples

The following is an example of 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 COS definitions predefined to SNASw.

show snasw node

To display details and statistics of the SNASw operation, use the **show snasw node** command.

show snasw node

Syntax Description

This command has no arguments or keywords.

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.

Examples

The following is an example of 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 directroy 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
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**] [**all | next** *number-records* **| last** *number-records*] [**filter** *filterstring*] [**id** *recordid*]

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.
all	(Optional) Specifies all records are displayed.
next *number-records*	(Optional) Displays records from the beginning or following a record ID.
last *number-records*	(Optional) Indicates that the last *n* 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 *filterstring*	(Optional) Shows output filtered on a specific string.
id *recordid*	(Optional) Indicates the 1 to 99999 trace record identifier. Only the frame ID that matches the record specified is displayed.

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.

Examples

The following is an example of 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 SNA problem determination log cyclic buffer.

show snasw port

To display the SNASw port objects, use the **show snasw port** command.

show snasw port [**brief** | **detail**] [**name** *portnamefilter*]

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.
name *portnamefilter*	(Optional) Indicates the name of the port to filter for which information is displayed. Only ports matching name are displayed.

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.

Examples

The following is an example of 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 SNASw PUs that require or request SSCP-PU services, use the **show snasw pu** command.

show snasw pu [**brief** | **detail**] [**dlus** *dlusfilter*] [**name** *punamefilter*]

Syntax Description

brief	(Optional) Indicates that one-line per PU is displayed. The brief version includes the PU name, PU ID, state, defined DLUS, and current DLUS.
detail	(Optional) Indicates that a detailed, multiline display that shows all possible fields returned for a link is displayed.
dlus *dlusfilter*	(Optional) Indicates the fully qualified DLUS name (1 to 17 characters). Only PUs that are currently served by the DLUS specified are displayed.
name *punamefilter*	(Optional) Indicates a PU name to filter (1 to 8 characters). Only PUs matching this name are displayed.

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.

Examples

The following is an example of 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 SNASw RTP connections, use the **show snasw rtp** command.

show snasw rtp [**brief** | **detail**] [**class-of-service** *cosname*] [**cpname** *netid.cpname*] [**name** *connectionnamefilter*] [**tcid** *tcidconnection*]

Syntax Description

brief	(Optional) Indicates that one-line per RTP is displayed. The brief version includes the RTP name, local TCID, remote TCID, remote cpname, and COS.
detail	(Optional) Indicates a detailed, multiline display with all fields returned for RTP is displayed.
class-of-service *cosname*	(Optional) Shows specific HPR RTP connections by COS name.
cpname *netid.cpname*	(Optional) Shows specific HPR RTP connections by fully qualified partner CP name, consisting of both network ID and cpname.
name *connectionnamefilter*	(Optional) Indicates the name of the RTP connection (1 to 8 characters). Only TG records origins or destinations that match the specified name or node records are displayed.
tcid *tcidconnection*	(Optional) Shows the specific HPR RTP connection for the local TCID connections.

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.

Examples

The following is an example of the **show snasw rtp** command:

```
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
```

Related Commands

Command	Description
show snasw session	Displays the SNASw session objects.

show snasw session

To display the SNASw session objects, use the **show snasw session** command.

show snasw session [**local | dlur | intermediate**] [**name** *sessionnamefilter*] [**pcid** *pcidfilter*] [**brief | detail | intermediate**]

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 CP-CP sessions and DLUR-DLUS sessions.
dlur	(Optional) Indicates that the scope of the display is limited to the types of sessions indicated. DLUS sessions are 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 *sessionnamefilter*	(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 *pcidfilter*	(Optional) Indicates an 8-byte 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 a detailed, multiline display that shows all fields returned for the session is displayed.

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.

Examples

The following is an example of 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
      ----------------  -----------------  -----------------  -------- -------

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 the SNASw node-wide information, use the **show snasw statistics** command.

show snasw statistics

Syntax Description

This command has no arguments or keywords.

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.

Examples

The following is an example of 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 [**all** | **next** *number-records* | **last** *number-records*] [**id** *recordid*] [**filter** *filter-string*]

Syntax Description

all	(Optional) Specifies all records are displayed.
next *number-records*	(Optional) Displays records from the start or starting with the record ID.
last *number-records*	(Optional) Displays records from the end or prior to the record ID. Indicates that the last *n* 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.
id *recordid*	(Optional) Indicates a 1 to 999,999 trace record identifier.
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.

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.

Examples

The following is an example of 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 the SNASw topology records, use the **show snasw topology** command.

show snasw topology [**name** *cpnamefilter*] [**brief** | **detail**]

Syntax Description

name *cpnamefilter*	(Optional) Indicates the fully qualified name of the 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 a detailed, multiline display of topology information.

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.

Examples

The following is an example of 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 an example of the **show snasw topology detail** command:

```
bernie# 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.

snasw cpname

To define a control point name for SNASw, use the **snasw cpname** global configuration command. To deactivate SNASw and remove the control point definition, use the **no** form of this command.

snasw cpname {*netid.cpname* | *netid* [*hostname*| **ip-address** *interface-name*]}
[**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 cpname.
netid	Partial CP name, which consists of only a network ID. If this option is selected, the hostname or IP address operands must also be configured to complete the fully qualified cpname.
hostname	(Optional) Indicates a CP name built using the hostname configured on the router. When configuring this operand, code a NET ID only. The last eight characters of the hostname are used to complete the CP name.
ip-address *interface-name*	(Optional) Indicates the CP name built by deriving the cpname from the IP address on the interface indicated in the *interface-name*. When configured, this operand requires a *netid* operand. In addition, a portion of the cpname may be configured. The remaining characters of the cpname that are not configured are generated from the IP address indicated. The generated characters are derived from a hexadecimal format of the IP address for the interface specified.
max-pacing-window *max-value*	(Optional) Indicates the upper limit of the receive pacing window size for intermediate sessions. When variable pacing is being used, the receive window size will never exceed this value. It may be necessary to configure a small 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) are to be removed from incoming BINDs 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.

Usage Guidelines

You can also deactivate SNASw without removing the **snasw cpname** definition using the **snasw stop** privileged EXEC command. This enables you to stop and restart SNASw without losing the SNASw configuration. Using **no snasw cpname** loses all SNASw configuration commands entered.

Coding of a cpname is required for SNASw. Only one **snasw cpname** command is allowed at a time. The **snasw cpname** command cannot be changed without first deleting the previous definition using the **no** form of the command. If SNASw is active, the **no** form deactivates it. If it is inactive, **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
```

Related Commands

Command	Description
snasw start	Starts SNASw.
snasw stop	Shuts down SNASw.

snasw dlcfilter

To filter frames being captured, use the **snasw dlcfilter** global configuration command. To disable the filtering of frames arriving and leaving SNASw, use the **no** form of this command.

snasw dlcfilter [**link** *linkname* [**session** *session-address*]] [**port** *portname*] [**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 *linkname* [**session** *session-address*]	(Optional) Specifies the link name upon which the DLC trace is filtered (one to eight characters). All incoming and outgoing frames matching this link are traced.
port *portname*	(Optional) Specifies the port name upon which the port is filtered (one to eight characters). All incoming and outgoing frames matching this port are traced.
rmac *mac-address-value* [**session** *session-address*]	(Optional) Specifies the MAC address upon which the DLC trace is filtered. All incoming and outgoing frames matching this MAC address are traced.
rtp *rtp-name* [**session** *session-address*]	(Optional) Specifies the RTP name upon which the RTP is filtered (one to eight characters). All incoming and outgoing frames matching this RTP connection name are traced.
type	(Optional) Indicates that one or more frame type filters follow. Use the **type** operand to further refine the filter to specify one or more frame types.
cls	(Optional) Indicates that commands to the local DLC are traced.
hpr-cntl	(Optional) Indicates that the HPR format identifier 5 (FID5), which does not carry an SNA data payload, is traced.
hpr-data	(Optional) Indicates that the HPR format identifier 5 (FID5), which carry an SNA data payload, is traced.
isr	(Optional) Indicates that the SNA and APPN format identifier 2 (FID2) are traced.
xid	(Optional) Indicates that the XID frames are traced.

Defaults

This command defaults to no filtering, and all frames are traced.

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.

Usage Guidelines

The **snasw dlcfilter** command is typically used to limit the output of the **snasw dlctrace** command to a manageable amount of trace data. Running the **snasw dlctrace** consumes CPU and memory. Using the **snasw dlctrace** 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 multiple filters are coded for all filters except the type filter, the frame only has to pass a single filter to be included in the trace. If the type filter is coded, the frame must pass the type filter and at least one of the other filters that is coded to be included in the trace.

Examples

The following are examples of how to configure the **snasw dlcfilter** command:

```
snasw dlcfilter link cmc1link
snasw dlcfilter rmac 4001.1234.1001
snasw dlcfilter type xid
```

Related Commands

Command	Description
snasw dlctrace	Traces frames arriving and leaving SNASw.
debug snasw dlc	Displays real-time DLC trace data to the console.
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.

snasw dlctrace

To trace frames arriving and leaving SNASw, use the **snasw dlctrace** global configuration command. 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 DLC trace buffer requested. The minimum buffer size is 100, while the maximum is 16000.
file *filename*	(Optional) Specifies the file name for the DLC trace buffer file when writing this file to the file server. Use the following format: protocol://host/path/filename.
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 are truncated and are not included in the trace. The default is that the entire frame is traced.
auto-terse	(Optional) Indicates LU-LU and SSCP-LU session data frames should be truncated after the SNA RH. Also truncates NMVTs on the SSCP-PU session. Control frames (for example, XID, BIND, 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**—Indicates a text file is written with a one-line-per-frame summary for each frame. • **detail**—Indicates a text file is written with a frame summary line followed by a complete hexadecimal dump of the frame. • **analyzer**—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.

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 using the analyzer format, 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 there was routing information field (RIF) data present on the actual data-link frame, that information is omitted in the dlctrace. In addition, information in the LLC header (for example, Nr, Ns counts) are not reliably transferred to the traced frame. However, the remainder of the frame, including all 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://171.69.120.21/dlcfiles/dlc/trc
```

Related Commands

Command	Description
snasw dlcfilter	Filters frames being captured.
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.
show snasw dlctrace	Displays the captured DLC trace information on the console.

snasw dlus

To specify parameters related to DLUR/DLUS functionality, use the **snasw dlus** global configuration command. 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 DLUS/DLUR connection was established, an incoming 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** argument 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.

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
```

Related Commands

Command	Description
show snasw dlus	Displays the SNASw DLUS objects.

snasw dump

To copy problem determination logs and traces from internal buffers to an external file server, use the **snasw dump** privileged EXEC command.

snasw dump all | dlctrace | ipstrace | summary-ipstrace | pdlog

Syntax Description

all	Indicates all configured trace and problem determination buffers should be transferred. The **file** operand must be configured on the enabling configuration command for the buffers to be dumped. Traces that run but do not have the **file** operand coded are not transferred.
dlctrace	Indicates the DLC trace buffer is transferred to a file server. If **file** is configured on the **snasw dlctrace** command, the URL specified is used for transferring the DLC trace file. If **file** is not configured on the **snasw dlctrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and file name for the transferred file.
ipstrace	Indicates the IPS trace buffer is transferred to a file server. If **file** is configured on the **snasw ipstrace** command, the URL specified is used for transferring the ipstrace file. If **file** is not configured on the **snasw ipstrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and file name for the transferred file.
summary-ipstrace	Indicates the summary IPS trace buffer is transferred to a file server. If **file** is coded on the **snasw summary-ipstrace** command, the URL specified is used for transferring the summary ipstrace file. If **file** is not coded on the **snasw ipstrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and file name for the transferred file.
pdlog	Indicates the problem determination log buffer is transferred to a file server. If **file** is coded on the **snasw pdlog** command, the URL specified is used for transferring the pdlog file. If **file** is not coded, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and file name for the transferred file.

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.

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. 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 under the **snasw trace** configuration (for example, **snasw dlctrace**).

When you use FTP, make sure you configure **ip ftp username** and **ip ftp password** 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:

```
snasw dump all
snasw dump dlctrace
```

Related Commands

Command	Description
snasw dlctrace	Traces frames arriving and leaving SNASw.
snasw ipstrace	Sets up a trace buffer and begins tracing IPS trace elements.
snasw pdlog	Controls message logging to the console and the SNA problem determination log cyclic buffer.

snasw event

To indicate which normal events are logged to the console, use the **snasw event** global configuration command. 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 CP-CP session state changes.
dlc	(Optional) Indicates 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 DLUS events are sent to the pdlog/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.

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 APPN priorities, use the **snasw ip-precedence** global configuration command. 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.

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** commands, use the **snasw ipsfilter** global configuration command. 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 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 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.

Usage Guidelines

The command defaults to no 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
snasw ipstrace	Sets up a trace buffer and begins tracing IPS trace elements.
show snasw ipstrace	Displays the interprocess signal trace on the router console.
debug snasw ips	Displays realtime ipstrace information to the console.

snasw ipstrace

To set up a trace buffer and begin tracing IPS trace elements, use the **snasw ipstrace** global configuration command. 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 if 10 KB; the maximum is 16000 KB.
file *filename*	(Optional) Specifies the file name for the IPS trace buffer file when writing this file to the server.
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.

Usage Guidelines

Use the **snasw ipstrace** command when directed by 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
snasw ipsfilter	Filters interprocess signal trace elements being traced using the **snasw ipstrace** or **debug snasw ips** commands.
show snasw ipstrace	Displays interprocess signal trace on the router console.
debug snasw ips	Displays realtime IPS trace information to the console.

snasw link

To configure upstream links, use the **snasw link** global configuration command. To remove the configuration of upstream links, use the **no** form of this command.

snasw link *linkname* **port** *portname* **rmac** *mac-address* | **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 SNASw port from which this link will connect.
rmac *mac-address*	Specifies the 48-bit MAC address of the destination station. Either this operand or **ip-dest** is required. RMAC is required for all links associated with ports that are not HPR/IP ports.
ip-dest *ip-address*	Indicates the IP address or DNS name of the destination stations. Either this operand or **rmac** is required. For all links associated with HPR/IP ports, **ip-dest** is required.
rsap *sap-value*	(Optional) Indicates the destination 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 non-secure.

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 12.0T.

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.

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
```

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** global configuration command. To disable the location of a resource, use the **no** form of this command.

snasw location *resource-name* **owning-cp** *cpname*

no snasw location *resource-name*

Syntax Description

resource-name	Indicates the fully qualified name of the resource for which location information is being configured (3 to 17 characters).
owning-cp *cpname*	Indicates the fully qualified CP name where the resource resides.

Defaults

No default behaviors 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	Support for wildcards in the *cpname* argument was added.

Usage Guidelines

The **snasw location** command is typically used when a LEN node link is established with a destination LU. The **snasw location** command allows SNASw to route session requests over the LEN node link to the resources named.

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 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 in. 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 in.

Do not use the **snasw location** command to predefine the location of any resource that can be found dynamically using APPN searches (for example, resources on upstream APPN nodes or upstream/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 using the wildcard character for this purpose, the * symbol must be coded in both the *resource-name* and the *cpname*. If any real device attaches with a CP name that matches the non-wildcard portion of the **owning-cp** *cpname* specified, a location association will be made that replaces the wildcard characters of the CPname in the position of the *resource-name*. For example, if a definition **snasw location NETA.LU*01 owning-cp NETA.CP*** is coded and CP with the name NETA.CPABCD connects in, 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 non-wildcard portion of the *cpname* argument, a corresponding location association will be made for the *resource-name* with that CP name.

Examples

The following is an example of how to configure the **snasw location** command:

```
snasw location NETA.INDEPLU owning-cp NETA.LENHOSTA
```

Related Commands

Command	Description
show snasw directory	Displays the SNASw directory entries.

snasw mode

To define a new mode and associate it with an existing class of service (COS), use the **snasw mode** global configuration command. 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.

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 DLC trace, IPS trace, and problem determination log when a specified SNA Switching Services (SNASw) message is displayed, use the **snasw msgdump** global configuration command. To disable automatic dumping, use the **no** form of this command.

snasw msgdump *message*

no snasw msgdump *message*

Syntax Description

message	SNASw message to trigger the automatic dump.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Examples

The following are examples of the **snasw msgdump** command:

```
snasw msgdump %SNASW-6-CS_LOG_60
```

snasw pathswitch

To force an HPR pathswitch for an RTP connection, use the **snasw pathswitch** privileged EXEC command.

snasw pathswitch [*rtp-connection-name* | **all**]

Syntax Description

rtp-connection-name	(Optional) Specifies the RTP connection to path-switch. This is an eight-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.

Usage Guidelines

If a specific connection name is coded, and no such connection is known to 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:

```
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 SNA problem determination log cyclic buffer, use the **snasw pdlog** global configuration command. 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 is 10 KB, and the maximum is 16000 KB.
file *filename*	(Optional) Indicates the URL for writing the pdlog file to a server. Use the following format: *protocol://host/path/filename*.
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.

Usage Guidelines

Use the **snasw pdlog** command to customize the type of information you prefer to see on the router console from the 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 SNA 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* [**ldlc** [*liveness-time t1-retry-time t1-retry-count*]] [**maxbtu** *max-btu-size*] [**vnname** *virtual-node-name*] [**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**] [**hpr-sap** *hpr-sap-value*] [**max-links** *link-limit-value*] [**maxbtu** *max-btu-size*] [**nns-required**] [**sap** *sap-value*] [**vnname** *virtual-node-name*] [**nostart**]

no snasw port *port-name*

All Other Types of Ports

snasw port *port-name interface-name* [**conntype nohpr | len | dyncplen**] [**nns-required**] [**hpr-sap** *hpr-sap-value*] [**max-links** *link-limit-value*] [**maxbtu** *max-btu-size*] [**sap** *sap-value*] [**vnname** *virtual-node-name*] [**nostart**]

no snasw port *port-name*

Syntax Description

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 will communicate. Allowable interfaces are Token Ring, Ethernet, VLAN, or loopback.
hpr-ip	Indicates that the port is High-Performance Routing (HPR)/IP.
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, and the default is 2 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, and the default is 2 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, and the default is 10 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.
vnname *virtual-node-name*	(Optional) Indicates the network qualified virtual node name 3 to 17 characters) of the connection network being defined.
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	Indicates the name of the virtual Token Ring interface.
conntype nohpr | len | dyncplen	(Optional) The **conntype** keyword indicates the connection type for the port. The connection type can be set to one of three values: **nohpr**, **len**, or **dyncplen**. If this keyword is not configured, HPR-capable links are established. The **nohpr** keyword indicates that the HPR is not supported but Advanced Peer-to-Peer Networking (APPN) connections with control point (CP)-CP sessions are permitted. The **len** keyword indicates that APPN connections are not allowed; only low-entry networking node (LEN) node-level connectivity is negotiated. The **dyncplen** keyword (similar to LEN node in functionality) also replaces the **cpname** keyword. This option is specifically intended for users with XID3-capable devices that send CP names, but whose CP names configured on these devices have not been configured uniquely across the devices. Therefore, a default **cpname** must be generated to have a properly functioning APPN connection management and directory function.
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. When this link limit is reached, the port will 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.
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.

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.
vnname *virtual-node-name*	(Optional) Indicates the network qualified virtual node name 3 to 17 characters) of the connection network being defined.
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	Indicates the name of the virtual Token Ring interface.
conntype nohpr | len | dyncplen	(Optional) The **conntype** keyword indicates the connection type for the port. The connection type can be set to one of three values: **nohpr**, **len**, or **dyncplen**. If this keyword is not configured, HPR-capable links are established. The **nohpr** keyword indicates that the HPR is not supported but Advanced Peer-to-Peer Networking (APPN) connections with control point (CP)-CP sessions are permitted. The **len** keyword indicates that APPN connections are not allowed; only low-entry networking node (LEN) node-level connectivity is negotiated. The **dyncplen** keyword (similar to LEN node in functionality) also replaces the **cpname** keyword. This option is specifically intended for users with XID3-capable devices that send CP names, but whose CP names configured on these devices have not been configured uniquely across the devices. Therefore, a default **cpname** must be generated to have a properly functioning APPN connection management and directory function.
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. When this link limit is reached, the port will 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.
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.

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. • 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 logical unit (LU)-LU or Intermediate Session Routing (ISR) sessions. **Note** This keyword is relevant only for ports that will be accepting downstream connections from devices. It is not relevant for upstream ports.
sap *sap-value*	(Optional) Indicates the local SAP (LSAP) value.

Defaults

No default behaviors 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.

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.

Note 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 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.

Examples

The following are examples of how to configure the **snasw port** command:

```
snasw port SRBG Virtual-TokenRing0 conntype nohpr
snasw port UPSTREAM TokenRing1/1
snasw port dlswport vdlc 30 mac 4000.33333.4444
snasw port HPRIP hpr-ip Loopback0
snasw port TRVLAN Vlan1/1 vnname NETA.CONNET
```

Related Commands

Command	Description
snasw link	Configures upstream links.
show snasw port	Displays the SNASw port objects.

snasw rtp pathswitch-timers

To tune the Realtime Transport Protocol (RTP) path-switch timers for an SNASwitch, use the **snasw rtp pathswitch-timers** command in global configuration mode. To restore the default settings for the RTP path-switch 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 path switch for low-priority RTPs. Allowed values are from 5 to 65535 seconds.
medium-priority	Number of seconds to attempt path switch for medium-priority RTPs. Allowed values are from 5 to 65535 seconds.
high-priority	Number of seconds to attempt path switch for high-priority RTPs. Allowed values are from 5 to 65535 seconds.
network-priority	Number of seconds to attempt path switch for network-priority RTPs. Allowed values are from 5 to 120 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.

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 SNASwitch router or any other 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 path-switch timer argument 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 path-switch timers:

```
router(config)# snasw rtp pathswitch-timers 160 80 40 20
```

snasw start

To start SNASw, use the **snasw start** privileged EXEC command.

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.

Usage Guidelines

If not enough memory exists to start SNASw, a message indicating lack of memory is issued. A 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:

```
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 CP-CP sessions with a partner CP, use the **snasw start cp-cp** privileged EXEC command.

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.

Usage Guidelines

Use the **snasw start cp-cp** command if CP-CP sessions fail permanently or temporarily, but beyond the timeframe 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, 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 timeframe for automatic session retry indicates a problem, and should be reported.

Examples

The following is an example of the **snasw start cp-cp** command:

```
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** privileged EXEC command.

snasw start link *linkname*

Syntax Description

linkname	Indicates the name of the link as configured or shown in **show snasw link**.

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.

Usage Guidelines

Use the **snasw start link** command to initiate a connection sequence for a link that is defined but not currently active. Unless **nostart** 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:

```
snasw start link CMCHOST1
```

Related Commands

Command	Description
show snasw link	Displays the SNASw link objects.
snasw stop link	Stops an active link.

snasw start port

To start an inactive port, use the **snasw start port** privileged EXEC command.

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.

Usage Guidelines

Use the **snasw start port** command to enable a port that is defined to the configuration but is not currently active. Unless **nostart** 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:

```
snasw start port TOKEN0
```

Related Commands

Command	Description
show snasw port	Displays the SNASw port objects.
snasw stop port	Stops an active port.

snasw stop

To shut down SNASw, use the **snasw stop** privileged EXEC command.

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.

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:

```
snasw stop
```

Related Commands

Command	Description
snasw start	Starts SNASw.

snasw stop cp-cp

To terminate CP-CP sessions with a partner CP, use the **snasw stop cp-cp** privileged EXEC command.

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.

Usage Guidelines

If the primary NN server (uplink) fails, CP-CP sessions are established with a backup, if one is available. When the link to the primary recovers, 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 SNA switch to potentially restart sessions with the same or alternate destination LU.

Examples

The following is an example of the **snasw stop cp-cp** command:

```
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** privileged EXEC command.

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.

Usage Guidelines

Use the **snasw stop link** command to deactivate a link to a specified partner CP. All non-HPR sessions established using the link are disconnected. HPR sessions are disrupted only if there is no alternate route 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:

```
snasw stop link CMCHOST1
```

Related Commands

Command	Description
show snasw link	Displays the SNASw link objects.

snasw stop port

To stop an active port, use the **snasw stop port** privileged EXEC command.

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.

Usage Guidelines

Use the **snasw stop port** command to disable a specified port without removing it from the configuration. All non-HPR sessions established using the port and all links are shut down on the port. HPR sessions are disrupted only if there is no alternate route available.

Examples

The following is an example of the **snasw stop port** command:

```
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** privileged EXEC command.

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.

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 don't expect to use the session later.

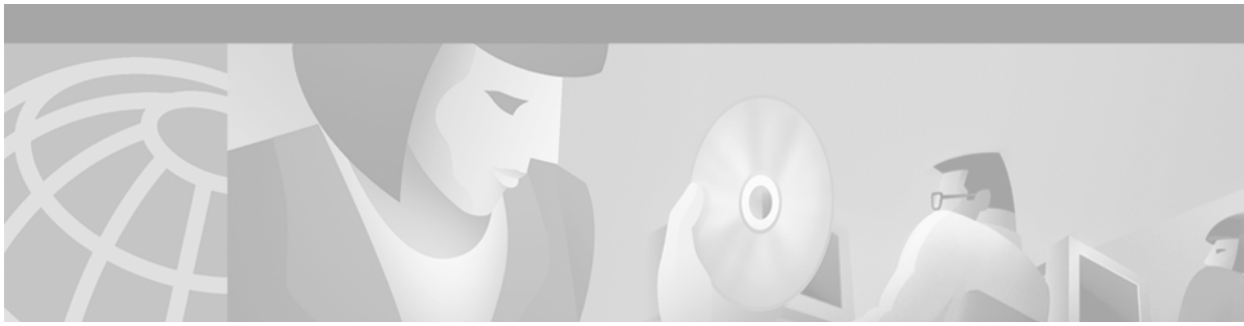
Examples

The following is an example of the **snasw stop session** command:

```
snasw stop session C3BBD36EA9CBA1AF
```

Related Commands

Command	Description
show snasw session	Displays the SNASw session objects.



Cisco Transaction Connection Commands

Use the commands in this chapter to configure and monitor the Cisco Transaction Connection (CTRC) feature. Refer to the *Cisco IOS Debug Command Reference* for information about using debugging commands, including those available for CTRC. For CTRC configuration tasks and examples, refer to the "Configuring Cisco Transaction Connection" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

clear dbconn connection

To break a client connection to DB2, use the **clear dbconn connection** privileged EXEC command, specifying the ID of the connection you want to terminate.

clear dbconn connection *connection-id*

Syntax Description

connection-id	Identification number for client connection to DB2.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples

The following example shows the client connection 786A7C being cleared:

```
clear dbconn connection 786A7C

Connection 786A7C cleared
```

Related Commands

Command	Description
show dbconn connection	Displays the status of CTRC connections to DB2.

clear dbconn statistic

To clear a specific statistic or all CTRC statistics concerning communications with DB2, use the **clear dbconn statistic** privileged EXEC command.

clear dbconn statistic {**chains** | **clientturnaround** | **connectionsdown** | **connectionsup** | **every** | **hostreceived** | **hostresponse** | **hostsent** | **maxconnections**}

Syntax Description

chains	Clears the number of command chains created between CTRC and DB2.
clientturnaround	Clears statistics for average time from receiving a DB2 client communication to sending that client a response.
connectionsdown	Clears statistics for number of connections down between CTRC and DB2.
connectionsup	Clears statistics for number of connections created between CTRC and DB2.
every	Clears the complete statistics dump between CTRC and DB2.
hostreceived	Clears statistics for number of bytes received from DB2 hosts.
hostresponse	Clears statistics for average DB2 host response time.
hostsent	Clears statistics for number of bytes sent to DB2 hosts.
maxconnections	Clears statistics for maximum number of concurrent connections to CICS clients.

Defaults

No default behavior 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.

Examples

The following example clears the stored statistics for the number of bytes the current router has received from DB2 hosts:

```
clear dbconn statistic hostreceived
```

Related Commands

Command	Description
show dbconn statistic	Displays all CTRC statistics concerning communications with DB2.

clear txconn connection

To clear a CTRC connection to a CICS client and all associated transactions, use the **clear txconn connection** privileged EXEC command.

clear txconn connection *connection-id*

Syntax Description

connection-id	CICS connection identification number.

Defaults

No default behavior 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.

Examples

The following example clears the specified CICS client connection number 62146088 and all its transactions:

```
clear txconn connection 62146088

% Connection 62146088 cleared
```

Related Commands

Command	Description
clear txconn transaction	Terminates a specified CICS transaction.
show txconn connection	Displays a list of all of the CTRC connections of the router to CICS clients.

clear txconn statistic

To clear a specific statistic or all CTRC statistics concerning communications with CICS, use the **clear txconn statistic** privileged EXEC command.

clear txconn statistic {**allocatetime** | **clientreceived** | **clientsent** | **clientturnaround** | **every** | **hostreceived** | **hostresponse** | **hostsent** | **maxconnections** | **maxtransactions** | **totalconnections** | **totaltransactions**}

Syntax Description

allocatetime	Clears statistics for average time spent waiting for APPC allocate operation to complete.
clientreceived	Clears statistics for number of bytes received from CICS clients.
clientsent	Clears statistics for number of bytes sent to CICS clients.
clientturnaround	Clears statistics for average time from receiving a CICS client communication to sending that client a response.
every	Clears every statistic concerning the current router's CTRC communications with CICS.
hostreceived	Clears statistics for number of bytes received from CICS hosts.
hostresponse	Clears statistics for average CICS host response time.
hostsent	Clears statistics for number of bytes sent to CICS hosts.
maxconnections	Clears statistics for maximum number of concurrent connections to CICS clients.
maxtransactions	Clears statistics for maximum number of concurrent transactions with CICS hosts.
totalconnections	Clears statistics for total number of connections to CICS clients.
totaltransactions	Clears statistics for total number of CICS transactions processed.

Defaults

No default behavior 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.

Examples

The following example clears the stored statistics for the number of bytes the current router has received from CICS clients:

```
clear txconn statistic clientreceived
```

Related Commands

Command	Description
show txconn statistic	Displays information about the CTRC communications of the current router with CICS.

clear txconn transaction

To terminate a specified CICS transaction, use the **clear txconn transaction** privileged EXEC command. This command terminates the conversation with the host and returns DEALLOC_ABEND_PROG to the client.

clear txconn transaction *transaction-id*

Syntax Description

transaction-id	ID of the CICS transaction to be cleared.

Defaults

No default behavior 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.

Examples

The following example clears the CICS transaction number 621FC8E0:

```
clear txconn transaction 621FC8E0

% Transaction 621FC8E0 cleared
```

Related Commands

Command	Description
clear txconn connection	Clears a CTRC connection to a CICS client and all associated transactions.
show txconn transaction	Displays a list of all the CTRC transactions of the current router with CICS, transactions of a specified CTRC server, or transactions of a specified CICS client connection.

dbconn license

To configure client licenses for CTRC connections to DB2 or CICS, use the **dbconn license** global configuration command. To remove the licenses, use the **no** form of this command in privileged EXEC mode.

dbconn license *license-key* **connections** *licensed-connections* **expiration-date** *yyyymmdd*

no dbconn license

Syntax Description

license-key	License key obtained from your Cisco representative. The license key is a 32-character hexadecimal string that specifies the maximum number of CICS conversations or DB2 connections allowed for the CTRC router. The license key is generated for a specific router, and is based on the SNA Switching Services cpname for the router. Use the **show config | include cpname** command to view the cpname so you can provide it when you request the license key.
connections *licensed-connections*	Number of licensed connections. If the license is for an unlimited number of connections, omit the **connections** parameter.
expiration-date *yyyymmdd*	Date when a temporary license key expires, where *yyyy* is the year expressed in four digits, *mm* is the month expressed in two digits, and *dd* is the date expressed in two digits. If the license is for an unlimited time period (permanent license), omit the **expiration-date** parameter.

Defaults

If the number of licensed connections is not specified, the license key must allow an unlimited number of licensed connections. If the expiration date is not specified, the license key must be for a permanent license.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

Licenses are required for all CTRC installations. For testing and evaluation purposes, unlicensed CTRC installations allow you to establish two connections to DB2, or two conversations to CICS, or one to each. One license key is used for both CICS and DB2 communications, so you can use either the **dbconn license** command or the **txconn license** command to configure the CTRC router.

Examples

The following example shows the configuration of a CTRC router with a license that allows up to 4000 connections until January 1, 2005:

```
dbconn license 3C09A051320BAF020BFF45B3A2FF21D2 connections 4000 expiration-date 20050101
```

Related Commands

Command	Description
show dbconn license	Displays the status of CTRC licenses for DB2 communications.
show snasw node	Displays details and statistics of the SNASw operation.
show txconn license	Displays the status of licenses used for CTRC.
txconn license	Licenses a Cisco router for CTRC communications with CICS or DB2.

dbconn pem

To configure password expiration management (PEM) support for connections to DB2, use the **dbconn pem** global configuration command. To remove PEM support, use the **no** form of this command.

dbconn pem server *server-name* **rlu** *rlu-name* **mode** *mode-name* [**tpname** *tp-name*]

no dbconn pem server *server-name*

Syntax Description

server *server-name*	Name of the CTRC server that you want to configure for password management.
rlu *rlu-name*	Host remote LU name the server connects to when performing password management. This RLU ordinarily differs from the RLU values used in **dbconn server** or **txconn destination** commands. It may or may not be fully qualified.
mode *mode-name*	APPC stack mode the server uses when performing password management.
tpname *tp-name*	(Optional) Name of the PEM transaction program on the host (the APPC Signon transaction program, an architected APPC TP). The default value is \x06301 (0x06F3F0F1 in EBCDIC).

Defaults

If *tp-name* is not specified, the default value is \x06301 (0x06F3F0F1 in EBCDIC).

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.

Examples

The following example shows the configuration of PEM support on a CTRC server named DB2BUDD:

```
dbconn pem DB2BUDD rlu MVSLU01 mode #INTER
```

Related Commands

Command	Description
show dbconn server	Displays information about CTRC servers configured for DB2 communications.

dbconn ping

To determine whether CTRC servers are successfully connecting to DB2 host databases, use the **dbconn ping** EXEC command.

dbconn ping *server-name* [**userid** *user-id*] [**password** *password*] [**rdbname** *rdbname*]

Syntax Description

server-name	Name of the CTRC server for DB2 communications.
userid *user-id*	(Optional) User ID used to connect to the DB2 system.
password *password*	(Optional) Password used to connect to the DB2 system.
rdbname *rdbname*	(Optional) Name of the relational database to be contacted.

Defaults

If no user ID is specified, the ping connection is made without APPC security. The DB2 system's security settings determine whether the ping can succeed.

If no *rdbname* is specified, the relational database name configured for the CTRC server is used.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

This command can be used for CTRC servers that communicate with DB2 over either SNA or TCP/IP (dbconn servers and dbconn tcpservers). There is not a **no** form this command.

Examples

The following example illustrates using **dbconn ping** to verify the connection to the default database for the CTRC server BUDDY:

```
dbconn ping BUDDY

RDB named DB2510 on database server BUDDY successfully contacted!
Database server product id is QSQ03020, DB2 for OS/400 V3R2
Elapsed time was 00:00:00
```

Related Commands

Command	Description
show dbconn server	Displays information about CTRC servers configured for DB2 communications.
ping sna	Initiates an APPC session with a named destination LU to run the APING transaction program to check network integrity and timing characteristics.

dbconn server

To configure a CTRC server process for APPC communications with DB2, use the **dbconn server** global configuration command. To disable the server and remove its configuration, use the **no** form of this command.

dbconn server *server-name* [**idle-timeout** *minutes*] [**ipaddress** *ip-address*] [**keepalive attempts** *number*] [**keepalive interval** *seconds*] [**mode** *mode*] [**port** *port-number*] [**rdbname** *rdbname*] [**rlu** *remote-lu*] [**tpname** *tp-name*] [**window-size** *bytes*] [**wlm** {**off** | **on**}]

no dbconn server *server-name*

Syntax Description

server-name	Name of the CTRC server. Server names are user-defined strings up to 16 characters.
idle-timeout *idle-timeout*	(Optional) Time, in minutes, to wait for an idle client. If there is no activity from the client for this amount of time, the connection is forcibly broken. The time spent in waiting for a response from the DB2 system is not counted, only idle time in between client requests is counted. The maximum is 1440 minutes (24 hours). If no idle timeout is specified, the default is 0 (zero) for no timeout.
ipaddress *ip-address*	(Optional) IP address used by the CTRC server to receive a connection requesting DB2 communications. When a connection arrives, this IP address is used for matching and selecting the server from multiple configured servers. If you do not specify an IP address, the current server can handle DB2 connectivity requests sent to any IP address on the local router.
keepalive attempts *number*	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the client to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.
keepalive interval *seconds*	(Optional) The frequency for the CTRC server to send an acknowledgment message to the client to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
mode *mode*	(Optional) APPC mode used to allocate the conversation to the DB2 system. If no mode is specified, the default is #INTER. Performance might improve if you choose a mode such as IBMRDB. If you specify a mode that does not already exist, CTRC will create it.
port *port-number*	(Optional) Port used to listen for connections requesting DB2 communications. If no port is specified, the default is 446.
rdbname *rdbname*	(Optional) DB2 remote database name on the host. When a connection arrives, this name is used to identify and select the appropriate server from multiple configured servers. The string is used to match the RDB name sent by the client in the DRDA data stream at connect time. The default RDB name is an asterisk (*), which indicates that this CTRC server serves any remote database.

rlu *remote-lu*	(Optional) APPC remote LU used to allocate the connection to the DB2 system. An example is NETA.S103B345. If no remote LU is specified, the default is the configured server name which is set to uppercase and truncated to eight characters. An RLU need not be qualified with a NET ID. If you omit the NET ID, the NET ID of the router's SNA Switching Services control point is used to fully qualify the LU name.
tpname *tp-name*	(Optional) APPC remote transaction program name used to allocate the conversation to the DB2 system. If no TP name is specified the default is the architected DRDA TP name \x076DB.
window-size *bytes*	(Optional) TCP/IP receive window size. The maximum window size you can specify is 65,535 bytes, and the default is 4096 bytes.
wlm {**off** | **on**}	(Optional) Enables or disables Workload Manager load balancing. The default is "inactive-enabled."

Defaults

If you do not specify an idle timeout, client connections can continue regardless of how long they have been idle.

If you do not specify an IP address, the current server can handle DB2 connectivity requests sent to any IP address on the local router.

If you do not specify a keepalive attempt or a keepalive interval, the server makes up to three attempts to send an acknowledgment message every 120 seconds.

If you do not specify an APPC mode, the default value is #INTER. If you specify a mode that does not already exist, CTRC will create it.

If you do not specify a port number, the current server uses the default value of 446.

If you do not specify an rdbname, the server is configured to serve any remote database.

If you do not specify a remote LU, the default is the configured server name that is set to uppercase and truncated to eight characters. An RLU need not be qualified with a NET ID. If you omit the NET ID, the NET ID of the router's SNA Switching Services control point is used to fully qualify the LU name.

If you do not specify an APPC transaction program name, the default value is the architected DRDA TP name \x076DB.

If you do not specify a TCP receive window size, the default value is 4096 bytes.

The Workload Manager load balancing default is "inactive-enabled."

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.1(5)T	This command was enhanced to allow configuration of keepalive messages.

Usage Guidelines

You can configure more than one CTRC server per router for communications with DB2 or CICS. There is no limit on the number of CTRC servers. For each DB2 database system in your network, you can configure a CTRC server in the router configuration. Servers that are configured on the same router can share a port. CTRC txconn servers should use a different port.

Set **keepalive attempts** or **keepalive interval** to zero (0) to disable the keepalive messages.

Examples

The following example shows configuring a CTRC server named BUDDY to manage communications to a DB2 database named DB2510, using the IBMRDB APPC mode to allocate the conversation, and attempting five acknowledgment messages every 300 seconds:

```
dbconn server BUDDY rdbname DB2510 rlu STARW.BUDDY idle-timeout 20 keepalive attempts 5
keepalive interval 300 mode IBMRDB
```

Related Commands

Command	Description
clear dbconn connection	Breaks a client connection to DB2.
dbconn ping	Determines whether or not CTRC servers are successfully connecting to DB2 host databases.
show dbconn ports	Displays information about ports used for CTRC server communications to DB2.
show dbconn server	Displays information about CTRC servers configured for DB2 communications.
show snasw mode	Displays information about SNASw modes.

dbconn tcpserver

To configure a CTRC server process to communicate with IP-enabled DB2 databases, use the **dbconn tcpserver** global configuration command. To disable a server and remove its configuration, use the **no** form of this command.

dbconn tcpserver *server-name* [**idle-timeout** *minutes*] [**ip** *ip-address*] [**keepalive attempts** *number*] [**keepalive interval** *seconds*] [**port** *port-num*] [**rdbname** *rdbname*] **remote-hostname** *remote-hostname* **| remote-ip** *remote-ip-address* [**remote-keepalive attempts** *number*] [**remote-keepalive interval** *seconds*] [**remote-port** *remote-port*] [**window-size** *bytes*] [**wlm** {**off | on**}]

no dbconn tcpserver *server-name*

Syntax Description

server-name	Name of the CTRC server being configured for TCP passthrough communications with DB2.
idle-timeout *minutes*	(Optional) Time in minutes to wait for an idle client. If there is no activity from the client for this amount of time, the connection is forcibly broken. The time spent in waiting for a response from the DB2 system is not counted, only idle time in between client requests is counted. The maximum time is 1440 minutes (24 hours). If no idle timeout is specified, the default is 0 (zero) for no timeout.
ip *ip-address*	(Optional) IP address for the CTRC tcpserver process being configured. If not specified, the tcpserver receives client requests on all IP addresses configured for the router.
keepalive attempts *number*	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the client to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.
keepalive interval *seconds*	(Optional) The frequency for the CTRC server to send an acknowledgment message to the client to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
port *port-num*	(Optional) Port the tcpserver listens on for client requests. The default value is 446. A dbconn server and a dbconn tcpserver can share the same port.
rdbname *rdbname*	(Optional) DB2 remote database name on the host. When a connection arrives, this name is used to identify and select the appropriate tcpserver from multiple configured tcpservers. The string is used to match the RDB name sent by the client in the DRDA data stream at connect time. The default RDB name is an asterisk (*) which indicates that this CTRC tcpserver serves any remote database.
remote-hostname *remote-hostname* **| remote-ip** *remote-ip-address*	DNS host name of the remote database server to which you want to connect, or the IP address for the host where DB2 resides. You must specify either the name or the IP address of the host.
remote-keepalive attempts *number*	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the host to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.

remote-keepalive interval *seconds*	(Optional) The frequency for the CTRC server to send an acknowledgment message to the host to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.
remote-port *remote-port*	(Optional) Host port that listens for tcpserver communications from the router. The default value is 446.
window-size *bytes*	(Optional) This value is used for the TCP/IP receive window size. If no window size is specified, the default is 4096 bytes.
wlm {**off** | **on**}	(Optional) Enables or disables Workload Manager load balancing. The default is "inactive-enabled."

Defaults

If you do not specify an idle timeout period, the default value is zero for no timeout.

If you do not specify an IP address for the tcpserver, it can receive requests on any IP address configured for the router.

If you do not specify a keepalive attempt or a keepalive interval, the server makes three attempts to send an acknowledgment message to the client every 120 seconds. If you do not specify a remote-keepalive attempt or a remote-keepalive interval, the server makes three attempts to send an acknowledgment message to the host ever 120 seconds.

If you do not specify a port for the tcpserver, the default port is 446.

If you do not specify a remote database name for the DB2 system, the tcpserver can communicate with any rdbname.

If you do not specify a port for the remote DB2 system, the tcpserver uses the default value of 446.

If you do not specify a TCP/IP receive window size, the default value is 4096 bytes.

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(5)T	This command was enhanced to allow configuration of the keepalive interval.

Usage Guidelines

Configure a separate tcpserver for each DB2 system IP address. A dbconn server and a dbconn tcpserver can share the same port.

Examples

The following example shows configuring a tcpserver named BUDDTCP to manage connections to a DB2 database named DB2510, attempting up to five keepalive messages to the client and to the host every 300 seconds:

```
dbconn tcpserver BUDDTCP keepalive attempts 5 keepalive interval 300 port 446 rdbname
DB2510 remote-ip 198.147.235.39 remote-keepalive attempts 5 remote-keepalive interval 300
remote-port 446
```

Related Commands

Command	Description
dbconn ping	Determines whether or not CTRC servers are successfully connecting to DB2 host databases.
show dbconn server	Displays information about CTRC servers configured for DB2 communications.

show dbconn connection

To display the status of CTRC connections to DB2, use the **show dbconn connection** EXEC command.

show dbconn connection [*connection-id* | **server** *server-name* | **userid** *user-id* | **rdbname** *rdb-name*]

Syntax Description

connection-id	(Optional) Displays the status of a specified connection.
server *server-name*	(Optional) Displays connection information for the specified server.
userid *user-id*	(Optional) Displays connections for the specified user ID.
rdbname *rdb-name*	(Optional) Displays connections for the specified RDB name.

Defaults

If you do not specify any arguments, this command displays information for all CTRC connections to DB2 on the current router.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples

The following is sample output from the **show dbconn connection** command:

```
Router> show dbconn connection

ID       Server           Userid     ClientIPAddress Connect   Idle
6127E428 SERVERA          ALLIE      198.999.989.36  00:01:26  00:01:12
6127D34C BUDDY                       198.999.989.84  00:00:48  00:00:41
```

The following is sample output from the **show dbconn connection** command for a specified connection:

```
Router> show dbconn connection 6127D34C
               connection id: 6127D34C
            connection state: active
                      server: BUDDY
                     rdbname: DB2510
                      userid: (none)
                 client name:
            local ip-address: 198.147.235.2
                  local port: 500
           client ip-address: 198.999.989.84
                 client port: 4258
                connect time: 00:53:27
                   idle time: 00:00:04 (client)
  bytes received from client: 30478
    bytes received from host: 318222
                      client: licensed StarSQL
```

Table 4 describes significant fields shown in the display.

Table 4 show dbconn connection Field Descriptions

Field	Description
connection id	Identification number of the connection made by a DRDA client to the CTRC server.
connection state	Status of the connection made by a DRDA client.
server	Name of the CTRC server.
rdbname	Name of the relational database on the IBM system.
userid	Userid of the user connected through a port to the CTRC server.
client name	Name of the client system.
local ip-address	IP address of the CTRC server in the router to which the client connects.
local port	Port in the CTRC server through which the client connects.
client ip-address	IP address of the client connected to the CTRC server.
client port	Port used by the client to connect to the CTRC server.
connect time	Time when connection was made by the client to the CTRC server.
idle time	Amount of time that the active client connection has been idle.
bytes received from client	Number of bytes the router has received from the client via the specified connection.
bytes received from host	Number of bytes the router has received from the host via the specified connection
client	Indicates whether the client connection uses a licensed StarSQL ODBC-DRDA driver or another DRDA driver.

Related Commands

Command	Description
show dbconn license	Displays the status of CTRC licenses for DB2 communications.
show dbconn ports	Displays information about CTRC ports used for DB2 communications.
show dbconn server	Displays information about CTRC servers configured for DB2 communications.

show dbconn license

To display the status of CTRC licenses for DB2 communications, use the **show dbconn license** EXEC command.

show dbconn license

Syntax Description

This command has no arguments or keywords

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

This command produces the same results as the **show txconn license** command because CTRC licenses are shared between DB2 connections and CICS conversations.

Examples

The following is sample output for a CTRC router that is configured to allow up to 1000 connections until January 1, 2005:

```
Router> show dbconn license
CTRC is licensed for 1000 connections, 756 connections in use
 Expires on 1-1-2005.
```

Related Commands

Command	Description
dbconn license	Configures client licenses for CTRC connections to DB2 or CICS.
show txconn license	Displays the status of licenses used for CTRC.
txconn license	Licenses a Cisco router for CTRC communications with CICS or DB2.

show dbconn ports

To display information about ports that CTRC is using for communications to DB2, use the **show dbconn ports** EXEC command.

show dbconn ports

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples

The following is sample output from the **show dbconn ports** command:

```
Router> show dbconn ports

Port  State
446   listening
447   listening
```

Table 5 describes significant fields shown in the display.

Table 5 show dbconn ports Field Descriptions

Field	Description
Port	Port number.
State	Listening or disabled status.

Related Commands

Command	Description
show dbconn connection	Displays the status of CTRC connections to DB2.
show dbconn license	Displays the status of CTRC licenses for DB2 communications.
show dbconn server	Displays information about CTRC servers configured for DB2 communications.

show dbconn server

To display information about CTRC servers configured for DB2 communications, use the **show dbconn server** EXEC command.

show dbconn server [*server-name*]

Syntax Description

server-name	(Optional) Specific server for which information should be displayed. When omitted, this command displays information for all CTRC servers configured for DB2 communications on the current router.

Defaults

If no server name is specified, this command displays information for all CTRC servers configured for DB2 communications on the current router.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples

The following is sample output from the **show dbconn server** command:

```
Router> show dbconn server
Server      Port   IPAddress       RDBName     State     NumConn
SERVERA     446    0.0.0.0         MATTY       enabled   56
SERVERB     446    0.0.0.0         SCU_DSNM    enabled   24
SERVERC     446    0.0.0.0         DSN4        enabled   19
SERVERD     446    0.0.0.0         MKTG        enabled   130
SERVERE     446    0.0.0.0         ABBY        enabled   76
SERVERF     446    0.0.0.0         DB2510      enabled   320
SERVERG     446    0.0.0.0         ELLE        enabled   3
SERVERH     446    0.0.0.0         SUNSET      enabled   0
SERVERI     446    0.0.0.0         NELL        enabled   1
SERVERJ     446    198.989.999.32  SAMPLE      enabled   12
SERVERK     446    0.0.0.0         DB2410      enabled   154
SERVERL     446    0.0.0.0         SQLDS       enabled   50
SERVERM     446    0.0.0.0         STELLA     disabled   0
SERVERN     446    10.10.19.4      OAK         enabled   2
SERVERO     447    0.0.0.0         DB2510      enabled   237
BUDDY       446    0.0.0.0         DB2510      enabled   756
```

The following is sample output from the **show dbconn server** command where the server BUDDY is specified:

```
Router> show dbconn server BUDDY
                server: BUDDY
          server state: enabled (accepting connections)
            ip-address: 0.0.0.0
                  port: 446
               rdbname: DB2510
       connection type: SNA
                   rlu: STARW.DSNV510
                  mode: IBMRDB
                tpname: \x076DB
          idle-timeout: 0 (none)
           window-size: 4096 bytes
  database server name: (unknown)
   database product id: (unknown)
                   PEM: not configured
 number of connections: 0
           RDB server: active
                   WLM: inactive-enabled
```

Table 6 describes significant fields shown in the display.

Table 6 show dbconn server Field Descriptions

Field	Description
server	CTRC server name.
server state	Current state of the server (enabled or disabled).
ip-address	IP address of the CTRC server in the router to which the client connects.
port	Port number through which the CTRC server accepts a client connection.
rdbname	Name of the remote database accessed by the CTRC server.
connection type	Indicates whether the type of connection between the CTRC router and the DB2 host is via SNA or TCPIP.
rlu	Remote SNA LU used when connecting to the database server.
mode	SNA mode used when connecting to the database.
tpname	SNA transaction program name used for DRDA server on the database system.
idle-timeout	Maximum length of time allowed for inactive connections to the CTRC server.
window-size	TCP receive window size.
database server name	System name returned by the database server. Field shows *none* until first contact.
database product id	Database product ID. Field shows *none* until first contact.
PEM rlu	The host remote LU name the server will connect to when performing password management.
PEM mode	The APPC mode the server will use when performing password management.
PEM tpname	The name of the PEM transaction program on the host (the APPC Signon transaction program, an architected APPC TP).
number of connections	Number of all ODBC clients currently connected to the CTRC server.

Table 6 show dbconn server Field Descriptions (continued)

Field	Description
RDB server	Indicates whether the host database status is active or unreachable.
wlm	Indicates whether the Workload Manager status is not enabled, inactive-enabled, or active-enabled.

Related Commands

Command	Description
show dbconn connection	Displays the status of CTRC connections to DB2.
show dbconn ports	Displays information about CTRC ports used for DB2 communications.

show dbconn statistic

To display all CTRC statistics concerning communications with DB2, use the **show dbconn statistic** privileged EXEC command.

show dbconn statistic [**kind** {**histogram** | **summary**}] **name** {**chains** | **clientturnaround** | **connectionsdown** | **connectionsup** | **dump** | **hostreceived** | **hostresponse** | **hostsent** | **latency** | **maxconnections**}

Syntax Description

kind {**histogram** | **summary**}	(Optional) Desired format for the statistics to be displayed. Valid values are: • **histogram** displays the named statistic in a graphical format. You cannot use the histogram format when displaying all the statistics (in conjunction with the **name dump** parameter). • **summary** displays the named statistic in a tabular format. If you do not specify the **kind** parameter, the statistics are displayed in **summary** format (tabular). See the Usage Guidelines for a description of time periods in the summary statistics.
name {**chains** | **clientturnaround** | **connectionsdown** | **connectionsup** | **dump** | **hostreceived** | **hostresponse**| **hostsent** | **latency** | **maxconnections**}	The statistics you can display with the **name** keyword are: • **chains** displays statistics for number of chains created. • **clientturnaround** displays statistics for average time from receiving a DB2 client communication to sending that client a response. • **connectionsdown** displays the number of connections completed between CTRC and DB2 during the indicated time period. • **connectionsup** displays the number of connections created between CTRC and DB2 during the indicated time period. • **dump** displays a compact statistics summary, in tabular format, for the last 24 hours. The statistics dump includes all the individual statistics you can specify with the **name** keyword. • **hostreceived** displays the total number of bytes the router has received from DB2 hosts during the indicated time period. • **hostresponse** displays the average host response time in seconds for DB2 connections during the indicated time period. • **hostsent** displays the total number of bytes the router has sent to DB2 hosts during the indicated time period. • **latency** displays the average amount of time in seconds used by the txconn server per CICS client request (clientturnaround minus hostresponse). • **maxconnections** displays the maximum number of concurrent connections to CICS clients established during the indicated time period.

- **maxtransactions** displays the maximum number of concurrent CICS transactions during the indicated time period.
- **totalconnections** displays the total number of connections to CICS clients used during the indicated time period.
- **totaltransactions** displays the total number of CICS transactions processed during the indicated time period.

Defaults

No default behavior 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.

Usage Guidelines

Summary statistics are displayed by time period, where:

- [24] indicates statistics for the hour currently in progress.
- [00] through [23] indicate statistics for the preceding 24 hours, with [00] always corresponding to the last midnight-to-1 a.m. period and [23] always corresponding to the last 11 p.m.-to-midnight period, regardless of the current time.
- At the top of each hour, the statistics for the current period are moved from [24] to the appropriate period, [00] through [23], and [24] is reset to 0.

In the following example, at 3 a.m. the statistics for the current period are moved to [02], overwriting the old statistics for that period, and [24] is reset to 0:

At 2:59 a.m.:

```
                          [24]=228
[00]=217     [01]=352     [02]=209     [03]=313     [04]=156     . . .
Mid-1 am     1-2 a.m.     2-3 a.m.     3-4 a.m.     4-5 a.m.     . . .
02-24-2001   02-24-2001   02-24-2001   02-23-2001   02-23-2001   . . .
```

At 3 a.m.:

```
                                       [24]=0
[00]=217     [01]=352     [02]=228     [03]=313     [04]=156     . . .
Mid-1 am     1-2 a.m.     2-3 a.m.     3-4 a.m.     4-5 a.m.     . . .
02-24-2001   02-24-2001   02-24-2001   02-24-2001   02-23-2001   . . .
```

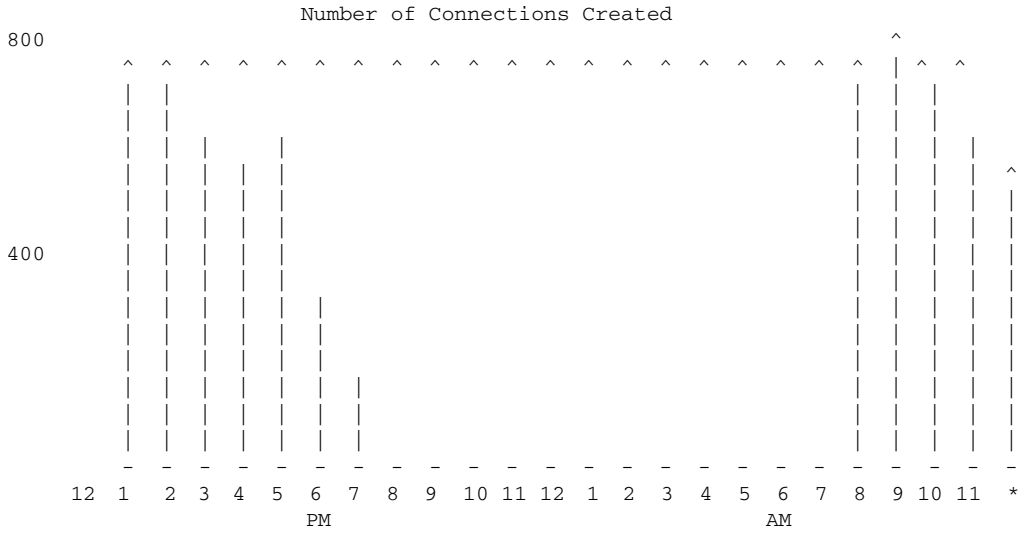
Examples

The following command displays all the statistics relating to communications with DB2:

```
Router# show dbconn statistic name dump
```

The following example shows the **connectionsup** statistic in histogram format.

```
Router# show dbconn statistic kind histogram name connectionsup
```



The following example shows the **connectionsup** statistic in the default summary format.

```
Router# show dbconn statistic name connectionsup
Number of Connections Created
               yesterday       today         today
----hour---    ----PM----    ----AM----    ----PM----

12:00-12:59            0             0         536 *
01:00-01:59          726             0
02:00-02:59          718             0
03:00-03:59          597             0
04:00-04:59          549             0
05:00-05:59          607             0
06:00-06:59          298             0
07:00-07:59          162             5
08:00-08:59            3           704
09:00-09:59            0           817
10:00-10:59            0           725
11:00-11:59            0           598

24-hour total: 5636  (excludes hour in progress *)
```

Related Commands

Command	Description
clear dbconn statistic	Clears statistics related to CTRC communications with DB2.

show dbconn wlm

To display information about a CTRC server that is configured to use Workload Manager for DB2 communications, use the **show dbconn wlm** EXEC command.

show dbconn wlm *server-name*

Syntax Description

server-name	Name of the CTRC server that is configured to use Workload Manager to manage DB2 communications.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Examples

Following is sample output from the **show dbconn wlm** command for a TCP/IP-enabled DB2 server:

```
IP              Port     Weight  Hits
198.147.235.2   500       251     90
198.147.235.2   501       182     64
198.147.235.2   502        29      0
```

Following is sample output from the **show dbconn wlm** command for a DB2 server in an SNA network:

```
RLU              Weight  Hits
STARW.DSNV510     500     230
```

As each connection is established with DB2, CTRC obtains information from the Workload Manager subsystem to calculate the best route to use for the next connection. The fastest and most available connection is assigned the highest weight, and the Hits column shows how many times CTRC has used that route.

Related Commands

Command	Description
show dbconn connection	Displays the status of CTRC connections to DB2.
show dbconn ports	Displays information about CTRC ports used for DB2 communications.

show txconn connection

To display a list of all of the router's CTRC connections to CICS clients, a list of a specified CTRC server's connections to CICS clients, or detailed status information for a specific CTRC connection to a CICS client, use the **show txconn connection** EXEC command.

show txconn connection [*connection-id* | **server** *server-name*]

Syntax Description

connection-id	(Optional) Specifies a CTRC connection to a CICS client for which to display detailed status information.
server *server-name*	(Optional) Specifies a CTRC server for which to list connections to CICS clients.

Defaults

If neither *connection-id* nor *server-name* are specified, a list of all of the current router's CTRC connections to CICS clients is displayed.

Command Modes

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.

Examples

The following example displays information about a CICS client connections for the current router:

```
Router> show txconn connection

Server           ConnID     State     #Transact. IP Address      Port  Bytes
---------------- ---------- --------- ---------- --------------- ----- --------
CICSB            6241464C   receiving 20         198.147.235.88  1365  2.89K
AMELIA           625443BC   receiving 0          198.147.235.88  1371  15.60K
```

The following example displays information about a specified CICS client connection:

```
Router> show txconn connection 6241464C
connection: 6241464C
server: CICSB
state: receiving
transactions: 2
ip address: 198.147.235.88
port: 1365
total transactions: 20
connect timestamp: 06:04:26
idle time: 06:17:34
total bytes received: 2963
total bytes sent: 28121 (2.89K)
idle timeout: 0 (none)
```

Table 7 describes significant fields shown in the display.

Table 7 show txconn connection Field Descriptions

Field	Description
connection	Unique identifier for the CICS client connection.
server	CTRC txconn server process that is handling the connection.
state	Status of the connection. Possible values are: • **closing** indicates that the connection is in the process of closing. • **halt** indicates that the connection has been manually cleared and is in the process of releasing resources. • **receiving** indicates that the connection is receiving data from the client. • **reset** indicates that the connection has just opened or just closed.
transaction	Number of CICS transactions currently in progress for the connection.
ip address	IP address of the CICS client that is using the connection.
port	Port of the CICS client that is using the connection.
total transactions	Total number of CICS transactions performed using the connection.
connect timestamp	Amount of time elapsed since the connection was first established. Values of less than 24 hours are displayed in hours, minutes, and seconds. Longer periods are displayed in days and hours.
idle time	Amount of time that the connection has been idle.
total bytes received	Number of bytes received from the CICS client via this connection.
total bytes sent	Number of bytes sent to the CICS client via this connection.
idle timeout	Number of minutes after which the connection will be automatically closed if there is no activity. A value of zero (0) indicates that the connection will not be closed for lack of activity.

Related Commands

Command	Description
clear txconn connection	Clears a CTRC connection to a CICS client, and all associated transactions.
show txconn transaction	Displays a list of all the CTRC transactions of the current router with CICS, transactions of a specified CTRC server, or transactions of a specified CICS client connection.

show txconn destination

To display a list of all of the current router's CICS destinations for CTRC, or to display detailed status information for a specified CTRC CICS destination, use the **show txconn destination** EXEC command.

show txconn destination [*destination-name*]

Syntax Description

destination-name	(Optional) CTRC destination for which to display detailed status information. A destination is defined by a unique remote LU and mode pair.

Defaults

If *destination-name* is omitted, a list of all CTRC destinations for the current router is displayed.

Command Modes

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.

Examples

The following examples show the CTRC destinations for CICS communications that are available on the current router and information specifically about the destination GEN:

```
Router> show txconn destination
Name              Remote LU          Mode        Hits
----------------- ------------------ ----------- --------
CICSB             CICSB              IBMRDB      31
GEN               CICSB              IBMRDB      50
                  CICSC              IBMRDB      51
GUAVA             GUAVA              IBMRDB      0
CICSC             CICSC              IBMRDB      7

Router> show txconn destination GEN
Name              Remote LU          Mode        Hits
----------------- ------------------ ----------- --------
GEN               CICSB              IBMRDB      50
                  CICSC              IBMRDB      51
```

The HITS column displays the number of times the router has routed transactions or pings to each destination since the last time the router was started up.

Related Commands

Command	Description
txconn destination	Configures CICS destinations for CTRC.

show txconn license

To show the status of licenses used for CTRC, use the **show txconn license** EXEC command.

show txconn license

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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.

Usage Guidelines

This command produces the same result as the **show dbconn license** command because CTRC licenses are shared between DB2 connections and CICS conversations.

Examples

The following is sample output for a CTRC router that is licensed to allow up to 4990 connections for an unlimited time period:

```
Router> show txconn license
CTRC is licensed for 4990 connections, 2850 licensed connections in use
 This is a permanent license
```

Related Commands

Command	Description
dbconn license	Configures CTRC licenses for connections to DB2 or CICS.
show dbconn license	Displays the status of CTRC licenses for DB2 communications.
txconn license	Configures CTRC licenses for connections to CICS or DB2.

show txconn route

To display a list of all CTRC routes defined for specified CICS transaction IDs, or to display a particular CTRC server's routes to CICS, use the **show txconn route** EXEC command.

show txconn route [**server** *server-name*]

Syntax Description

server *server-name*	(Optional) Server for which you wish to display routing information. If not specified, a list of all CICS communications routes for CTRC servers on the current router is displayed.

Defaults

If a value for the *server-name* argument is not specified, a list of all CICS communications routes for CTRC servers on the current router is displayed.

Command Modes

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.

Examples

The following examples show information about all the CTRC routes to CICS that are available on the current router and information about the route for CTRC server **CICSB&C**. A **<default>** entry in the SERVER column indicates a global route that is used by all txconn servers on the router. A **<default>** entry in the TranID column indicates the default route for the listed txconn server.

```
Router> show txconn route
Server             TranID             Destination
------------------ ------------------ ----------------
CICSC              <default>          CICSC
CICSB              <default>          CICSB
CICSB&C            <default>          GEN
GUAVA              <default>          GUAVA
<default>          CPMI               CICSC
CICSB              CPMI               CICSB

Router> show txconn route CICSB&C
Server             TranID             Destination
------------------ ------------------ ----------------
CICSB&C            <default>          GEN
```

Related Commands

Command	Description
txconn route	Configures CTRC routes to CICS for specified transaction IDs.

show txconn server

To display information about the current router's CTRC servers for CICS communications, or to display detailed status information for a single CTRC server, use the **show txconn server** EXEC command.

show txconn server [*server-name*]

Syntax Description

server-name	(Optional) CTRC server for which to display detailed status information. When omitted, a list of CTRC servers is displayed.

Defaults

When a value for the *server-name* argument is not specified, a list of the current router's CTRC servers that communicate with CICS is displayed.

Command Modes

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.

Examples

The following example shows summary information about the CTRC servers for CICS communications that are available on the current router:

```
Router> show txconn server
Server    Port  IP Address   Dest       State    NumConn
--------- ----- ------------ ---------- -------- -------
AMELIA    1436  0.0.0.0      AMELIA     enabled  0
CICSB     1444  0.0.0.0      CICSB      enabled  0
CICSC     1434  0.0.0.0      CICSC      enabled  0
TEST      1446  0.0.0.0      CICSC      enabled  0
```

You can specify the name of a particular txconn server to display detailed information about it, as shown in the following example for the CTRC server named CICSB.

```
Router> show txconn server CICSB
                server: CICSB
           destination: CICSB
          server state: enabled (accepting connections)
            ip address: 0.0.0.0
                  port: 1444
        client timeout: 0 (none)
          host timeout: 1 minute
           window size: 4096 bytes
     fold program name: on
                 ccsid: 273
 number of connections: 178
number of transactions: 20
           client type: cics
```

If this example had been for a Microsoft COMTI client, the client type value would be **comti** rather than **cics**. Table 8 describes the significant information shown for each server, in the order it appears.

Table 8 show txconn server Field Descriptions

Field	Description
server	Name of the txconn server.
destination	Default destination for the server.
server state	Status of the server process. Possible values are: • **disabled (unable to accept connections)** indicates that CICS client connections will be rejected. • **enabled (accepting connections)** indicates that the server is ready to accept connections from CICS clients.
ip address	TCP/IP address for which the server accepts connections. A value of 0.0.0.0 indicates that the server accepts connections for any IP address that is configured on the router.
port	TCP/IP port number on which the server listens.
client timeout	Number of minutes a CICS client can remain idle before it is automatically disconnected. A value of zero (0) indicates that the server does not disconnect clients for inactivity.
host timeout	Number of minutes a CICS host may remain idle before it is automatically disconnected. A value of zero (0) indicates that the server does not disconnect hosts for inactivity.
window size	TCP/IP receive window size.
fold	CTRC folds the CICS program name to upper case. Options are off or on. Default is on.
ccsid	The Coded Character Set Identifier.
number of connections	Number of currently active CICS client connections to the server.
number of transactions	Number of currently active CICS transactions being handled by the server.
client type	Shows whether the server provides connectivity for Microsoft COMTI clients or for IBM CICS Universal Client or TXSeries clients.

Related Commands

Command	Description
show txconn destination	Displays the CICS destinations configured for the current CTRC router.
show txconn route	Displays the CTRC routes defined for specific CICS transaction IDs.
txconn server	Configures CTRC servers for CICS communications.

show txconn statistic

To display information about the current router's CTRC communications with CICS, use the **show txconn statistic** EXEC command.

show txconn statistic [**kind** {**histogram** | **summary**}] **name** {**activeconnections** | **activetransactions** | **allocatetime** | **clientreceived** | **clientsent** | **clientturnaround** | **dump** | **hostreceived** | **hostresponse** | **hostsent** | **latency** | **maxconnections** | **maxtransactions** | **totalconnections** | **totaltransactions**}

Syntax Description

kind {**histogram** | **summary**}	(Optional) Desired format for the statistics to be displayed. Valid values are: • **histogram** displays the named statistic in a graphical format. You cannot use the histogram format when displaying all the statistics (in other words, in conjunction with the **name dump** parameter). • **summary** displays the named statistic in a tabular format. If you do not specify the **kind** parameter, the statistics are displayed in **summary** format (tabular). See the Usage Guidelines for a description of time periods in the summary statistics.
name {**activeconnections** | **activetransactions** | **allocatetime** | **clientreceived** | **clientsent** | **clientturnaround** | **dump** | **hostreceived** | **hostresponse** | **hostsent** | **latency** | **maxconnections** | **maxtransactions** | **totalconnections** | **totaltransactions**}	Specific statistic to display. Valid values are: • **activeconnections** displays the number of connections to CICS clients currently active. • **activetransactions** displays the number of CICS transactions currently being processed. • **allocatetime** displays the average time in seconds spent waiting for APPC allocate operation to complete. • **clientreceived** displays the total number of bytes received from CICS clients during the indicated time period. • **clientsent** displays the total number of bytes sent to CICS clients during the indicated time period. • **clientturnaround** displays the average time in seconds from receiving a request from a CICS client to sending that client a response during the indicated time period. • **dump** displays a compact statistics summary, in tabular format, for the last 24 hours. The statistics include all the individual statistics you can specify with the **name** parameter except the activeconnections and activetransactions data. • **hostreceived** displays the total number of bytes received from hosts for CICS connections during the indicated time period. • **hostresponse** displays the average host response time in seconds for CICS connections during the indicated time period. • **hostsent** displays the total number of bytes sent to hosts for CICS connections during the indicated time period.

- **latency** displays the average amount of time in seconds used by the txconn server per CICS client request (**clientturnaround** minus **hostresponse**).
- **maxconnections** displays the maximum number of concurrent connections to CICS clients during the indicated time period.
- **maxtransactions** displays the maximum number of concurrent CICS transactions during the indicated time period.
- **totalconnections** displays the total number of connections to CICS clients used during the indicated time period.
- **totaltransactions** displays the total number of CICS transactions processed during the indicated time period.

Defaults

If the kind of statistics display is not specified, **summary** is used.

Command Modes

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.

Usage Guidelines

Summary statistics are displayed by time period, where:

- [24] indicates statistics for the hour currently in progress.
- [00] through [23] indicate statistics for the preceding 24 hours, with [00] always corresponding to the last midnight-to-1 a.m. period and [23] always corresponding to the last 11 p.m.-to-midnight period, regardless of the current time.
- At the top of each hour, the statistics for the current period are moved from [24] to the appropriate period, [00] through [23], and [24] is reset to 0.

In the following example, at 3 a.m. the statistics for the current period are moved to [02], overwriting the old statistics for that period, and [24] is reset to 0:

At 2:59 a.m.:

```
                        [24]=228
[00]=217     [01]=352   [02]=209    [03]=313    [04]=156     . . .
Mid-1 am     1-2 a.m.   2-3 a.m.    3-4 a.m.    4-5 a.m.     . . .
02-24-2001   02-24-2001 02-24-2001  02-23-2001  02-23-2001   . . .
```

At 3 a.m.:

```
                                        [24]=0
[00]=217     [01]=352     [02]=228     [03]=313     [04]=156     . . .
Mid-1 am     1-2 a.m.     2-3 a.m.     3-4 a.m.     4-5 a.m.     . . .
02-24-2001   02-24-2001   02-24-2001   02-24-2001   02-23-2001   . . .
```

Examples

The following examples show histogram and summary displays of the **clientreceived** statistic.

```
Router> show txconn statistic kind histogram name clientreceived
                    Number of Bytes Received from Clients
18.82MB                                                ^
          ^  ^  ^  ^  ^  ^  ^  ^  ^  ^  ^  |  ^  ^  ^  ^  ^  ^  ^  ^  ^  ^  ^
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
9.41MB    |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  ^
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
          |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
0         -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
      7  8  9 10 11 12  1  2  3  4  5  6  7  8  9 10 11 12  1  2  3  4  5  6  *
                                       PM                                    AM

Router> show txconn statistic name clientreceived
Number of Bytes Received from Clients

               yesterday     yesterday       today
----hour---    ----AM----    ----PM----    ----AM----

12:00-12:59                   19728481      19727299
01:00-01:59                   19732711      19727299
02:00-02:59                   19722903      19727382
03:00-03:59                   19728398      19731695
04:00-04:59                   19729497      19726200
05:00-05:59                   19730596      19733893
06:00-06:59                   19722986      19708616
07:00-07:59             0     19734992       8736034 *
08:00-08:59      19726283     19725101
09:00-09:59      19725101     19728398
10:00-10:59      19726283     19727382
11:00-11:59      19729497     19730596

24-hour total: 453731589 (excludes hour in progress *)
```

Related Commands

Command	Description
show txconn connection	Displays a list of all of the CTRC connections of the router to CICS clients.
show txconn destination	Displays a list of all of the CICS destinations of the current router for CTRC, or displays detailed status information for a specified CTRC CICS destination.
show txconn license	Displays the status of licenses used for CTRC.
show txconn route	Displays a list of all CTRC routes defined for specified CICS transaction IDs, or displays the server routes of a particular CTRC server to CICS.
show txconn server	Displays information about CTRC servers that communicate with CICS.
show txconn transaction	Displays a list of all the CTRC transactions of the current router with CICS, transactions of a specified CTRC server, or transactions of a specified CICS client connection.

show txconn transaction

To display a list of all the current router's CTRC transactions with CICS, a specified CTRC server's transactions, or a specified CICS client connection's transactions, use the **show txconn transaction** EXEC command.

show txconn transaction [**server** *server-name* | **connection** *connection-id* | *transaction-id*]

Syntax Description

server *server-name*	(Optional) Specifies a CTRC server for which to display a list of transactions.
connection *connection-id*	(Optional) Specifies a CICS client connection to CTRC for which to display a list of transactions.
transaction-id	(Optional) Specifies an individual transaction for which to display detailed status information.

Defaults

If no arguments are specified, all the CICS transactions for the current router are listed.

Command Modes

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.

Examples

The following example shows information about all the CICS transactions being handled by the current router:

```
Router> show txconn transaction

Transaction ID Server     Conn ID    State     TP Name  User ID
-------------- ---------- ---------- --------- -------- --------
6246ECD8       CICSB      62494598   receiving CPMI     QAUSER
62476188       CICSB      62494598   receiving CPMI     QAUSER
623130D4       CICSB      62494598   receiving CPMI     QAUSER
6229E88C       CICSB      62494598   receiving CPMI     QAUSER
```

You can specify a particular transaction ID to display details about it, as shown in the following example:

```
Router> show txconn transaction 6246ECD8
                   transaction: 6246ECD8
                        server: CICSB
                 connection id: 62494598
                         state: receiving
                       tp name: CPMI
                       user id:
  session RU address (OAF+DAF): 6
                     idle time: 1788
--- Transaction Totals ---
number of transactions executed: 1
number of bytes received from client: 1099
number of bytes received from host: 0
```

Table 9 describes the significant information shown for each transaction in the order it appears in the display.

Table 9 show txconn transaction Field Descriptions

Field	Description
transaction	Unique identifier for the transaction.
server	CTRC txconn server process that is handling the transaction.
connection id	Unique identifier for the CICS client connection associated with the transaction.
state	Status of the transaction. Possible values are: • **closing** indicates that the SNA session is in the process of closing. • **exception** indicates that an error has occurred. An error indication will be sent to the client and the host session will be terminated. • **exc. resp.** indicates that the router has sent an error indication to the client. • **opening** indicates that the SNA session is about to open. • **parsing FMH** indicates that the SNA session has received the first portion of an FM header. • **parsing FMH5** indicates that CTRC is about to establish a SNA session with the host. • **parsing FMH7** indicates that the router just received an error from the CICS client. • **parsing DFC** indicates that the SNA session is about to close. • **receiving** indicates that the SNA session is receiving data from the host. • **reset** indicates that the SNA session is idle, waiting for a new transaction request from the CICS client. • **sending** indicates that the SNA session is sending data to the host. • **waiting** indicates that the SNA session is waiting for data from the client.
tp name	CICS transaction program name.
user id	CICS user ID associated with the transaction.
session RU address	SNA architected address that allows multiple sessions to share one connection.

Table 9 show txconn transaction Field Descriptions (continued)

Field	Description
idle time	Time in milliseconds that the SNA session has been idle.
number of transactions executed	Number of CICS transactions executed by the current SNA session.
number of bytes received from client	Number of bytes received from the CICS client during the current SNA session.
number of bytes received from host	Number of bytes received from the CICS host during the current SNA session.

Related Commands

Command	Description
show txconn connection	Displays a list of all of the CTRC connections of the router to CICS clients.
show txconn destination	Displays a list of all of the CICS destinations of the current router for CTRC, or displays detailed status information for a specified CTRC CICS destination.
show txconn server	Displays information about CTRC servers that communicate with CICS.

txconn destination

To configure a CTRC destination, use the **txconn destination** global configuration command. To remove the configuration for a txconn destination, use the **no** form of this command.

txconn destination *destination-name* **rlu** *rlu-name* **mode** *mode-name*

no txconn destination *destination-name*

Syntax Description

destination-name	Name of the destination being defined or added to. This name is used in the route configuration command to identify the destination for the route. If the destination does not exist, it is created; if it exists, the **rlu** and **mode** parameters are added as an additional routing target for this destination. When a destination contains multiple routing targets, it is like configuring a cluster where the various targets are chosen on a round-robin basis for load balancing.
rlu *rlu-name*	Remote LU name on the host. This parameter defines to which remote LU the server will connect when using this destination. A remote LU corresponds directly to a CICS region. The value you enter here should match your VTAM APPLID.
mode *mode-name*	Name of the APPC mode. This parameter defines which mode the server will use for its APPC connections when using this destination. If the mode you specify does not already exist, CTRC will create it.

Defaults

No defaults exist for the **txconn destination** command. However, the remote LU name of the host and the APPC mode name are optional for the **no** form of the command. If you omit them, CTRC removes the configuration for all routing targets defined for the destination. If you use **rlu** *rlu-name* **mode** *mode-name* to specify a particular routing target within a destination that has multiple targets, the configuration is removed only for the specified target.

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.

Examples

The following example shows the CTRC destination newdest being defined on the current router:

```
txconn destination newdest rlu CICSB mode IBMRDB
```

A second pair of rlu and mode values could be assigned to this same logical destination, to allow load sharing between the two destination CICS systems:

```
txconn destination newdest rlu CICSC mode IBMRDB
```

Related Commands

Command	Description
show snasw mode	Displays the SNASw modes.
show txconn destination	Displays a list of all of the CICS destinations of the current router for CTRC, or displays detailed status information for a specified CTRC CICS destination.

txconn license

To license a Cisco router for CTRC communications with CICS or DB2, use the **txconn license** global configuration command. To remove the license, use the **no** form of this command.

txconn license *license-key* **connections** *licensed-connections* **expiration-date** *yyyymmdd*

no txconn license

Syntax Description

license-key	License key obtained from your Cisco representative. The license key is a 32-character hexadecimal string that specifies the maximum number of CICS conversations or DB2 connections allowed for the CTRC router. The license key is generated for a specific router, and is based on the SNA Switching Services cpname for the router. Use the **show config | include cpname** command to view the cpname so you can provide it when you request the license key.
connections *licensed-connections*	Number of licensed connections. If the license is for an unlimited number of connections, omit the **connections** parameter.
expiration-date *yyyymmdd*	Date when a temporary license key expires, where *yyyy* is the year expressed in four digits, *mm* is the month expressed in two digits, and *dd* is the date expressed in two digits. If the license is for an unlimited time period (permanent license), omit the **expiration-date** parameter.

Defaults

If the number of licensed connections is not specified, the license key must allow an unlimited number of licensed connections. If the expiration date is not specified, the license key must be for a permanent license.

Command Modes

Global configuration

Command History

Release	Modification
11.3(2)T	This command was introduced.
12.0(5)XN	Command moved from CDBC feature to CTRC feature.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

Licenses are required for all CTRC installations. For testing and evaluation purposes, unlicensed CTRC installations allow you to establish two connections to DB2, or two conversations to CICS, or one to each. One license key is used for both CICS and DB2 communications, so you can use either the **dbconn license** command or the **txconn license** command to configure the CTRC router.

Examples

The following example shows the configuration of a CTRC router with a license that allows up to 4000 connections until January 1, 2005:

```
txconn license 3C09A051320BAF020BFF45B3A2FF21D2 connections 4000 expiration-date 20050101
```

Related Commands

Command	Description
show dbconn license	Displays the status of CTRC licenses for DB2 communications.
show snasw node	Displays details and statistics of the SNASw operation.
show txconn license	Displays the status of licenses used for CTRC.

txconn ping

To test communications between the CTRC router and a CTRC destination (a host defined by a pair of RLU and mode values), use the **txconn ping** EXEC command.

txconn ping *destination-name*

Syntax Description

destination-name	Specifies the CICS system for which to test communications.

Defaults

No default behavior or values.

Command Modes

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.

Usage Guidelines

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

Examples

The following example shows communications being tested between the current router and the CTRC destination GEN. Note that GEN is a destination that has two RLU-Mode pairs defined, and that the **txconn ping** command automatically tests connections to both:

```
txconn ping GEN
Trying GEN CICSC:IBMRDB
Destination GEN successfully contacted!
Elapsed time was 00:00:01.001
Trying GEN CICSB:IBMRDB
Destination GEN successfully contacted!
Elapsed time was 00:00:01.001

Elapsed time is noted in hours, minutes, seconds, and milliseconds.
```

Related Commands

Command	Description
ping sna	Initiates an APPC session with a named destination LU to run the APING transaction program to check network integrity and timing characteristics.

txconn route

To configure a CTRC route that will transmit specified transactions to a particular CICS destination, use the **txconn route** global configuration command. To remove the configuration of a CTRC route, use the **no** form of this command.

txconn route [**server** *server-name*] **tranid** *transaction-id* **destination** *destination-name*

no txconn route [**server** *server-name*] **tranid** *transaction-id*

Syntax Description

server *server-name*	(Optional) Name of the CTRC server to which this route applies. If omitted, this route is applied to all CTRC servers on the current router that are configured for communication with CICS.
tranid *transaction-id*	CICS transaction ID (a TP name). When the server processes a transaction that uses this transaction ID, the server routes the transaction using this route entry.
destination *destination-name*	Name of the destination to which the transaction is routed.

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.

Examples

The following example shows a CTRC route to destination GEN being defined on the current router for transaction ID PNG1:

```
txconn route server newsvr tranid PNG1 destination GEN
```

Related Commands

Command	Description
show txconn route	Displays a list of all CTRC routes defined for specified CICS transaction IDs, or displays the server routes of a particular CTRC server to CICS.

txconn server

To configure a CTRC server for communications with CICS, use the **txconn server** global configuration command. To disable a CTRC server, use the **no** form of this command.

txconn server *server-name* **destination** *destination-name* [**access** {**cics** | **comti**}] [**ccsid** *number*] [**client-timeout** *minutes*] [**fold** {**on** | **off**}] [**host-timeout** *minutes*] [**ipaddress** *ip-address*] [**keepalive attempts** *number*] [**keepalive interval** *seconds*] [**port** *port-number*] [**target** {**cics** | **ims-tm**}] [**window-size** *bytes*]

no txconn server *server-name*

Syntax Description

server-name	Name of the server being defined. This name is used in other commands to identify the server being administered.
destination *destination-name*	Name of the server's default destination. Any transactions whose *tranid* is not associated with a particular route will be routed to this destination. The destination must already be defined when configuring the server.
access {**cics** | **comti**}	(Optional) Indicates whether *server-name* supports IBM CICS (Universal Client or TXSeries) or Microsoft COMTI clients. If this value is not specified, a default of CICS is used.
ccsid *number*	(Optional) The Coded Character Set Identifier. This is used for TXSeries clients.
client-timeout *minutes*	(Optional) Number of minutes of client connection inactivity after which the server decides the client has gone away. When this happens the server closes the client connection. If no client timeout is specified, the default is 0 (zero) for no timeout.
fold {**on** | **off**}	(Optional) Enables/disables the fold program. Default is on. CTRC folds the CICS program name to uppercase.
host-timeout *minutes*	(Optional) Number of minutes of host connection inactivity after which the server decides the host has gone away. When this happens the server closes the host connection. If no host timeout is specified, the default is 0 (zero) for no timeout.
ipaddress *ip-address*	(Optional) TCP/IP network address for which the server accepts connections. If this parameter is omitted, the server accepts connections for any IP address, like a wildcard address. If multiple servers are configured to listen on the same port, they must each specify a different IP address. If a server is configured with the IP address omitted, no other servers may listen on the same port. So, on a given port, you may configure either 1 wildcard IP address server, or *n* address-specific servers, where *n* is 1 or more.
keepalive attempts *number*	(Optional) The number of times for the CTRC server to attempt sending an acknowledgment message to the client to keep the connection alive. You can specify 1 to 100 attempts, or 0 (zero) to disable the keepalive messages. The default is 3 attempts.
keepalive interval *seconds*	(Optional) The frequency for the CTRC server to send an acknowledgment message to the client to keep the connection alive. The interval can be from 1 to 3600 seconds, or 0 (zero) to disable the keepalive messages. The default is 120 seconds.

port *port-number*	(Optional) TCP/IP port number on which the server listens. If no IP address is specified, only one server can listen on a port. Multiple servers can use the same port number if the combination of IP address and port number is unique to each server. If the port number is omitted, the server listens on port 1435.
target {**cics** | **ims-tm**}	(Optional) Indicates whether the host connection is to a CICS or IMS transaction server. The default is cics.
window-size *bytes*	(Optional) Size, in bytes, of the TCP/IP window for incoming CICS client connections. If no window size is specified, the default is 4096 bytes.

Defaults

If the CTRC server's IP address is not configured, the server accepts connections for any IP address that is configured for the router.

If you do not specify a client timeout, CICS client connections can continue regardless of how long they have been idle.

If you do not specify a host timeout, host connections can continue regardless of how long they have been idle.

If you do not specify a keepalive attempt or a keepalive interval, the server makes up to three attempts to send an acknowledgment message every 120 seconds.

If the port number is not configured, the server listens on port 1435.

If you do not specify a target, the server uses a default of cics.

If you do not specify a TCP/IP window size, the default value is 4096 bytes.

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(5)T	This command was enhanced to allow configuration of the keepalive feature.

Usage Guidelines

You can configure more than one CTRC server per router for communications with DB2 or CICS. There is no limit on the number of CTRC servers. However, be sure that CTRC txconn servers and CTRC dbconn servers are configured to use different ports, and that each txconn server is configured to use a unique combination of port number and IP address, or a unique port number with no IP address. Set **keepalive attempts** or **keepalive interval** to zero (0) to disable the keepalive messages.

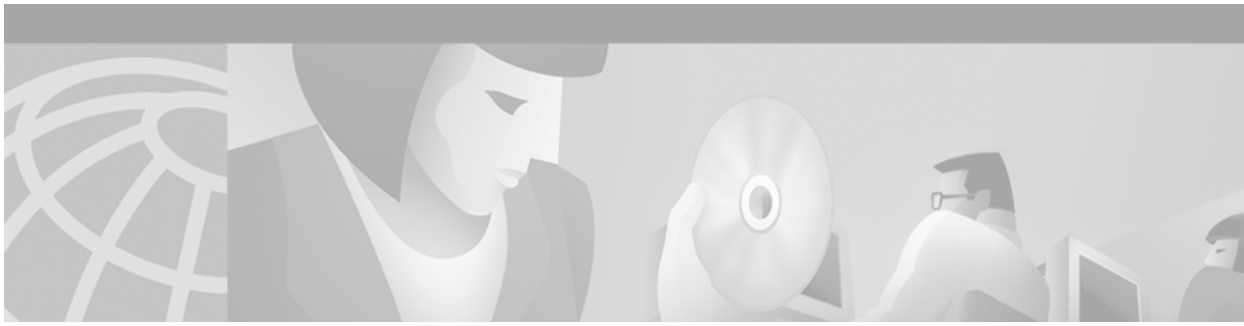
Examples

The following example shows the CTRC server newsvr being defined on the current router with the keepalive feature enabled to attempt five acknowledgment messages every 300 seconds:

```
txconn server newsvr destination GEN keepalive attempts 5 keepalive interval 300 port
1438
```

Related Commands

Command	Description
show txconn destination	Displays a list of all of the CICS destinations of the current router for CTRC, or displays detailed status information for a specified CTRC CICS destination.
show txconn server	Displays information about CTRC servers that communicate with CICS.



Cisco Mainframe Channel Connection Commands

Use the commands in this chapter to configure and monitor the Cisco Mainframe Channel Connection (CMCC) products which include the Channel Interface Processor (CIP) and the Channel Port Adapter (CPA). For commands to configure specific features on a CMCC adapter, see the corresponding chapters in this publication.

For hardware technical descriptions and for information about installing the router interfaces, refer to the hardware installation and maintenance publication for your particular product.

Note Unless otherwise specified, all commands in this chapter are supported on the Cisco 7000 with RSP7000, Cisco 7500 and the Cisco 7200 series routers.

For interface configuration information and examples, refer to the "Configuring Cisco Mainframe Channel Connection Adapters" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

For a conversion table of the modular products and Cisco 7000 family processors, refer to the "Platform Support" appendix of the *Cisco IOS Configuration Fundamentals Command Reference*.

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 adaptor 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.

Defaults

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.

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 router prompt appears as follows:

```
router(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 2000
  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 Channel1/0
 lan TokenRing 20
  source-bridge 310 3 100
  adapter 9 4043.1313.9009 hsma-partner 4043.3333.001a
 lan TokenRing 26
  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 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.

channel-protocol

To define a data rate of either 3 MBps or 4.5 MBps for Parallel Channel Interfaces, use the **channel-protocol** interface configuration command. 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.

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
```

clear extended counters

To clear the extended interface counters associated with CMCC features, use the **clear extended counters** EXEC command.

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 CSNA feature counters.
icmp-stack	(Optional) Clears ICMP stack counters.
ip-stack	(Optional) Clears IP stack counters.
llc2	(Optional) Clears 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 TG counters.
tn3270-server	(Optional) Clears TN3270 Server counters.
udp-stack	(Optional) Clears UDP stack counters.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.

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 successful completion of the command.

These counters will be cleared in the show commands and remain uncleared when obtained through the SNMP interface.

Examples

The following is an example of the command:

```
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.

exception slot

To provide a core dump of a CMCC adapter, use the **exception slot** global configuration command. 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* 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.
host	Name or IP address of the host that receives the core dump information.
filename	Filename on the host that receives the core dump information. The maximum name length is 31 characters. When written to the host, *slot* 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.

Usage Guidelines

This command is only supported 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. An additional 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 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.

interface channel

To specify a channel-attached interface and enter interface configuration mode, use the **interface channel** global configuration command.

interface channel *slot*/*port*

Syntax Description

slot	Slot number where the CMCC adapter is located.
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.

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 CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
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.
lan	Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode.
max-llc2-sessions	Specifies the maximum number of LLC2 sessions supported on the CMCC adapter.

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.
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.

lan

To configure an internal LAN on a CMCC adapter interface and enter the internal LAN configuration mode, use the **lan** interface configuration command. 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 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.

Usage Guidelines

Token Ring is the only type of internal LAN that is supported.

This command is valid only on the virtual channel interface. All internal adapters configured on the internal LAN must be removed first before the internal LAN can be removed.

A CMCC internal LAN can be configured as a SRB LAN. This allows LLC packets to be bridged between the CMCC adapter and IOS, providing a means to link the internal LAN to Cisco IOS SNA features such as SRB, DLSw+, RSRB, SDLLC, QLLC, APPN, and SR/TLB.

An internal LAN can only be configured on a virtual channel interface of a CMCC adapter. You enter the internal LAN configuration mode by issuing the command for an internal LAN that already exists or when you configure an internal LAN for the first time. In the internal LAN configuration mode, the router prompt appears as follows:

```
router (cfg-lan-type n) #
```

In this syntax, *type* is the specified internal LAN type and *n* 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.

max-llc2-sessions

To specify the maximum number of LLC2 sessions supported on the CMCC adapter, use the **max-llc2-sessions** interface configuration command. 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 1 to 6000 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.

Usage Guidelines

This command is configured on the virtual interface of a CIP, and the physical interface of a 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 there is not enough memory currently 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
```

name

To assign a name to the internal adapter, use the **name** internal adapter configuration command. 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 8 characters (not including blanks).

Defaults

No default behavior or values.

Command Modes

Internal adapter configuration

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following example assigns a name to an internal adapter interface:

```
name VTAM_B14
```

Related Commands

Command	Description
adapter	Configures internal adapters.

show controllers channel

To display CPA-specific information, including the currently loaded microcode, use the **show controllers channel** EXEC command.

show controllers channel [*slot*/*port*]

Syntax Description

slot	(Optional) Slot number.
port	(Optional) Interface number.

Command Modes

EXEC

Command History

Release	Modification
11.3T	This command was introduced.

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 extended channel connection-map llc2

To display 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, use the **show extended channel connection-map llc2** privileged EXEC command.

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.

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 icmp-stack

To display information about the Internet Control Message Protocol (ICMP) stack running on the CMCC channel interfaces, use the **show extended channel icmp-stack** EXEC command.

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

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Alias addresses field added to the output.

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 80.11.198.2
  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 80.11.198.3
  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 example shows 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 of 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 10 describes the fields shown in the display.

Table 10 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 ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
InErrors	Number of ICMP messages which 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 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.

show extended channel ip-stack

To display information about the IP stack running on CMCC channel interfaces, use the **show extended channel ip-stack** EXEC command.

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

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Alias addresses field added to the output.

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 80.11.198.2
  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 80.11.198.3
  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 example shows 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 of 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 example shows 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 11 describes the fields shown in the display.

Table 11 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, etc.

Table 11 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 which 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 successfully 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 which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
InDelivers	Total number of input datagrams successfully delivered to IP user-protocols (including 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 which 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 which 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 successfully 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 since 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 successfully 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 11 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-up 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 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.

show extended channel lan

To display the internal LANs and adapters configured on a CMCC adapter, use the **show extended channel lan** EXEC command.

show extended channel *slot/port* **lan** [*tokenring* [*lan-id* [*adapno*]]]

Syntax Description

slot	Slot number.
port	Port number.
tokenring	(Optional) Specify 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

EXEC

Command History

Release	Modification
11.0	This command was introduced.

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 LLC2 sessions running on the CMCC adapter interfaces, use the **show extended channel llc2** EXEC command.

show extended channel *slot*/*port* **llc2** [**admin** | **oper** | **stats**] [*lmac* [*lsap* [*rmac* [*rsap*]]]]

Syntax Description

slot	Slot number.
port	Port number.
admin	(Optional) Shows configured values. This is the default.
oper	(Optional) Shows operational values for: • Internal adapters • SAPs 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 service access point (SAP) address, 0 to 256.
rmac	(Optional) Remote MAC address.
rsap	(Optional) Remote SAP address, 0 to 256.

Command Modes

EXEC

Command History

Release	Modification
11.0(3)	This command was introduced.

Usage Guidelines

The **show extended channel llc2** command is valid on virtual channel interfaces.

To specify LLC information for internal adapters:

- 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:

- 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:

- 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 12 describes the fields shown in the display.

Table 12 show extended channel llc2 admin Field Descriptions—All LLC2 Connections

Field	Description
t1-time	Length of time the CMCC LLC2 link station waits for an acknowledgment to a sent I-frame before polling the remote LLC2 station.
tpf-time	Amount of time the CMCC LLC2 link station waits for a final response to a poll before resending the original poll frame.
trej-time	Amount of time the CMCC LLC2 link station waits for a correct frame after sending a reject command to a remote LLC2 station.
tbusy-time	Amount of time 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.
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.

Table 12 show extended channel llc2 admin Field Descriptions—All LLC2 Connections (continued)

Field	Description
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 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 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 currently 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 stat

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 13 describes the 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 13 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.

Table 13 show extended channel llc2 stats Field Descriptions—all LLC2 Connections (continued)

Field	Description
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, send RNRs 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 14 describes the fields shown in the display.

Table 14 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 15 describes the fields shown in the display. All statistics for SAPs are based on the time the SAP was last opened.

Table 15 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 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.
UIFreamesIn	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/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, 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 a 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, SNMP trap, and a router console message.

Table 15 show extended channel llc2 stats Field Descriptions for Specified Interface (continued)

Field	Description
DMsInABM	Number of times the CMCC LLC2 link station went into disconnect mode after receiving a DM. 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.
SABMEDsInABM	Number of times the CMCC LLC2 link station went into disconnect mode after receiving a 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, 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 16 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 16 show extended channel llc2 Field Descriptions for Internal LAN Adapter

Field	Description
State	• ADM (Asynchronous Disconnect Mode) • setup • conn • normal • busy • reject • await • awaitBusy • 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 the CMCC LLC2 link station waits for an acknowledgment to a sent I-frame before polling the remote LLC2 station.
tpf-time	Amount of time the CMCC LLC2 link station waits for a final response to a poll before resending the original poll frame.
trej-time	Amount of time the CMCC LLC2 link station waits for a correct frame after sending a reject command to a remote LLC2 station.
tbusy-tim	Amount of time 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 amount of time the CMCC LLC2 link station allows received I-frames to remain unacknowledged. The CIP LLC2 connection will acknowledge received I-frames within the ack-delay time.

Table 16 show extended channel llc2 Field Descriptions for Internal LAN Adapter (continued)

Field	Description
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.
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 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 17 describes the fields shown in the display.

Table 17 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 *n* I-frames received from the remote LLC2 station on the CMCC queued to be sent over the channel to VTAM. Where *n* is two times the recv-wind. 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.

Table 17 show extended channel llc2 stats Field Descriptions

Field	Description
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.
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 Nw field description in Table 15 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 LLC2 sessions supported on the CMCC adapter, use the **show extended channel max-llc2-sessions** privileged EXEC command.

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

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 18 describes the fields shown in the display.

Table 18 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**/**no shut**), both the administrative and operational max-llc2-sessions numbers will match.

Table 18 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 failure	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 SAP and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.

show extended channel statistics

To display statistical information about subchannels on the physical interface of a CMCC adapter, use the **show extended channel statistics** EXEC command. 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 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 0x00 to 0xFE. This value is the unit address associated with the control unit number and path as specified in the host IOCP file. For CLAW and offload support, the device address must have an even value.
connected	(Optional) For each backup group, only display information about the active subchannel or the first subchannel defined in the group if none are active.

Command Modes

EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.0(3)T	Support for the CMPC+ feature was added.

Examples

The following is sample output for the **show extended channel statistics** command from a CMCC adapter configured with CLAW, Offload, CSNA, and 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 for the **show extended channel statistics** command from a CMCC adapter configured with CLAW, Offload, CSNA, and CMPC+:

```
tanzania# 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
tanzania#
```

Table 19 describes the fields shown in the display.

Table 19 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 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 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 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 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/Bytes Write	Sum of the bytes in the blocks.
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 *n* times for a given block. See the Memd wait counter.

Table 19 show extended channel statistics Field Descriptions (continued)

Field	Description
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 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 for 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 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 CMCC adapter physical interfaces, use the **show extended channel subchannel** EXEC command. 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

EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.0(3)T	Support for the CMPC+ feature was added.

Examples

The following is sample output from the **show extended channel subchannel connected** command used on a CMCC adapter configured for CLAW, Offload, and 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 20 describes the fields shown in the display.

Table 20 show extended channel subchannel Field Descriptions

Field	Description
Channel*x/y*: 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. • 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 only be set if the LOADED flag is set as well. 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.

Table 20 show extended channel subchannel Field Descriptions (continued)

Field	Description
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 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.
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 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 +/- .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 off-line 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.
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.
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 Transmission Control Protocol (TCP) sockets on a channel interface, use the **show extended channel tcp-connections** EXEC command.

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

EXEC for summary and privileged EXEC for detail.

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Stack address field added to the output.

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 for 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
80.11.198.2     21    0.0.0.0         0      listen             0           0
80.11.198.2     21    172.18.48.194   38668  establish         62         298
80.11.198.2     23    0.0.0.0         0      listen             0           0
80.11.198.2     23    172.18.48.194   38666  establish        124       11966
80.11.198.2     1025  0.0.0.0         0      listen             0           0
80.11.198.2     1025  172.18.48.194   38705  closeWait         24           1
80.11.198.3     7     0.0.0.0         0      listen             0           0
80.11.198.3     9     0.0.0.0         0      listen             0           0
80.11.198.3     19    0.0.0.0         0      listen             0           0
80.11.198.3     21    0.0.0.0         0      listen             0           0
80.11.198.3     23    0.0.0.0         0      listen             0           0
80.11.198.3     23    172.18.48.194   38667  establish         85         446
```

The following example shows 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 channel3/1 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    70.70.5.140     61954  establish         59         105
```

Table 21 describes the fields shown in the display.

Table 21 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 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, an RST segment may be sent from the managed node to the other TCP endpoint (note however that RST segments are not sent reliably).

Table 21 show extended channel tcp-connections Field Descriptions (continued)

Field	Description
In Bytes	Number of bytes sent for this TCP connection. **Note** To support SNMP Version 1 Managers, this variable is supplied as a 32-bit value which can wrap very 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 which can wrap very frequently.

The following is sample output for 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 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.
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 CMCC adapter interfaces, use the **show extended channel tcp-stack** EXEC command.

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

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Alias addresses field added to the output.

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 80.11.198.2
  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 80.11.198.3
  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 example shows 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 example shows 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 22 describes the fields shown in the display.

Table 22 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 22 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 currently established connections.
OutSegs	Total number of segments sent, including those on current connections but excluding those containing only resent octets.
RetransSegs	Total number of segments resent—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 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 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.
show extended channel tcp-connections	Displays information about the TCP sockets on a channel interface.

show extended channel udp-listeners

To display information about the User Datagram Protocol (UDP) listener sockets running on the CMCC adapter interfaces, use the **show extended channel udp-listeners** EXEC command.

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

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

The **show extended channel tn3270-server udp-listeners** command is valid on both physical and virtual channel interfaces.

Examples

The following is sample output from the **show channel udp-listeners** command:

```
Router# show extended channel 0/1 udp-listeners

UDP Listener: IP Address 80.11.198.3        LocalPort 7
UDP Listener: IP Address 80.11.198.3        LocalPort 9
UDP Listener: IP Address 80.11.198.3        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.
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.

show extended channel udp-stack

To display information about the UDP stack running on the CMCC adapter interfaces, use the **show extended channel udp-stack** EXEC command.

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

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Alias addresses field added to the output.

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 udp-stack

rispix#show extended channel 0/1 udp-stack
UDP Statistics for IP Address 80.11.198.2
  InDatagrams : 6            NoPorts     : 6
  InErrors    : 0            OutDatagrams: 0
UDP Statistics for IP Address 80.11.198.3
  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 23 describes the fields shown in the display.

Table 23 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 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.

show interfaces channel

To display information about the CMCC adapter interfaces, use the **show interfaces channel** privileged EXEC command. 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.

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 198.92.1.145, 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 24 describes the fields shown in the display.

Table 24 show interfaces channel Field Descriptions

Field	Description
Channel... is {up | down | administratively down}	Indicates whether the interface hardware is currently 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 | down | administratively down}	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% 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 or not.
keepalive	Indicates whether keepalives are set or not.
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 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 24 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 5 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 no buffer, runts, giants, CRCs, 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 packets received incorrectly having a 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 buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.

Table 24 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, as 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.

shutdown (CMCC)

To shut down an interface or the virtual interface on the CMCC adapter when you are in interface configuration mode, use the **shutdown** CMCC command. The **shutdown** TN3270 server command also shuts down TN3270 entities, such as PU, DLUR, and DLUR SAP, depending on which configuration mode you are 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.

Usage Guidelines

In channel interface configuration mode, the command applies to the entire CMCC adapter.

Examples

The following example issued in interface configuration mode shuts down the entire CMCC adapter:

```
shutdown
```

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** interface configuration command. To disable tracking of the physical interface signal on a Channel Port Adapter 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.

Usage Guidelines

The **state-tracks-signal** command is useful in environments where you are using Hot Standby Router Protocol (HSRP) or 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 ECPA and PCPA are examples of this type of channel interface. The command is not valid for the CIP, which has a separate channel interface for the virtual channel functions.

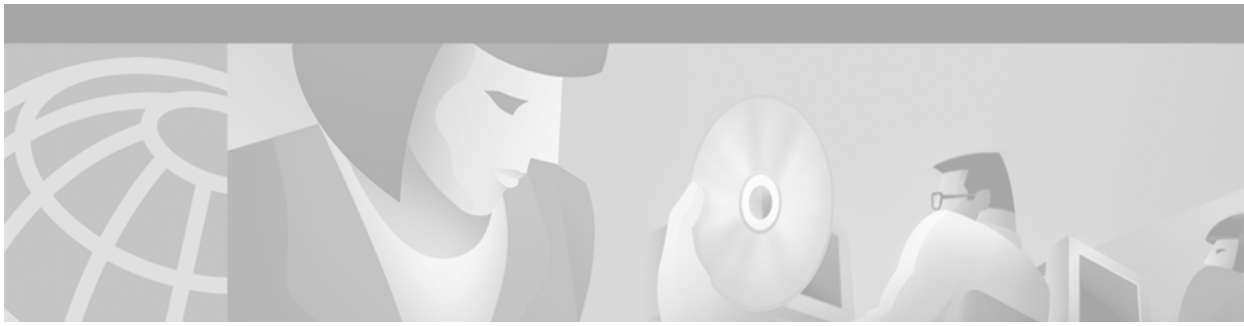
When the **state-tracks-signal** command is used on an interface that is configured for **no shutdown**, then the state of the channel interface is reported according to the status of the physical channel interface signal. If the physical channel interface signal is not present, then the channel interface status is DOWN/DOWN.

When the channel interface is configured for **no state-tracks-signal** (the default) and **no shutdown**, 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 is configured for **no shutdown**:

```
interface channel 5/0
state-tracks-signal
```



CLAW and TCP/IP Offload Commands

Use the commands in this chapter to configure and monitor the Cisco Mainframe Channel Connection (CMCC) products, which include the Channel Interface Processor (CIP) and the Channel Port Adapter (CPA). For hardware technical descriptions and for information about installing the router interfaces, refer to the hardware installation and maintenance publication for your particular product.

Note Unless otherwise specified, all commands in this chapter are supported on the Cisco 7000 with RSP7000, Cisco 7500, and the Cisco 7200 series routers.

For interface configuration information and examples, refer to the "Configuring Cisco Mainframe Channel Connection Adapters" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

For a conversion table of the modular products and Cisco 7000 family processors, refer to the "Platform Support" appendix of the *Cisco IOS Configuration Fundamentals Command Reference*.

claw (primary)

To configure a 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** interface configuration command. 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 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 IOCP, the default values for channel logical address and control unit logical address is 0.
device-address	Hexadecimal value in the range 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 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. 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 *host-app* parameter 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* parameter 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** You can use the **packed** value as an optional keyword for the *host-app* and *device-app* arguments.

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.

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 (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.
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 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.

claw (backup)

To configure a 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**]

```
claw c000 00 198.92.10.5 sysa router1 tcpip tcpip backup
```

no claw *device-address*

Syntax Description

path	Hexadecimal value in the range 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 IOCP, the default values for channel logical address and control unit logical address is 0.
device-address	Hexadecimal value in the range 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 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.

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 non-backup 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 00 198.92.10.5 sysa router1 tcpip tcpip backup
claw c100 00 198.92.10.5 sysa router1 tcpip tcpip backup
claw c200 00 198.92.10.5 sysa router1 tcpip tcpip backup
```

Shortcut form:

```
path c000 c100 c200
  claw 00 198.92.10.5 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 (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.
show extended channel packing names	Displays CLAW packing names and their connection state.

Command	Description
show extended channel packing stats	Displays CLAW packing statistics.
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.

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** interface configuration command. To cancel the offload task on the 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 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 IOCP, the default values for channel logical address and control unit logical address is 0.
device-address	Hexadecimal value in the range 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 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	CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.
host-ip-link	CLAW host link name for the IP link as specified by the host application. For IBM 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 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**.**

Usage Guidelines

Offload devices provide IP connectivity to a mainframe while at the same time 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 which is supporting a directly connected ESCON channel:

```
interface channel 3/0
ip address 198.92.0.1 255.255.255.0
offload 0100 00 198.92.0.21 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.
show extended channel packing names	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.
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.
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 CMCC adapter, use the **offload alias** interface configuration command. 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.

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
```

Related Commands

Command	Description
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 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.

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-stack	Displays information about the UDP listener sockets running on the CMCC adapter interfaces.

offload (backup)

To configure a backup group of Offload devices, use the **offload** IP host backup configuration command. To cancel the offload task on the 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 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 IOCP, the default values for channel logical address and control unit logical address is 0.
ip-address	Hexadecimal value in the range 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 value.
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-ip-link	Host 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.
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 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.

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 at the same time offloading a large part of the TCP/IP processing to the CMCC adapter. Not every mainframe TCP/IP stack supports offload.

The **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 a **offload** IP host backup configuration command.

Long form:

```
offload c000 00 198.92.10.5 sysa router1 tcpip tcpip tcpip api backup
offload c100 00 198.92.10.5 sysa router1 tcpip tcpip tcpip api backup
offload c200 00 198.92.10.5 sysa router1 tcpip tcpip tcpip api backup
```

Shortcut form:

```
path c000 c100 c200
  offload 00 198.92.10.5 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.
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.
show extended channel packing names	Displays CLAW packing names and their connection state.

Command	Description
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.

path

To specify one or more data paths for the IP host backup, use the **path** interface configuration command. 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 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 IOCP, the default values for channel logical address and control unit logical address is 0.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Up to 16 values for the *path* argument can be specified in the **path** command.

The path command places you in IP host backup configuration mode, where you can enter additional commands to define backup groups for 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** interface configuration command. The second group of commands is the shortcut, using the **path** interface configuration command and a **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.

show extended channel backup

To display information about the CLAW and offload commands for each backup group configured on CMCC channel interfaces, use the **show extended channel backup** privileged EXEC command.

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.

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: 80.11.198.2
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 packing names

To display CLAW packing names and their connection state, use the **show extended channel packing names** EXEC command.

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 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 IOCP, the default values for channel logical address and control unit logical address is 0.
device-address	(Optional) Hexadecimal value in the range 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 value.

Command Modes

EXEC

Command History

Release	Modification
12.0	This command was introduced.

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 25 describes the fields shown in the display

Table 25 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 2 devices. You need only specify the even 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 CLAW packing statistics, use the **show extended channel packing stats** EXEC command.

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 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 00 to FE. This value is the unit address associated with the control unit number and path as specified in the host IOCP file. For CLAW and offload support, the device address must have an even value.

Command Modes

EXEC

Command History

Release	Modification
12.0	This command was introduced.

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
```

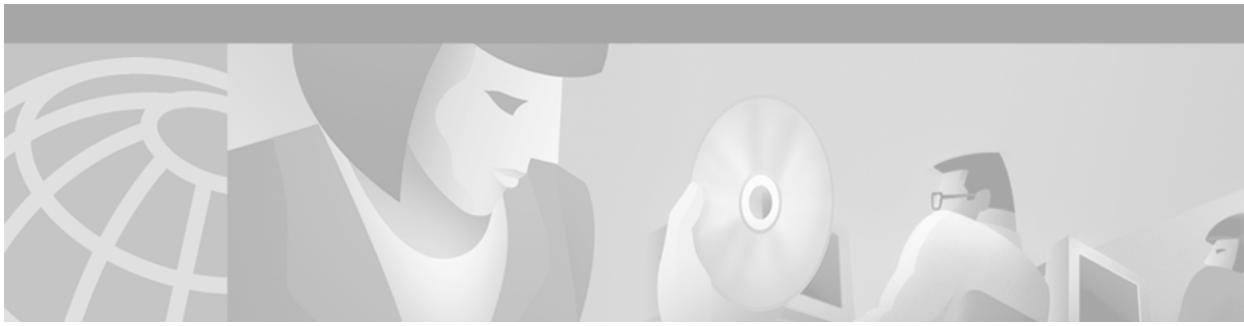
Table 26 describes the fields shown in the display

Table 26 show extended channel packing stats Field Descriptions

Field	Description
Path	Path from the CLAW, offload, or CSNA configuration.
Devs	Device address for each device. One CLAW connection requires 2 devices. You need only specify the even 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.



CMPC, CMPC+ and CSNA Commands

Use the commands in this chapter to configure and monitor the Cisco Mainframe Channel Connection (CMCC) products, which include the Channel Interface Processor (CIP) and the Channel Port Adapter (CPA). For hardware technical descriptions and for information about installing the router interfaces, refer to the hardware installation and maintenance publication for your particular product.

Note Unless otherwise specified, all commands in this chapter are supported on the Cisco 7000 with RSP7000, Cisco 7500 and the Cisco 7200 series routers.

For interface configuration information and examples, refer to the "Configuring Cisco Mainframe Channel Connection Adapters," "Configuring CSNA and CMPC," and "Configuring CMPC+" chapters of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

For a conversion table of the modular products and Cisco 7000 family processors, refer to the "Platform Support" appendix of the *Cisco IOS Configuration Fundamentals Command Reference*.

cmpc

To configure a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel, use the **cmpc** interface configuration command. 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 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 IOCP, the default values for channel logical address and control unit logical address is 0.
device	Hexadecimal value in the range of 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+ TG. The maximum length of the name is 8 characters.
read	Same read value as specified in the 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 for the CMPC+ feature was added.

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 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-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 LLC connection parameters for the CMPC transmission group.
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 SNA support on a CMCC physical channel interface, use the **csna** interface configuration command. This command is used to specify the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe. To delete the 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 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 IOCP, the default values for channel logical address and control unit logical address is 0.
device	Hexadecimal value in the range 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 4096 to 65535 bytes. The default is 20470 bytes.
time-delay *value*	(Optional) Number of milliseconds a host-bound SNA frame may be delayed in order to maximize the channel I/O block size. The range is 0 to 100 ms. The default is 10 ms.
length-delay *value*	(Optional) Amount of SNA frame data in bytes the CSNA subchannel accumulates before sending the accumulated channel I/O block to the attached mainframe. The range is 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.

Usage Guidelines

The parameters **maxpiu**, **time-delay** and **length-delay** 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** parameter allows you to set the maximum size of a host-bound channel I/O block.

The **time-delay** parameter 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 parameter instructs the CSNA subchannel to delay sending the channel I/O block until it contains the number of bytes specified by the length-delay parameter. 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 LLC2 sessions established over the subchannel.

Examples

The following example shows CSNA, offload, and 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
lan	Configures an internal LAN on a CMCC adapter interface and enters the internal LAN configuration mode.
adapter	Configures internal adapters.
show extended channel csna	Displays information about the CSNA subchannels configured on the specified CMCC interface.
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.
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.

show extended channel cmgr

To display information about the MPC+ transmission group (TG) connection manager, use the **show extended channel cmgr** privileged EXEC command.

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.

Usage Guidelines

This command is valid on the CIP's virtual channel interface or the 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 27 describes the fields shown in the display.

Table 27 show extended channel cmgr Field Descriptions

Field	Description
Local Group Token	CMCC's 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.

Table 27 show extended channel cmgr Field Descriptions (continued)

Field	Description
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 and/or 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 CMPC or CMPC+ subchannel configured on the specified channel interface, use the **show extended channel cmpc** privileged EXEC command.

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) 2-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 for the CMPC+ feature was added.

Usage Guidelines

This command is valid only on the 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 28 describes the fields shown in the display.

Table 28 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 VTAM has allocated for each Read. This will match the MAXBFRU value configured in the VTAM 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 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 shutdown. 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—XID2 handshaking in progress. • Active—XID2 exchange completed; CMPC or CMPC+ subchannel is active. • Active**+**—XID2 exchange is complete; subchannel is active in 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 csna

To display information about the CSNA subchannels configured on the specified CMCC interface, use the **show extended channel csna** privileged EXEC command.

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 of 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 of 00 to FE. This is the unit address associated with the control unit number and path as specified in the host 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**, or **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.

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 29 describes the fields shown in the displays.

Table 29 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 VTAM. • open—Subchannel is open. • pendingSetup—VTAM has queried CIP for all configured MAC adapters. • setupComplete —All internal MAC adapter information has been responded to 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 29 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 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 29 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 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.
SlowDowns Sent	Number of times CSNA put VTAM into a slow down (flow control) for this subchannel device.
SlowDowns Received	Number of times VTAM put CSNA into a slow down (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 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 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 hsma

To display hot standby MAC address (HSMA) information, use the **show access-lists hardware** command in privileged EXEC mode.

show extended channel *slot*:*port* **hsma**

Syntax Description

slot:	Chassis slot number of the ISE line card and port number on that line card. Refer to the appropriate hardware manual or online help for port numbers on your networking device.
port	Number of the port on the interface. Refer to the appropriate hardware manual or online help for port numbers on your networking device.

Defaults

There are no defaults.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(3)	This command was introduced.

Examples

The following example shows sample output of the **show extended channel hsma** command:

```
LC-Slot2# show extended channel 1/0 hsma

HSMA information for Channel1/0:
  Control adapter:
    LAN Token-26
    Adapter 26
    MAC Address 4043.1111.001a

  HSMA peers for this control adapter:
                     Hot Standby    HSMA-Partner     Link
  LAN       Adapter  Mac Address     Mac Address     State
  ========================================================
  Token 20  09       4043.1313.9009  4043.3333.001a  UP
   Control Sap: EC(configured)(E8 on next restart)
    Peer State : Active
    Local State: Standby (Preferred)
      Open Stations: 1
    Open SAPs: 1
    XCA Query Interval:  30 seconds.
    Hello Interval    :   2 seconds.
    Dead Interval     :   8 seconds.
```

Table 30 describes the significant fields shown in the display.

Table 30 show extended channel hsma Field Descriptions

Field	Description
Control Adapter	Information about the control adapter.
LAN Token-26	CMCC virtual lan on which the control adapter is configured.
LAN	The number of the CMCC virtual LAN on which the control adapter is configured.
Adapter-26	The adapter number of the control adapter with MAC address 4043.1111.001a
Hot Standby Mac Address	The HSMA MAC address.
HSMA-Partner Mac Address	The MAC address of the control adapter.
Link state	The status of the LLC connection between the control adapters. Valid values are: • UP—The connection is active. • DOWN—The connection is disabled. • Unknown—The router is unable to retrieve the information from the CMCC Control Sap. • OK Peer State– Status of the peer (remote) HSMA adapter
Control Sap	The address of the control service access point (SAP) for this peer. In this example, EC is the current address of the control SAP, but this has been changed, by using the **hsma control-sap** command, to E8. Once the interface is restarted, E8 will become the new control SAP address.
Peer State	The current state of the peer (remote) HSMA adapter. Valid values are: • UNDEFINED—Mismatched configuration options- an error occurred in retrieving the information from the CMCC. • Active—This adapter is active. • Adapter Starting—The adapter is being started. • Checkpointing—Both adapters are active and beginning negotiations to decide which will remain active. • Negotiating—The peers are negotiating their roles. • Pending Enable—The HSMA adapter is being enabled. • Shutdown—The HSMA adapter has been shutdown. • Standby—The HSMA adapter is not active because the peer is active. • Stopped—HSMA is initializing. • XCA Inactive—The XCA associated with this adapter is not active. • (Preferred)—The **hsma preferred** command is configured on this adapter.

Table 30 show extended channel hsma Field Descriptions (continued)

Field	Description
Local State	Status of the HSMA adapter on this interface (same as for peer).
Open Stations	The number of LLC2 connection stations open on this internal adapter.
Open SAPs	The number of SAPs open on this internal MAC adapter.
XCA Query Interval	The time interval between checks of the status of the XCA that has opened the HSMA adapter.
Hello Interval	The time interval between hello messages between the peered HSMA CIP or CPAs. This is configured by the **hsma hello-interval** command.
Dead Interval	Time interval during which at least one hello packet must be received from the peer HSMA adapter before the router declares that neighbor down. This is configured by the **hsma dead-interval** command.

show extended channel tg

To display configuration, operational information, and statistics information for CMPC or CMPC+ transmission groups configured on the specified CMCC adapter's virtual interface, use the **show extended channel tg** EXEC command.

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+ 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

EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.0(3)T	Support for the CMPC+ feature was added.

Usage Guidelines

The **show extended channel tg** command is valid only on the virtual channel interface. If *tg-name* argument is not specified, information about all TGs configured on the specified interface is displayed.

If neither the **oper** or **stats** arguments are 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 31 describes the fields shown in the display.

Table 31 show extended channel tg oper Field Descriptions

Field	Description
Status	Connection status of the CMPC TG. Valid values are: • Shutdown—CMCC virtual interface is shutdown. In this state, all nonconfigurable values will not be displayed and the LLC connection operational values displayed when the detailed argument 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—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 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 VTAM. The name is extracted from XID3s received from 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 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 SAP value.
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 detail 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 32 describes the fields shown in the display.

Table 32 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.
UIFramesIn	Number of connectionless PIUs (HPR frames) received by this CMPC TG from the remote network node.
UIFramesOut	Number of connectionless PIUs (HPR frames) 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.
SweepReqsIn	Number of CMPC sweep requests received from VTAM on this CMPC TG.

Table 32 show extended channel tg stats Field Descriptions (continued)

Field	Description
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.
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.
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.
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.
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.
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 a 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 detail 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:201.44.4.1                    Remote IP Address :201.44.4.2

  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 33 describes the fields shown in the display.

Table 33 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 argument 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 HSAS stack.
Local VC Token	CMCC adapter's token for the virtual circuit.
Remote VC Token	Host's token for the virtual circuit.

Table 33 show extended channel tg Field Descriptions (continued)

Field	Description
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 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 34 describes the fields shown in the display.

Table 34 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.
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.

tg (CMPC)

To define LLC connection parameters for the CMPC transmission group, use the **tg** (CMPC) interface configuration command. 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 TG. The maximum length of the name is eight characters. This must match the name specified on the **cmpc** statements.
llc	Specifies that this TG is connected to the LLC stack on the CMCC adapter card.
token-adapter	Internal adapter type on the CMCC adapter card. The currently 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 SAP number, 04 to FC, in hexadecimal. The value must be even and should normally 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 even 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.

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, the existing TG must be removed first by using the **no tg** command.

The **no tg** command removes the CMPC TG from the configuration. If the TG is used for a non-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 CMPC+ transmission group, use the **tg** (CMPC+) interface configuration command. 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+ 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 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* parameter 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* parameter 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.

Usage Guidelines

The **tg** (CMPC+) command is valid only on the CIP's virtual channel interface and the CPA's physical channel interface. This command defines either an IP connection or an HSAS IP connection.

To change any parameter of the **tg** (CMPC+) command, 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+:

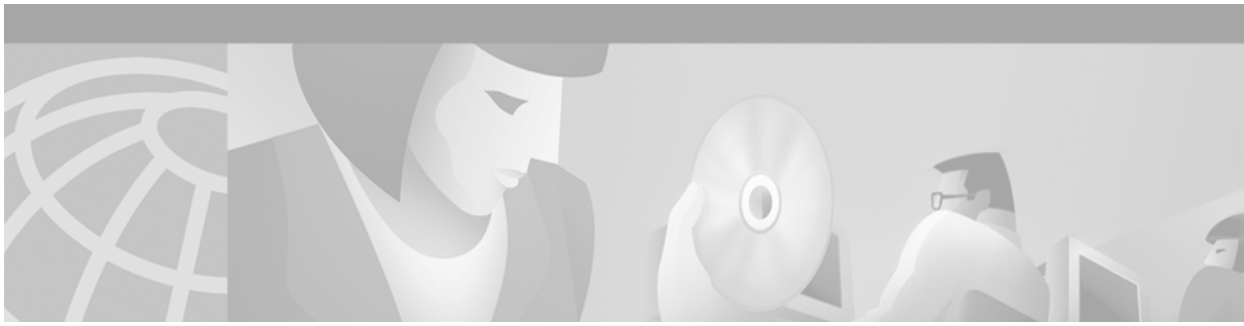
```
interface Channel0/2
 ip address 80.12.165.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip route-cache same-interface
 no ip mroute-cache
 no keepalive
 tg TG00 hsas-ip 80.12.165.2 80.12.165.1
```

The following example configures a TG name for an IP stack configured with CMPC+:

```
interface Channel0/2
 ip address 80.12.165.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip route-cache same-interface
 no ip mroute-cache
 no keepalive
 tg TG00     ip 80.12.165.2 80.12.165.1
```

Related Commands

Command	Description
cmpc	Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.



TN3270 Server Commands

Use the commands in this chapter to configure and monitor the Cisco Mainframe Channel Connection (CMCC) products, which include the Channel Interface Processor (CIP) and the Channel Port Adapter (CPA). For hardware technical descriptions and for information about installing the router interfaces, refer to the hardware installation and maintenance publication for your particular product.

Note Unless otherwise specified, all commands in this chapter are supported on the Cisco 7000 with RSP7000, Cisco 7500 and the Cisco 7200 series routers.

For interface configuration information and examples, refer to the "Configuring the TN3270 Server" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide*.

For a conversion table of the modular products and Cisco 7000 family processors, refer to the "Platform Support" appendix of the *Cisco IOS Configuration Fundamentals Command Reference*.

allocate lu

To assign logical units (LUs) to a pool, use the **allocate lu** listen-point PU configuration command. 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 8 characters.
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.

Defaults

No default behavior or values.

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 T.

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 5 LOCADDRs, therefore 25 LOCADDRs (10 through 34) 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.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.
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.

certificate reload

To configure SSL Encryption Support enabled to read the profile security certificate from the file specified in the **servercert** command, use the **certificate reload** profile configuration command.

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.

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.

client ip

To add an IP subnet to a client subnet response-time group, use the **client ip** response-time configuration command. 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

No default behavior or values.

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.

Examples

Following is an example of the **client ip** command:

```
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.
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.

Command	Description
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 LU or range of LUs to a client at the IP address or subnet, use the **client ip lu** TN3270 PU configuration mode command. 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*n*, where *n* is any alphanumeric character. Moreover, it ensures that a printer matching the IP address condition can only use 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 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 locaddrs.
first-locaddr	Defines a single locaddr to nail.
last-locaddr	(Optional) Defines the end range of inclusive locaddrs 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.

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 only appear in 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 locaddrs are already nailed. If the locaddrs are currently in use by other remote clients, the nailing statement will take effect only when the locaddr 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 locaddrs was specified, to cancel this definition the whole range of locaddrs must be specified. There is no way to cancel only one locaddr if a whole range of locaddrs was configured.

Examples

In the following example, locaddrs 1 to 50 are reserved for remote devices in the 171.69.176.0 subnet:

```
interface channel 2/2
 tn3270-server
 pu BAGE4
  client ip 171.69.176.28 255.255.255.0 lu 1 50
```

In the following example, locaddrs 1 to 40 are reserved for screen devices in the 171.69.176.0 subnet, while 41 to 50 are reserved for printers in that subnet:

```
interface channel 2/2
 tn3270-server
 pu BAGE4
  client ip 171.69.176.28 255.255.255.0 lu 1 40
  client printer ip 171.69.176.28 255.255.255.0 lu 41 50
```

In the following example, there is an attempt to cancel a definition but this is rejected because it does not specify the full range of locaddrs and the second attempt fails to specify the correct nail type:

```
interface channel 2/2
 tn3270-server
  pu BAGE4
  client printer ip 171.69.176.50 255.255.255.0 lu 1 100
  no client printer ip 171.69.176.50 255.255.255.0 lu 1
  %Invalid LU range specified
  no client ip 171.69.176.50 255.255.255.0 lu 1 100
  %client ip 171.69.176.50 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** listen-point configuration command. 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 LOCADDRS.
poolname	Specifies a unique pool name. The pool name cannot exceed 8 characters.

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 into Cisco IOS Release 12.0 T.

Usage Guidelines

If the pool is configured while LUs 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 OMAHA:

```
tn3270-server
 pool OMAHA cluster layout 10s1p
 listen-point 172.18.4.18
  client ip 10.1.2.3 255.255.255.0 pool OMAHA
```

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.

client lu maximum

To limit the number of 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* [*ip-mask*]] **lu maximum** *number*

no client [*ip* [*ip-mask*]]

Syntax Description

ip	(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.

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 simply 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 **no client** to specify an unlimited number of LU sessions. The **lu number** 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 of 10.1.1.64 through 10.1.1.127) are limited to a maximum of 5 LU sessions while other clients with IP addresses in the subnet 10.1.1.0 are limited to a maximum of 4 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** listen-point configuration command. 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 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 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 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 8 characters.

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**.

Usage Guidelines

If the pool is configured while LUs 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 OMAHA:

```
tn3270-server
 pool OMAHA cluster layout 10s1p
 listen-point 172.18.4.18
 client ip 10.1.2.3 255.255.255.0 pool OMAHA
```

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 george-isdn29.cisco.com to the pool named GENERAL:

```
tn3270-server
  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 george-isdn29.cisco.com pool GENERAL
```

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 GENERAL:

```
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 lucy-isdn49 23 pool GENERAL
```

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 GENERAL:

```
tn3270-server
  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 domain-name .cisco.com pool GENERAL
```

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 GENERAL:

```
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 domain-id 23 pool GENERAL
```

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.

default-profile

To specify the name of the profile to be applied as a default to all the listen points, use the **default-profile** security command. To disable the default profile specification, use the **no** form of this command.

default-profile *profilename*

no default-profile *profilename*

Syntax Description

profilename	Profile name should already be configured.

Defaults

No default profile.

Command Modes

Security configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

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 non-secure 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**. This will not affect the non-secure connections.

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
sec-profile	Specifies the security profile to be associated with a listen point.
profile	Specifies a name and a security protocol for a security profile and enters profile configuration mode.

disable (TN3270)

To turn off security in the TN3270 server, use the **disable** (TN3270) security configuration command.

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.

Usage Guidelines

Configuring the **disable** (TN3270) command does not terminate any active secure or non-secure connections. This command specifies that all new connections established with the TN3270 server will be non-secure. 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 non-secure:

```
disable
```

Related Commands

Command	Description
enable (TN3270)	Turns on security in the TN3270 server.

dlur

To enable the Systems Network Architecture (SNA) session switch function on the CMCC adapter and enter dependent logical unit requester (DLUR) configuration mode, use the **dlur** TN3270 server configuration command. 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 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.

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 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 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 DLUS for the DLUR function, use the **dlus-backup** DLUR configuration command. To remove a backup DLUS name, use the **no** form of this command.

dlus-backup *dlusname2*

no dlus-backup

Syntax Description

dlusname2	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.

Usage Guidelines

This command is valid only on the virtual channel interface. Only one backup DLUS can be specified per 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 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 8 characters long; for example, RA12.NODM1PP. The portion of the name before the period is the 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 DNS nailing, use the **domain-id** TN3270 server configuration command. 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 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.

Usage Guidelines

The user can configure up to 255 domain names, one per statement.

This command must be configured 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
```

Related Commands

Command	Description
client pool	Nails clients to pools.

enable (TN3270)

To turn on security in the TN3270 server, use the **enable** (TN3270) security configuration mode command.

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.

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 configuration** 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.

encryptorder

To specify the security encryption algorithm for the SSL Encryption Support, use the **encryptorder** profile configuration command.

encryptorder [**DES**] [**3DES**] [**RC4**] [**RC2**] [**RC5**]

Syntax Description

DES	(Optional) Specifies the DES encryption algorithm.
3DES	(Optional) Specifies the 3DES encryption algorithm.
RC4	(Optional) Specifies the RC4 encryption algorithm.
RC2	(Optional) Specifies the RC2 encryption algorithm.
RC5	(Optional) Specifies the RC5 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.

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
```

generic-pool

To specify whether or not leftover LUs will be made available to TN3270 sessions that do not request a specific LU or LU pool through TN3270E, use the **generic-pool** TN3270 server configuration command. 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 currently configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration—The **generic-pool** command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **generic-pool** command at this level applies to all PUs defined at the listen point.

Listen-point PU configuration—The **generic-pool** command at this level applies only to the specified PU.

DLUR PU configuration—The **generic-pool** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **generic-pool** command at this level applies only to the specified PU.

Command History

Release	Modification
11.2	This command was introduced.

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 ACTLU during PU start-up.
- 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 **generic-pool** in 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 **generic-pool deny** 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 **generic-pool permit** is specified, any inactive LUs are immediately available for dynamic connections. Moreover, any active LUs that were dynamic previously (before **generic-pool deny** 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 how many seconds of LU inactivity, from both host and client, before the TN3270 session is disconnected, use the **idle-time** TN3270 server configuration command. 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 currently configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration—The **idle-time** command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **idle-time** command at this level applies to all PUs defined at the listen point.

Listen-point PU configuration—The **idle-time** command at this level applies only to the specified PU.

DLUR PU configuration—The **idle-time** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **idle-time** command at this level applies only to the specified PU.

Command History

Release	Modification
11.2	This command was introduced.

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 currently 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 between 600 and 900 seconds are immediately disconnected.

Note For the purposes of idle-time logic, TIMING-MARKs generated by the keepalive logic do not constitute “activity.”

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).

ip precedence (TN3270)

To specify the precedence level for voice over IP traffic in the TN3270 server, use the **ip precedence** TN3270 server configuration command. 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 the precedence is for screen devices.
printer	Specifies the precedence is for printer devices.
value	Sets the precedence priority. A value between 0 and 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—The **ip precedence** (TN3270) command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **ip precedence** (TN3270) command at this level applies to all PUs defined at the listen point.

DLUR PU configuration—The **ip precedence** (TN3270) command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **ip precedence** (TN3270) command at this level applies only to the specified PU.

Command History

Release	Modification
11.3	This command was introduced.

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.

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** TN3270 server configuration command. 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 the ToS is for screen devices.
printer	Specifies the ToS is for printer devices.
value	Sets the ToS priority. A value between 0 and 15. The default is 0.

Defaults

The default is a ToS value of 0 for both screens and printers.

Command Modes

TN3270 server configuration—The **ip tos** command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **ip tos** command at this level applies to all PUs defined at the listen point.

DLUR PU configuration—The **ip tos** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **ip tos** command at this level applies only to the specified PU.

Command History

Release	Modification
11.3	This command was introduced.

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 35 shows the values described in RFC 1349.

Table 35 ToS Defined Values

Value	Definition	Action
0	All normal.	Use default metric.
8	Minimize delay.	Use delay metric.
4	Maximize throughput.	Use default metric.

Table 35 ToS Defined Values (continued)

Value	Definition	Action
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 either 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.

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
  pu 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 transmits a DO TIMING-MARK or Telnet no operation (nop) to the TN3270 client, use the **keepalive** TN3270 server configuration command. 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* is the value of the interval. The value of the *max-response-time* should be less than or equal to the *interval*.

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* is the value of the interval.

Command Modes

TN3270 server configuration—The **keepalive** command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **keepalive** command at this level applies to all PUs defined at the listen point.

Listen-point PU configuration—The **keepalive** command at this level applies only to the specified PU.

DLUR PU configuration—The **keepalive** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **keepalive** command at this level applies only to the specified PU.

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The **send** {**nop** | **timing-mark** [*max-response-time*]} keywords were added.

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 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 currently active and future TN3270 sessions. For example, reducing the keepalive interval to a smaller 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, smaller 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.

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 first configured in TN3270 server configuration mode, followed by Listen-point PU configuration mode. The **keepalive** command values specified under the listen-point PU overrides 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 SSL Encryption Support, use the **keylen 128** profile configuration command. 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.

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.

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
```

link (TN3270)

To define and activate a link to a host, use the **link** DLUR SAP configuration command. 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 DLUR function.
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 *rsap* value must be even and should be a multiple of 4, but this 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.

Usage Guidelines

This command is valid only on the virtual channel interface. The combination of *rmac* and *rsap* must be unique within the DLUR SAP function. These values can only be changed by deleting the link definition, using the **no link** command, and recreating the link definition.

For a link via a channel on this 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 CSNA or 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** TN3270 server configuration command. 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 LU sessions under this 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 T.

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 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 configuring 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

Following is an example of the **listen-point** command showing 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.

lsap

To create a SAP in the SNA session switch and enter 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 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 and should normally be a multiple of four. It must be 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.

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 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 VTAM to delete the corresponding LU when a client disconnects, use the **lu deletion** TN3270 server configuration command. 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.
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.

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 in to Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to add the **named** keyword.

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 currently 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 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 RU is sent by the TN3270 server when a client turns off his device or disconnects, use the **lu termination** TN3270 server configuration command. 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 an 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—The **lu termination** command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **lu termination** command at this level applies to all PUs defined at the listen point.

Listen-point PU configuration—The **lu termination** command at this level applies only to the specified PU.

DLUR PU configuration—The **lu termination** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **lu termination** command at this level applies only to the specified PU.

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 T.

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 CICS.

If you use the **unbind** keyword for session termination with applications such as CICS, 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.

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
```

maximum-lus

To limit the number of LU control blocks that will be allocated for the TN3270 server, use the **maximum-lus** TN3270 server configuration command. 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 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 five 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.

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 PU is inactivated by DACTPU or by using the **no pu** command.

If the number of LUs in use reaches 94 percent of the current setting of maximum-lus, 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 ACTLU from the SSCP host.

By limiting the number of LU control blocks allocated, you can make sure enough memory is available to support other 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 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.

pool

To define pool names for the TN3270 server and specify the number of screens and printers in each logical cluster, use the **pool** TN3270 server configuration command. 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 which cannot exceed 8 characters. Valid characters are (alphabetic characters are not case sensitive): • 1st character—Alphabetic (A-Z) and national characters '@', '#', and '$' • 2nd-8th characters—Alphabetic (A-Z), numeric (0-9), and national characters '@', '#', and '$'
cluster layout *layout-spec-string*	(Optional) Name for the cluster and to indicate a cluster of LUs 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*. 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 T.

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 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 8 characters or at an invalid character (whichever comes first) when processing the CONNECT request.

When using a **pool** command to create a cluster, a combination of the following values is used in the *layout-spec-string*:

- s (screen)
- p (printer)
- a (any, or wildcard) [Refers to a printer or a screen]

Use the following format to define the *layout-spec-string*, where *decimal_num* is a decimal number between 1 and 255:

pool *poolname* **cluster layout** {*decimal_num***s**}{*decimal_num***p**}{*decimal_num***a**}

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*. The default is 1a, which defines 1 screen or 1 printer. A screen, printer, or a wildcard definition cannot be followed by a definition of the same type. A screen definition can only be followed 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 between 1 and 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* can support a maximum of 4 groups.

Consider the following example:

```
pool CISCO cluster layout 2s3p4a5s6a7s8p9s
```

There are 4 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 LOCADDRs:

- Pool and LU names must be unique; they cannot be identical.
- LOCADDR ranges for pools must not overlap.
- LOCADDR 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.

preferred-nnserver

To specify a preferred network node (NN) as server, use the **preferred-nnserver** DLUR configuration command. 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.

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 APPN products, including 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 NET ID and is shared between entities in the same logical network.

When no preferred server is specified, the 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, as above.

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.

profile

To specify a name and a security protocol for a security profile and enter profile configuration mode, use the **profile** security configuration command. To remove this name and protocol specification, use the **no** form of this command.

Create a new profile:

profile *profilename* {**ssl** | **none**}

Modify an existing profile:

profile *profilename*

Delete a profile:

no profile *profilename* {**ssl** | **none**}

Syntax Description

profilename	String of alphanumeric characters which 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.

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 only required 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 currently defined.

Entering the profile command moves the user into the profile configuration mode. Entering the **no** form of the command moves 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 non-secure.

```
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
```

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 PU entity that has no direct link to a host or to enter PU configuration mode, use the **pu** DLUR configuration command. 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 only enforces uniqueness within the set of DLUR PUs.
ip-address	IP address that the clients should use as host IP address to map to LU sessions under this PU.

Defaults

No PU is defined.

Command Modes

DLUR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If the PU is already created, the **pu** *pu-name* command with no arguments puts you 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 TSO specify an IP address that will be defined with PUs that have LOGAPPL=TSO.

Examples

The following example defines define 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 PU entity that has a direct link to a host or to enter listen-point PU configuration mode, use the **pu** listen-point configuration command. 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 cannot tell which remote hosts are in which subareas and does not enforce the unique value requirement.
type	Internal adapter type on the 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 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) 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 LOCADDR 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 and the entire string, including the # symbols, must not exceed 8 characters.

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 Release 12.0 T.

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 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 CSNA or 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 PU entity that has its own direct link to a host and enter PU configuration mode, use the **pu** TN3270 server configuration command. 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	The value for this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 Server cannot tell which remote hosts are in which subareas and does not enforce the unique value requirement.
ip-address	IP address that the clients should use as host IP address to map to LU sessions under this PU.
type	Internal adapter type on the 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 SAP number in hexadecimal, ranging from 04 to FC. 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, 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) Provides an LU name that the client can use when a specific LU name request is needed. The format can be *x...x*## or *x...x*### where *x...x* is an alphanumeric string. When ## is specified, it is replaced with the LU LOCADDR 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 and the entire string, including the # symbols, must not exceed 8 characters.

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.

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 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 CSNA or 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 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 PU entity that has no direct link to a host or to enter listen-point PU configuration mode, use the **pu dlur** listen-point configuration command. 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 for 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 only enforces uniqueness within the set of DLUR PUs.
lu-seed *lu-name-stem*	(Optional) 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 LOCADDR 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 8 characters. The # symbols are allowed in the middle 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.
12.0(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 lu-seed naming format was modified.

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 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 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 lu-seed 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 (i.e., 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 LOCADDR.

Table 36 LU Seed Name Examples

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.

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 of 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.

Usage Guidelines

Multiple response-time groups can be configured within the scope of available memory. When using this command, 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
```

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.

sec-profile

To specify a security profile to be associated with a listen point, use the **sec-profile** listen-point configuration command. 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.

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
```

Related Commands

Command	Description
profile	Specifies a name and a security protocol for a security profile and enters profile configuration mode.
default-profile	Specifies the name of the profile to be applied to the listen points by default.

security (TN3270)

To enable security on the TN3270 server, use the **security** command. 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.

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 non-secure) 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 the 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
```

servercert

To specify the location of the TN3270 server's security certificate in the router's Flash memory, use the **servercert** profile configuration command.

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.

Usage Guidelines

The certificate is in X.509 format, signed by a Certificate Authority (CA). The certificate must be created offline. It cannot be created using using the Cisco IOS software. Use third-party software or a Windows-based utility. The certificate should be in 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.

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 extended channel tn3270-server

To display current server configuration parameters and the status of the PUs defined for the TN3270 server, use the **show extended channel tn3270-server** EXEC command.

show extended channel *slot*/*port* **tn3270-server**

Syntax Description

slot	Specifies a particular CMCC adapter in the router where *slot* is the slot number.
port	Port value for a TN3270 server will always be 2.

Defaults

No default behavior or values.

Command Modes

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.

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 37 describes significant fields in the display. Those fields not described correspond to configured values.

Table 37 show extended channel tn3270-server Field Descriptions

Field	Description
server pickup	IP address and TCP port number, listen point, configured on one or more PUs.
lu *number*	Total number of LUs available for this listen point.
in-use *number*	Number of LUs currently in use.
connect *number*	Total number of connect ins since the TN3270 feature was started.
disconn *number*	Total number of disconnects since the TN3270 feature was started.
fail *number*	Total number of failed connects since the TN3270 feature was started.
response time, host *number*	The average response time from the host across all sessions through this server IP address. This is measured from sending CD to the host to receiving the reply.
response time, tcp *number*	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 only sent on special occasions, such as Bind.
idle-time *number*	Configured idle-time for this PU.
keepalive *number* (*action*)	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 *type*	Configured unbind action for LUs on this PU.
tcp-port *number*	Configured TCP port number.
generic-pool *type*	Configured generic-pool for LUs on this PU.
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 RU is sent by the TN3270 server when a client turns off the device or disconnects. The possible 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.

Table 37 show extended channel tn3270-server Field Descriptions (continued)

Field	Description
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 VTAM to delete the corresponding LU when a client disconnects. The possible 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 *fq-cpname*	Configured fully qualified DLUR CP name(fq-cpname).
status *status-value state-value*	Shows the status of the DLUR-DLUS pipe followed by the state of the pipe. Possible 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 *fq-dlusname*	Currently active DLUS.
name *pu-name*	This is the name of the PU as configured.
ip:tcp *ip-addr:tcpport*	IP address and TCP port number configured for the PU.
xid *number*	Configured XID—idblk and idnum.

Table 37 show extended channel tn3270-server Field Descriptions (continued)

Field	Description
STATE *value*	Possible 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 ACTPU is received. • ACTIVE—ACTPU is received and acknowledged positively. • ACT/BUSY—Awaiting host to acknowledge the SSCP-PU 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 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 SNA Session Switch PU.
DESTINATION *mac-address or PU-name*	If a direct PU, then it is the destination MAC address, otherwise, it is the name of the partner PU.
R-LSAP *number number*	Remote and local 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** EXEC command.

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 *ip-address* in disconnected state. Disconnected state refers to an LU session state of ACTIVE or INACTIVE. In this case, the *ip-address* refers to the client that last used the LU.
in-session	(Optional) Displays all clients with *ip-address* in active session state. Active session state refers to an LU session state of ACT/SESS.
pending	(Optional) Displays all clients with *ip-address* 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

EXEC

Command History

Release	Modification
11.2	This command was introduced.

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 show 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 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 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 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 10.14.1.21 pending
Total 2 clients found using 10.14.1.21
```

Table 38 describes significant fields in the display.

Table 38 show extended channel tn3270-server client-ip-address Field Descriptions

Field	Description
lu *locaddr*	LOCADDR of the LU.
name *lu-name*	If the PU is directly connected, then the name shown is the one generated by the seed. If DLUR, then only the unqualified portion is shown. The NET ID portion will be the same as the current DLUS.
client-ip:tcp *ip-address:port*	Client's IP address and TCP port number.
nail	Status of LU nailing, either Y or N.
state *lu-state*	LU state and their meanings are: • UNKNOWN—LU in an undefined state • INACTIVE—LU did not receive ACTLU • ACT/NA—LU received ACTLU and acknowledged positively • P-SDT—LU is bound but there is no 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 DACTLU response • P-PSID—Awaiting NMVT Reply PSID response • P-BIND—Waiting for host to send bind

Table 38 show extended channel tn3270-server client-ip-address Field Descriptions (continued)

Field	Description
state *lu-state* (continued)	• P-UNBIND—Awaiting host unbind response • WT-UNBND—Waiting for client to acknowledge disconnection • WT-SDT—Waiting for client to acknowledge SDT
model model	IBM 3278 model type of client; blank if STATIC LU.
frames in *number*	Number of frames sent inbound to the host.
frames out *number*	Number of frames sent outbound from the host.
idle for *time*	Time the client has been idle. The time is in HH:MM:SS.
pu is *pu-name*	Name of the PU.
lu is *type*	Whether LU is DYNAMIC or STATIC.
negotiated *type*	Whether client is TN3270 or TN3270E.
bytes in / out *number/number*	Total number of bytes sent to/received from the host.
RuSize in / out *number/number*	RU size as configured in the bind.
NegRsp in / out *number/number*	Number of SNA negative responses sent to/received from the host.
pacing window in / out *number/number*	SNA pacing window as configured in the bind.
credits in *number*	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue size in *number*	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 *number*	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** EXEC command.

show extended channel *slot/virtual channel* **tn3270-server client-name** *name*

Syntax Description

slot	Specifies a particular CMCC adapter in the router where *slot* 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

EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.

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 38 describes significant fields in the display.

Table 39 show extended channel tn3270-server client-name Field Descriptions

Field	Description
lu *locaddr*	LOCADDR of the LU.
name *lu-name*	If the PU is directly connected, then the name shown is the one generated by the seed. If DLUR, then only the unqualified portion is shown. The NET ID portion will be the same as the current DLUS.
client-name *name*	Client's machine name.
nail	Status of LU nailing, either Y or N.
state *lu-state*	LU state values and their meanings: • UNKNOWN—LU in an undefined state • INACTIVE—LU did not receive ACTLU • ACT/NA—LU received ACTLU and acknowledged positively • P-SDT—LU is bound but there is no SDT yet • ACT/SESS—LU is bound and in session • P-ACTLU—Telnet has connected 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 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 *model*	IBM 3278 model type of client; blank if STATIC LU.
frames in *number*	Number of frames sent inbound to the host.
frames out *number*	Number of frames sent outbound from the host.
idle for *time*	Time the client has been idle. The time is in HH:MM:SS.
pu is *pu-name*	Name of the PU.
lu is *type*	Whether LU is DYNAMIC or STATIC.
negotiated *type*	Whether client is TN3270 or TN3270E.
bytes in / out *number/number*	Total number of bytes sent to/received from the host.
RuSize in / out *number/number*	RU size as configured in the bind.
NegRsp in / out *number/number*	Number of SNA negative responses sent to/received from the host.
pacing window in / out *number/number*	SNA pacing window as configured in the bind.

Table 39 show extended channel tn3270-server client-name Field Descriptions (continued)

Field	Description
credits in *number*	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue- size in *number*	Number of SNA frames waiting to be sent to the host that are blocked and are waiting for a pacing response.
queue-size out *number*	SNA frames not yet acknowledged by an isolated pacing response by the TN3270 server.
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 SNA session switch, use the **show extended channel tn3270-server dlur** EXEC command.

show extended channel *slot*/*port* **tn3270-server dlur**

Syntax Description

slot	Slot number.
port	Port number.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

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 40 describes significant fields in the display.

Table 40 show extended channel tn3270-server dlur Field Descriptions

Field	Description
dlur *fq-luname*	Fully qualified CP name used by the SNA session switch and the LU name for the DLUR function configured as the *fq-cpname* on the dlur statement.
current dlus *fq-luname*	Name of the currently active DLUS, either the primary DLUS or the backup DLUS.

Table 40 show extended channel tn3270-server dlur Field Descriptions (continued)

Field	Description
dlur-dlus status *dlur-status*	Possible 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 CMCC adapter. • SHUT—The TN3270 server is shut down. • NOTKNOWN—Status cannot be obtained.
preferred dlus *fq-luname*	Name of the DLUS as configured on the DLUR statement.
backup dlus *fq-luname*	Name of the DLUS that is used if the preferred DLUS is unavailable.
preferred server *fq-luname*	Fully qualified name of the preferred network node server.
lsap	Configured value for the local SAP on the configured internal adapter. Token-adapter specifies the type of internal adapter used.
vrn *fq-name*	Name of the connection network as configured by the vrn statement for this LSAP and internal adapter pair.
lsap...status status	Possible *sap-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.
link *name*	Name of the configured link. If not a configured link, then the name is an invented name, @DLUR*nn*.

Table 40 show extended channel tn3270-server dlur Field Descriptions (continued)

Field	Description
remote *mac sap*	Remote MAC and SAP for this link.
link...status *status*	Possible *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 DLUR components, use the **show extended channel tn3270-server dlurlink** EXEC command.

show extended channel *slot*/*port* **tn3270-server dlurlink** *name*

Syntax Description

slot	Specifies a particular CMCC adapter in the router where slot is the slot number.
port	Port number.
name	Name of the SNA session switch link to be displayed.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

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 41 describes significant fields in the display.

Table 41 show extended channel tn3270-server dlurlink Field Descriptions

Field	Description
lsap...vrn...status *status*	Possible *lsap-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.
link *name*	Name is an invented name, @DLUR*nn*, if not a configured link.
link...status *status*	Possible *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 *name*	CP name of the remote node for this link.
tgn *tg-number*	Transmission group (TG) number for this link. Because the SNA session switch only supports 1 TG per pair of CP names, it is typically 0 or 1.
maxdata *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** EXEC command.

show extended channel *slot/virtual channel* **tn3270-server nailed-domain** *name*

Syntax Description

slot	Specifies a particular CMCC adapter in the router where *slot* 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 “.ciosco.com.”

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.

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 42 describes significant fields in the display.

Table 42 show extended channel tn3270-server nailed-domain Field Descriptions

Field	Description
.CISCO.COM	Nailed domain name.
listen point *ipaddress*	Listen point IP address under which the **client pool** command was configured.
pool *poolname*	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 LUs, use the **show extended channel tn3270-server nailed-ip** EXEC command.

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

EXEC

Command History

Release	Modification
12.0	This command was introduced.

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 43 describes significant fields in the display.

Table 43 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.
lu 1 50	LU LOCADDR range showing first LOCADDR and last LOCADDR. There need not be a last LOCADDR if only a single LOCADDR rather than a range is configured.
printer	Type of device being nailed to the LOCADDRs. If printer is specified, only clients which are printers are nailed to the LOCADDRs. If screen is specified, only clients that are screens are nailed to the LOCADDRs. If neither is specified, both screens and printers can use the LOCADDRs. A printer client is any client with a device type of “328*”. A screen client is a client with any other device type.

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 nailed-name

To list all nailing statements with a specific nailed machine name, use the **show extended channel tn3270-server nailed-name** EXEC command.

show extended channel *slot/virtual channel* **tn3270-server nailed-name** *name*

Syntax Description

slot	Specifies a particular CMCC adapter in the router where *slot* 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

EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.

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-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 44 describes significant fields in the display.

Table 44 show extended channel tn3270-server nailed-name Field Descriptions

Field	Description
MYCLIENT.CISCO.COM	Fully qualified domain name of nailed client.
listen point *ipaddress*	Listen point IP address under which the **client pool** command was configured.
pool *poolname*	Pool name to which the client is nailed.

show extended channel tn3270-server pu

To display configuration parameters for a PU and all the LUs currently attached to the PU, including the LU cluster layout and pool name, use the **show extended channel tn3270-server pu** EXEC command.

show extended channel *slot/virtual channel* **tn3270-server pu** *pu-name* [**cluster | client-name**]

Syntax Description

slot	Specifies a particular CMCC adapter in the router where *slot* 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

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 **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** optional keyword was added.
12.2	The **Named** value was added for the lu-deletion field in the output display.

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 SNA session switch PU.

The output for the **show extended channel tn3270-server pu** command varies based on using 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

This 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
```

Following is an example of the 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 161.44.100.162:1538   N   ACT/SESS 3278S2E  228     172    0:0:2
51  SHED1051 161.44.100.162:1539   N   ACT/SESS 3278S2E  240     181    0:0:2
151 SHED1151 161.44.100.162:1536   N   ACT/SESS 327802E  212     160    0:0:5
152 SHED1152 161.44.100.162:1537   N   ACT/SESS 3278S2E  220     166    0:0:4
200 SHED1200 161.44.100.162:1557   N   ACT/SESS 3278S2E  244     184    0:0:2
```

Following is an example of the output from the **show extended channel tn3270-server pu** command with the cluster keyword for a PU named PU1. In the example below, 1/1a identifies cluster 1 with a layout of 1a, which contains 1 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 161.44.100.162:1538   N   ACT/SESS 1/4s1p  PCPOOL   1/5
51  SHED1051 161.44.100.162:1539   N   ACT/SESS 1/49s1p UNIXPOOL 1/50
151 SHED1151 161.44.100.162:1536   N   ACT/SESS 1/1a    :GENERIC 1/1
152 SHED1152 161.44.100.162:1537   N   ACT/SESS 1/1a    :GENERIC 1/1
200 SHED1200 161.44.100.162:1557   N   ACT/SESS 1/1a    SIMPLE   1/1
```

Note If the cluster layout is very long, only the first 8 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.

Following is an example of the 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 45 describes significant fields in the display.

Table 45 show extended channel tn3270-server pu Field Descriptions

Field	Description
name (index) *pu-name* (*index*)	Name and index of the PU as configured.
ip:tcp *ip-addr:tcp-port*	IP address and TCP port number configured for the PU.
xid *number*	Configured XID—idblk and idnum.
state *pu-state*	Possible pu-state values and their meanings: • 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, XID is sent. • P-ACTPU—Link station is up but no ACTPU is received. • ACTIVE—ACTPU is received and acknowledged positively. • ACT/BUSY—Awaiting host to acknowledge the 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—DLUR PU and direct PU states disagree. • P-DACTPU—PU is pending DACTPU. • OTHER—State is an undefined value.
link *type*	LINK type is either internal adapter type and internal adapter number, or dlur if it is a SNA Session Switch PU.
destination *mac-address or pu-name*	If a direct PU, then it is the destination MAC address, otherwise, it is the name of the partner PU.
r-lsap *number number*	Remote and local SAP values.
idle-time *number*	Configured idle-time for this PU.
keepalive *number* (*action*)	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 *type*	Configured unbind action for LUs on this PU.
generic-pool *type*	Configured generic-pool for LUs on this PU.
ip-preced-screen *number*	IP precedence value for screen LUs on this PU.
ip-preced-printer *number*	IP precedence value for printer LUs on this PU.
ip-tos-screen *number*	IP Type of Service (ToS) value for screen LUs on this PU.

Table 45 show extended channel tn3270-server pu Field Descriptions (continued)

Field	Description
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 RU is sent by the TN3270 server when a client turns off the device or disconnects. The possible 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 VTAM to delete the corresponding LU when a client disconnects. The possible 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 *number/number*	Total number of bytes sent to/received from the host for this PU.
frames in / out *number/number*	Total number of frames sent to/received from the host for this PU.
NegRsp in / out *number/number*	Total number of SNA negative responses sent to/received from the host.
actlus *number*	Total number of ACTLUs received from the host.
dactlus *number*	Total number of DACTLUs received from the host.
binds *number*	Total number of BINDs received from the host.
lu *number*	LOCADDR of the LU.
name *lu-name*	Name of the TN3270 LU.
client-name *ip-addr:tcpport*	Client's IP address and TCP port number.
nail	Status of LU nailing, either Y or N

Table 45 show extended channel tn3270-server pu Field Descriptions (continued)

Field	Description
state *lu-state*	LU states and their meanings: • UNKNOWN—LU in an undefined state. • INACTIVE—LU didn't receive 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 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 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 *model*	IBM 3278 model type of client.
frames in *number*	Number of frames sent inbound to the host.
frames out *number*	Number of frames sent outbound from the host.
idle for *time*	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
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.
allocate lu	Assigns LUs to a pool.

show extended channel tn3270-server pu lu

To display information about the TN3270 server LUs running on CMCC adapter interface, use the **show extended channel tn3270-server pu lu** EXEC command.

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 *slot* 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	PU name that uniquely identifies this PU.
locaddr	LU LOCADDR that uniquely identifies the LU.
history	(Optional) Displays the LU trace history.

DefaultsDefaults

No default behavior or values.

Command Modes

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.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

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 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 171.69.176.77:3828    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 192.195.80.40:2480    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
```

This example shows the response-time information using the **show extended channel tn3270-server pu lu** command for the LU at LOCADDR 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 161.44.100.210:1315   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 46 describes significant fields in the display.

Table 46 show extended channel tn3270-server pu lu Field Descriptions

Field	Description
lu *locaddr*	LOCADDR of the LU.
name *lu-name*	Name of the TN3270 LU.
client-ip:tcp *ip-addr:tcpport*	Client's IP address and TCP port number.

Table 46 show extended channel tn3270-server pu lu Field Descriptions (continued)

Field	Description
state *lu-state*	LU states and their meanings are: • UNKNOWN—LU in an undefined state. • INACTIVE—LU didn't receive 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 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 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 *model*	3278 model type of client; blank if STATIC LU.
frames in *number*	Number of frames sent inbound to the host.
frames out *number*	Number of frames sent outbound from the host.
idle for *time*	Time the client has been idle. The time is in HH:MM:SS.
pu is *pu-name*	Name of the PU.
lu is *type*	Whether LU is DYNAMIC or STATIC.
negotiated *type*	Whether client is TN3270 or TN3270E.
bytes in/out *number/number*	Total number of bytes sent to or received from the host.
RuSize in/out *number/number*	RU size as configured in the bind.
NegRsp in/out *number/number*	Number of SNA negative responses sent to/received from the host.
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	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.

Table 46 show extended channel tn3270-server pu lu Field Descriptions (continued)

Field	Description
pacing window in/out *number/number*	SNA pacing window as configured in the bind.
credits in *number*	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue-size in *number*	If non-zero, indicates the number of SNA frames waiting to be sent to the host which are blocked, waiting for a pacing response.
queue-size out *number*	SNA frames not yet acknowledged by an isolated pacing response by the TN3270 server.

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** privileged EXEC command.

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 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.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

If optional keywords are not used for the **show extended channel tn3270-server response-time application** command, a complete list of currently existing per-application client groups is displayed along with their collection control parameters. If you specify the *appl-name* keyword, 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

Following is an example of output for the **show extended channel tn3270-server response-time application**:

```
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 47 provides descriptions of the output fields for the **show extended channel tn3270-server response-time application** command.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are currently configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 47 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 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.
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 information about the global client group, use the **show extended channel tn3270-server response-time global** privileged EXEC command.

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.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

The **show extended channel tn3270-server response-time global** command displays collection control parameters for the global client group.

Examples

Following is an example of output for 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 48 provides descriptions of the output fields for the **show extended channel tn3270-server response-time global** command.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are currently configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 48 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 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** privileged EXEC command.

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) PU name for a direct PU or link name for a 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.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

This command displays information clients groups by host link. If no optional keywords are specified, a complete list of currently 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

Following is an example of the output for the **show extended channel tn3270-server response-time link** command without optional keywords, which shows all current 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
```

Following is an example of the output for 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 49 provides descriptions of the output fields for the **show extended channel tn3270-server response-time link** command.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are currently configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 49 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 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.
average total response time	Displays the average response time (in tenths of seconds) for the total number of response-time transactions.

Table 49 show extended channel tn3270-server response-time link Field Descriptions (continued)

Field	Description
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** privileged EXEC command.

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.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

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

Following is an example of the output for the **show extended channel tn3270-server 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 50 provides descriptions of the output fields for the **show extended channel tn3270-server response-time listen-point** command.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are currently configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 50 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 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** privileged EXEC command.

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.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

This command shows information about client subnet client groups. This includes all configured groups plus 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* and *ip-mask* arguments, 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

Following is an example of the output for 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
```

Following is an example of the output for 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 51 provides descriptions of the output fields for the **show extended channel tn3270-server response-time subnet** command.

Note The aggregate, excludeip, and dynamic definite response field values are MIB parameters that are currently configured automatically by the TN3270 server according to the type of response-time group. These values are not configurable in the TN3270 server.

Table 51 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.
excludeip	Displays whether the IP component (the client/server path) is included in the response time for any transaction (NO) or if only the 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** EXEC command.

show extended channel *slot/virtual channel* **tn3270-server security** [[**sec-profile** *profilename*] [**listen-point** *ipaddress* [**tcp-port** *number*]]]

Syntax Description

slot	Specifies a particular CMCC adapter in the router where *slot* is the slot number.
virtual channel	Virtual channel number.
sec-profile *profilename*	(Optional) Alphanumeric name which 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 *ipaddress*	(Optional) 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 *number*	(Optional) Port number used for the listen operation. The default value is 23.

Defaults

The default **tcp-port** value is 23.

Command Modes

EXEC

Command History

Release	Modification
12.1(5)T	This command was introduced.

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 52 describes significant fields in the display.

Table 52 show extended channel tn3270-server security Field Descriptions

Field	Description
status *ENABLE/DISABLE*	Status of TN3270 server security. Enable or Disable.
Default Profile (*Not configured/configured)*	Shows 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*	Number of active LUs.
keylen *bits*	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. Choices 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.

shutdown (TN3270)

To shut down TN3270 entities, such as PU, DLUR, and DLUR SAP, use the **shutdown** command in one of the TN3270 server command modes. The **shutdown** TN3270 command shuts down the TN3270 entities according to which configuration mode you are in when the command is issued. 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 for the following configuration modes was added: • TN3270 • PU • DLUR • DLUR SAP
11.2(18)BC	Support for the following configuration modes was added: • Listen-point • Listen-point PU
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

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 SNA session switch configuration in the TN3270 server.

In DLUR SAP configuration mode, the command shuts down the local SAP 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
```

tcp-port

To override the default TCP port setting of 23, use the **tcp-port** TN3270 server configuration command. 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 of 0 to 65534. The default is 23, which is the IETF standard. The value 65535 is reserved by the TN3270 server.

Defaults

In TN3270 server configuration mode, the default is 23.

In PU configuration mode the default is the value currently configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration—The **tcp-port** command at this level applies to all PUs supported by the TN3270 server.

DLUR PU configuration—The **tcp-port** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **tcp-port** command at this level applies only to the specified PU.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **tcp-port** command is valid only on the virtual channel interface, and it 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. The **tcp-port** command affects only future TN3270 sessions.

The **no tcp-port** command entered in PU configuration mode removes the override.

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.

timing-mark

To select whether a WILL TIMING-MARK is transmitted when the host application needs an SNA response (definite or pacing response), use the **timing-mark** TN3270 server configuration command. 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.

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 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 CMCC adapter or to enter TN3270 server configuration mode, use the **tn3270-server** interface configuration command. 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.

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 DLUR and 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** TN3270 server configuration command. 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 PU configuration mode the default is the value currently configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration—The **unbind-action** command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **unbind-action** command at this level applies to all PUs defined at the listen point.

Listen-point PU configuration—The **unbind-action** command at this level applies only to the specified PU.

DLUR PU configuration—The **unbind-action** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **unbind-action** command at this level applies only to the specified PU.

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **unbind-action** command is valid only on the virtual channel interface. This command 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. The **unbind-action** command affects currently active and future TN3270 sessions.

The **no unbind-action** command entered in PU configuration mode removes the override.

The **unbind-action** command affects currently active and future TN3270 sessions.

Examples

The following example prevents automatic disconnect:

```
unbind-action keep
```

vrn

To tell the SNA session switch the connection network to which the internal adapter interface on the CMCC adapter belongs, use the **vrn** DLUR 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.

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). This 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 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 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 8 characters long; for example, RA12.NODM1PP. The portion of the name before the period is the NET ID and is shared between entities in the same logical network.

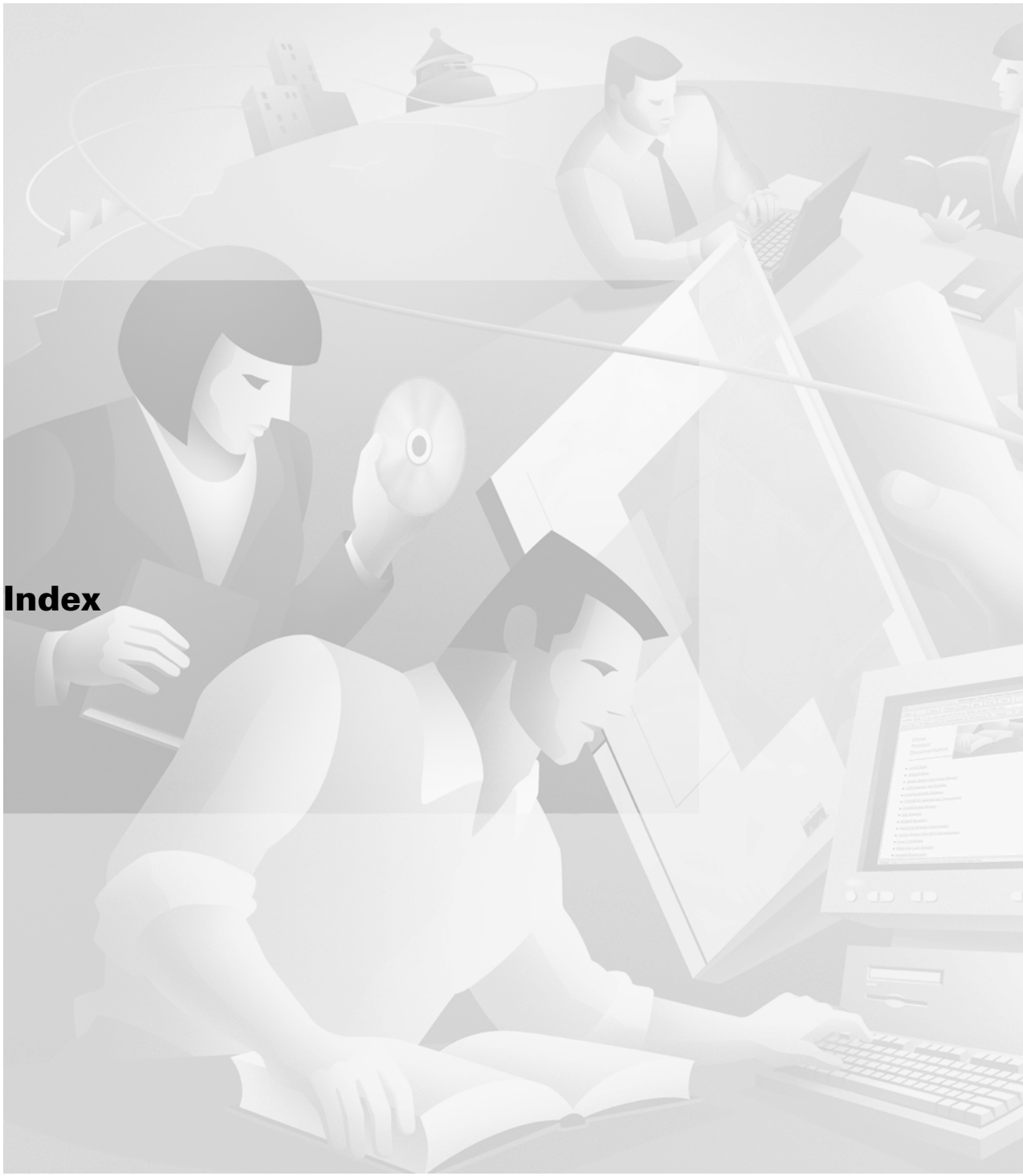
Examples

The following example sets a VRN name:

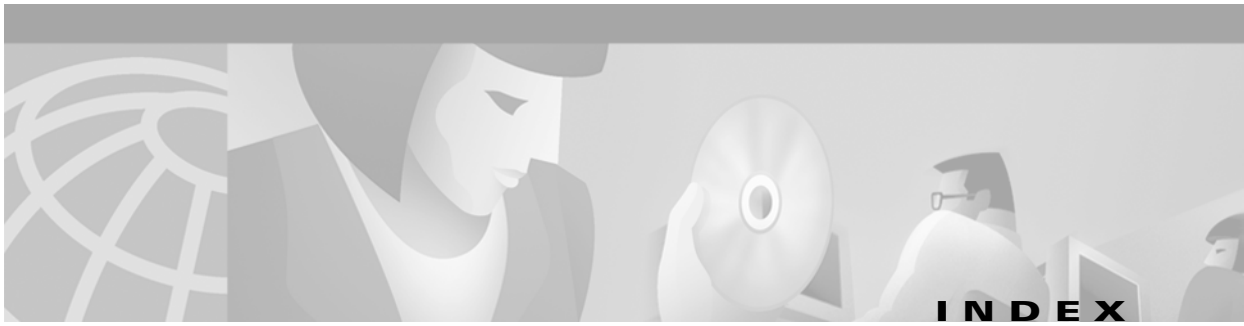
```
vrn SYD.BLAN25
```

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 SAP in the SNA session switch and enters DLUR SAP configuration mode.



Index



Symbols

<cr> xv
? command xiv

A

adapter command B2R-206
algorithms, security encryption B2R-339
allocate lu command B2R-316

C

carriage return (<cr>) xv
cautions, usage in text x
certificate reload command B2R-318
certificates, security
  reloading B2R-318
  specifying location of B2R-384
channel-protocol command B2R-208
CIP (Channel Interface Processor) data rate, PCA configuration B2R-208
Cisco IOS configuration changes, saving xviii
claw (backup) command B2R-269
CLAW (Common Link Access for Workstations)
  backup group, displaying B2R-282
  IP datagram configuration B2R-266, B2R-269, B2R-272
  IP host backup group configuration B2R-266
  packing connections, displaying B2R-283
  packing names, displaying B2R-283
  packing statistics, displaying B2R-285
claw command B2R-266
clear dbconn connection command B2R-154
clear dbconn statistic command B2R-155
clear extended counters command B2R-209
clear txconn connection command B2R-156
clear txconn statistic command B2R-157
clear txconn transaction command B2R-155
client, nailing to pool B2R-327
client ip command B2R-319
client ip lu command B2R-321
client ip pool command B2R-323, B2R-327
client lu maximum command B2R-325
client pool command B2R-327
CMCC (Cisco Mainframe Channel Connection) adapter
  channel interface
    hardware, displaying B2R-259
    physical, monitoring B2R-264
    shutting down B2R-263
    specification B2R-213
    statistics, displaying B2R-245
  channel statistics, displaying B2R-240
  CLAW configuration B2R-266, B2R-269, B2R-272
  CMPC
    configuration B2R-288
    subchannel, displaying B2R-294
    transmission group, displaying B2R-303, B2R-310
  CMPC+
    configuration B2R-288, B2R-312
    subchannel, displaying B2R-294
    transmission group, displaying B2R-303, B2R-310
  core dump, enabling B2R-211
  CSNA
    configuration B2R-290
    subchannel, displaying B2R-296

data rate parallel channel interface configuration B2R-208
DLUR (dependent logical unit requester) configuration B2R-333
DLUS backup configuration B2R-335
ICMP stack, displaying B2R-221
internal adapter
configuration B2R-206
internal adapters
naming B2R-218
VRN configuration B2R-439
internal LANs
configuration B2R-215
displaying B2R-227
IP host backup
offload device configuration B2R-277
path configuration B2R-280
IP stack, displaying B2R-223
LLC2 sessions
displaying B2R-229
maximum, displaying B2R-238
maximum specification B2R-217
SAP, displaying B2R-220
microcode version, displaying B2R-219
NN server, TN3270 server configuration B2R-368
SAP, LLC2 sessions, displaying B2R-220
sessions, TN3270 server configuration B2R-363
TCP/IP offload configuration B2R-275
TCP connections, displaying B2R-250
TCP stack, displaying B2R-253
TN3270 server configuration B2R-315 to B2R-440
UDP listener sockets, displaying B2R-256
UDP stack, displaying B2R-257
CMPC (Cisco Multipath Channel)
subchannel
configuration B2R-288
displaying B2R-294
transmission group, displaying B2R-303, B2R-310
CMPC+ (Cisco Multipath Channel+)
subchannel
configuration B2R-288
displaying B2R-294
TG connection manager, displaying B2R-292
transmission group
configuration B2R-312
displaying B2R-303, B2R-310
cmpc command B2R-288
command modes, understanding xiii to xiv
commands
context-sensitive help for abbreviating xiv
default form, using xvii
no form, using xvii
command syntax
conventions ix
displaying (example) xv
configurations, saving xviii
CPA (Channel Port Adapter) data rate, PCPA configuration B2R-208
creating security profile B2R-369
CSNA (Cisco SNA) subchannel
configuration B2R-290
displaying B2R-296
csna command B2R-290

D

dbconn license command B2R-160
dbconn pem command B2R-162
dbconn ping command B2R-163
dbconn server command B2R-164
dbconn tcpserver command B2R-167
debug dbconn command B2R-170
default profile, specifying B2R-330
default-profile command B2R-330
digital certificates, reloading B2R-318
disable (TN3270) command B2R-332
disabling security, TN3270 server B2R-332
DLUR (dependent logical unit requester) TN3270 server

displaying B2R-395, B2R-398
dlur command B2R-333
DLUS backup, TN3270 server configuration B2R-335
dlus-backup command B2R-335
documentation
conventions ix
feedback, providing xi
modules v to vii
online, accessing x
ordering xi
Documentation CD-ROM x
documents and resources, supporting viii
domain ID, specifying B2R-336
domain-id command B2R-336
DSPU (downstream physical unit)
activation request units, defining B2R-4
default PU, defining B2R-5
Ethernet
host, defining B2R-19
LSAP address, enabling B2R-10
PUs, defining B2R-34
upstream host B2R-7
FDDI
host, defining B2R-19
LSAP address, enabling B2R-10
PUs, defining B2R-34
upstream host B2R-7
Frame Relay
host, defining B2R-13
LSAP address, enabling B2R-10
PUs, defining B2R-28
upstream host B2R-7
LAN, naming B2R-53
LU pool, defining B2R-26
LUs
defining B2R-21
inactivity timeout specification B2R-26
monitoring B2R-54
NCIA server
configuration B2R-23
PUs, defining B2R-34
SAP, enabling B2R-24
notification level specification B2R-25
PUs
Ethernet, defining B2R-34
FDDI, defining B2R-34
NCIA server, defining B2R-34
RSRB, defining B2R-34
Token Ring, defining B2R-34
VDLC, defining B2R-34
QLLC
host, defining B2R-15
PUs, defining B2R-30
upstream host B2R-8
X.121 subaddress, enabling B2R-11
RSRB
defining B2R-37
host, defining B2R-19
PUs, defining B2R-34
SAP, enabling B2R-39, B2R-40
starting B2R-41
SAP, VDLC, enabling B2R-47, B2R-49
SDLC
address, enabling B2R-12
host, defining B2R-17
PUs, defining B2R-32
upstream host B2R-9
starting B2R-43
Token Ring
host, defining B2R-19
LSAP address, enabling B2R-10
PUs, defining B2R-34
upstream host B2R-7
VDLC
defining B2R-45
host, defining B2R-19
PUs, defining B2R-34
SAP, enabling B2R-47

starting B2R-51

dspu activation-window command B2R-4

dspu default-pu command B2R-5

dspu enable-host (QLLC) command B2R-8

dspu enable-host (SDLC) command B2R-9

dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay) command B2R-7

dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI) command B2R-10

dspu enable-pu (QLLC) command B2R-11

dspu enable-pu (SDLC) command B2R-12

dspu host (Frame Relay) command B2R-13

dspu host (QLLC) command B2R-15

dspu host (SDLC) command B2R-17

dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC) command B2R-19

dspu lu command B2R-21

dspu ncia command B2R-23

dspu ncia enable-pu command B2R-24

dspu notification-level command B2R-25

dspu pool command B2R-26

dspu pu (Frame Relay) command B2R-28

dspu pu (QLLC) command B2R-30

dspu pu (SDLC) command B2R-32

dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA) command B2R-34

dspu rsrb command B2R-37

dspu rsrb enable-host command B2R-39

dspu rsrb enable-pu command B2R-40

dspu rsrb start command B2R-41

dspu start command B2R-43

dspu vdlc command B2R-45

dspu vdlc enable-host command B2R-47

dspu vdlc enable-pu command B2R-49

dspu vdlc start command B2R-51

E

enable (TN3270) command B2R-338

enabling security, TN3270 server B2R-338, B2R-383

encryption

security algorithm B2R-339

session key B2R-351

encryptorder command B2R-339

Ethernet, SNA service point

defining B2R-66

enabling B2R-59

exception slot command B2R-211

F

FDDI (Fiber Distributed Data Interface), SNA service point

defining B2R-66

enabling B2R-59

Feature Navigator

See platforms supported

filtering output, show and more commands xviii

Frame Relay, SNA service point

defining B2R-60

enabling B2R-59

G

generic-pool command B2R-340

global configuration mode, summary of xiv

H

hardware platforms

See platforms supported

help command xiv

I

ICMP stack, CMCC adapter B2R-221

idle-time command B2R-342

indexes, master viii

interface channel command B2R-213

interface configuration mode, summary of xiv
internal adapters
  CMCC adapter, naming B2R-218
  VRN configuration B2R-439
internal LANs, CMCC adapter
  configuration B2R-215
  displaying B2R-227
IP addresses
  CMCC adapter offload device B2R-275
  TN3270 server
    configuration B2R-354
    displaying B2R-401
IP datagram, CMCC adapter configuration B2R-266, B2R-269, B2R-272
IP host backup
  CLAW configuration B2R-266
  CMCC adapter path configuration B2R-280
  TCP/IP offload configuration B2R-277
IP precedence, TN3270 server configuration B2R-344
ip precedence command B2R-344
IP stack, CMCC adapter, displaying B2R-223
IP ToS, TN3270 server configuration B2R-346
ip tos command B2R-346

K

keepalive (TN3270) command B2R-348
keylen command B2R-351

L

lan command B2R-215
lan-name command B2R-53
link (TN3270) command B2R-352
listen point, associating a security profile with B2R-381
listen-point command B2R-354
LLC2 sessions, CMCC adapter B2R-229, B2R-238
lsap command B2R-357
lu deletion command B2R-359
LU nailing, TN3270 server
  configuration B2R-321
  displaying B2R-401
  pool B2R-323, B2R-327
LU pools
  assigning LUs B2R-316
  DSPU, defining B2R-26
  TN3270 server
    configuration B2R-365
    displaying B2R-404, B2R-430
    nailing B2R-323, B2R-327
LUs (logical units)
  DSPU
    activation failure notification B2R-25
    dedicating to host B2R-21
    defining B2R-21
    inactivity timeout specification B2R-26
    pool assignment B2R-21
    state change notification B2R-25
  TN3270 server
    assigning B2R-316
    displaying B2R-404, B2R-411, B2R-430
lu termination command B2R-361

M

maximum bit length, session encryption key B2R-351
maximum-lus command B2R-363
max-llc2-sessions command B2R-217
MIB, descriptions online viii
modes
  See command modes

N

nailing client to pool B2R-327
name command B2R-218
NN server, TN3270 server configuration B2R-368

notes, usage in text x

O

offload (backup) command B2R-277
offload alias command B2R-275
offload command B2R-272

P

path command B2R-280
physical channel interface monitoring B2R-264
ping sna command B2R-78
platforms supported
  Feature Navigator, identify using xix
  release notes, identify using xix
pool command B2R-365
preferred-nnserver command B2R-368
privileged EXEC mode, summary of xiv
profile command B2R-369
profiles
  default, specifying B2R-330
  security
    associating with listen point B2R-381
    creating B2R-369
    modifying B2R-369
prompts, system xiv
pu (DLUR) command B2R-371
pu (listen-point) command B2R-372
pu (TN3270) command B2R-374
pu dlur (listen-point) command B2R-376
PUs (physical units)
  DSPU
    activation failure notification B2R-25
    Ethernet, defining B2R-34
    FDDI, defining B2R-34
    Frame Relay, defining B2R-28
    NCIA server, defining B2R-34
    QLLC, defining B2R-30
    RSRB, defining B2R-34
    SDLC, defining B2R-32
    state change notification B2R-25
    Token Ring, defining B2R-34
    VDLC, defining B2R-34
  TN3270 server
    configuration B2R-372, B2R-374
    displaying B2R-385, B2R-404, B2R-430
    DLUR, configuring B2R-376

Q

QLLC (Qualified Logical Link Control), SNA service point
  defining B2R-62
  enabling B2R-57
question mark (?) command xiv

R

release notes
  See platforms supported
reloading, digital certificates B2R-318
REPLY-PSID poweroff request, TN3270 server configuration B2R-359
response-time group, TN3270 server
  client subnet configuration B2R-319
  displaying B2R-415, B2R-418, B2R-420
response-time group command B2R-379
RFC
  full text, obtaining viii
ROM monitor mode, summary of xiv
RSRB (remote source-route bridging)
  DSPU
    defining B2R-37
    starting B2R-41
  SNA service point
    defining B2R-66

SAP, enabling B2R-69
starting B2R-70

S

SAP (Service Access Point)
DSPU
NCIA server, enabling B2R-24
RSRB, enabling B2R-39, B2R-40
VDLC, enabling B2R-49
SNA service point, RSRB, enabling B2R-69
TN3270 server configuration B2R-357
SDLC (Synchronous Data Link Control), SNA service point
defining B2R-64
enabling B2R-58
sec-profile command B2R-381
security (TN3270) command B2R-383
security, TN3270 server
disabling B2R-332
enabling B2R-338, B2R-383
modifying B2R-383
security certificates, specifying location of B2R-384
security encryption algorithm, specifying B2R-339
security profile
associating with listen point B2R-381
creating B2R-369
modifying B2R-369
servercert command B2R-384
session encryption key, maximum bit length B2R-351
show controllers channel command B2R-219
show dbconn connection command B2R-170
show dbconn license command B2R-173
show dbconn ports command B2R-174
show dbconn server command B2R-175
show dbconn statistic command B2R-178
show dbconn wlm command B2R-181
show dspu command B2R-54
show extended channel backup command B2R-282
show extended channel cmgr command B2R-292
show extended channel cmpc command B2R-294
show extended channel connection-map llc2 command B2R-220
show extended channel csna command B2R-296
show extended channel icmp-stack command B2R-221
show extended channel ip-stack command B2R-223
show extended channel lan command B2R-227
show extended channel llc2 command B2R-229
show extended channel max-llc2-sessions command B2R-238
show extended channel packing names command B2R-283
show extended channel packing stats command B2R-285
show extended channel statistics command B2R-240
show extended channel subchannel command B2R-245
show extended channel tcp-connections command B2R-250
show extended channel tcp-stack command B2R-253
show extended channel tg command B2R-303, B2R-310
show extended channel tn3270-server client-ip-address command B2R-389
show extended channel tn3270-server client-name command B2R-392
show extended channel tn3270-server command B2R-385
show extended channel tn3270-server dlur command B2R-395
show extended channel tn3270-server dlurlink command B2R-398
show extended channel tn3270-server nailed-domain command B2R-400
show extended channel tn3270-server nailed-ip command B2R-401
show extended channel tn3270-server nailed-name command B2R-403
show extended channel tn3270-server pu command B2R-404, B2R-430
show extended channel tn3270-server pu lu command B2R-411
show extended channel tn3270-server response-time application command B2R-415
show extended channel tn3270-server response-time global command B2R-418

show extended channel tn3270-server response-time link command B2R-420
show extended channel tn3270-server security command B2R-430
show extended channel udp-listeners command B2R-256
show extended channel udp-stack command B2R-257
show extended max-llc2-sessions command B2R-238
show interfaces channel command B2R-259
show sna command B2R-56
show snasw class-of-service command B2R-80
show snasw connection-network command B2R-81
show snasw directory command B2R-82
show snasw dlctrace command B2R-84
show snasw dlus command B2R-86
show snasw ipstrace command B2R-88
show snasw link command B2R-89
show snasw lu command B2R-91
show snasw mode command B2R-93
show snasw node command B2R-94
show snasw pdlog command B2R-96
show snasw port command B2R-97
show snasw pu command B2R-99
show snasw rtp command B2R-101
show snasw session command B2R-103
show snasw statistics command B2R-105
show snasw summary-ipstrace command B2R-107
show snasw topology command B2R-109
show txconn connection command B2R-182
show txconn destination command B2R-184
show txconn license command B2R-185
show txconn route command B2R-186
show txconn server command B2R-187
show txconn statistic command B2R-189
show txconn transaction command B2R-193
shutdown (CMCC) command B2R-263
shutdown (TN3270) command B2R-432
SNA (Systems Network Architecture)
  DSPU notification specification B2R-25
  RSRB configuration B2R-68
  session switching
    TN3270 server, displaying B2R-395, B2R-398
    TN3270 server configuration B2R-333, B2R-357, B2R-439
sna enable-host (QLLC) command B2R-57
sna enable-host (SDLC) command B2R-58
sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI) command B2R-59
sna host (Frame Relay) command B2R-60
sna host (QLLC) command B2R-62
sna host (SDLC) command B2R-64
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC) command B2R-66
sna rsrb command B2R-68
sna rsrb enable-host command B2R-69
sna rsrb start command B2R-70
SNA service point
  Ethernet
    defining B2R-66
    enabling B2R-59
  FDDI
    defining B2R-66
    enabling B2R-59
  Frame Relay
    defining B2R-60
    enabling B2R-59
  monitoring B2R-56
  QLLC
    defining B2R-62
    enabling B2R-57
  RSRB
    defining B2R-66
    SAP, enabling B2R-69
    starting B2R-70
  SDLC
    defining B2R-64
    enabling B2R-58
  starting B2R-71
  Token Ring
    defining B2R-66

enabling B2R-59
VDLC
defining B2R-66, B2R-72
SAP, enabling B2R-74
starting B2R-75
sna start command B2R-71
snasw cpname command B2R-111
snasw dlcfilter command B2R-113
snasw dlctrace command B2R-115
snasw dlus command B2R-117
snasw dump command B2R-119
snasw event command B2R-121
snasw ip-precedence command B2R-122
snasw ipsfilter command B2R-123
snasw ipstrace command B2R-125
snasw link command B2R-127
snasw location command B2R-130
snasw mode command B2R-132
snasw msgdump command B2R-133
snasw pathswitch command B2R-134
snasw pdlog command B2R-135
snasw port command B2R-137
snasw rtp pathswitch-timers command B2R-142
snasw start command B2R-143
snasw start cp-cp command B2R-144
snasw start link command B2R-145
snasw start port command B2R-146
snasw stop command B2R-147
snasw stop cp-cp command B2R-148
snasw stop link command B2R-149
snasw stop port command B2R-150
snasw stop session command B2R-151
sna vdlc command B2R-72
sna vdlc enable-host command B2R-74
sna vdlc start command B2R-75
SNMP (Simple Network Management Protocol), DSPU notification specification B2R-25
state-tracks-signal command B2R-264

T

Tab key, command completion xiv
TCP/IP offload
backup group, displaying B2R-282
IP address configuration B2R-275
TCP connections, B2R-250
TCP port, TN3270 server configuration B2R-434
tcp-port command B2R-434
TCP stack, CMCC adapter, displaying B2R-253
Telnet nops, TN3270 server configuration B2R-348
TERMSELF request, TN3270 server configuration B2R-361
tg (CMPC) command B2R-310
tg (CMPC+) command B2R-312
TG connection manager, CMPC+, displaying B2R-292
timing-mark command B2R-435
timing marks, TN3270 server configuration B2R-348, B2R-435
TN3270 server
clients, displaying B2R-389, B2R-392
configuration, displaying B2R-385
configuration mode, entering B2R-437
DLUR
configuration B2R-333
displaying B2R-395, B2R-398
DLUS backup configuration B2R-335
domain ID B2R-336
generic pool LU configuration B2R-340
host link configuration B2R-352
idle time configuration B2R-342
IP addresses
configuration B2R-354
displaying B2R-401
IP precedence configuration B2R-344
IP TOS configuration B2R-346
listen points configuration B2R-354
LU deletion B2R-359
LU nailing

configuration B2R-321
displaying B2R-401
pool, configuring B2R-327
pool configuration B2R-323
LU pool
assigning LUs B2R-316
client, nailing B2R-323, B2R-327
configuration B2R-365
displaying B2R-404, B2R-430
LUs, displaying B2R-404, B2R-411, B2R-430
LU sessions, limiting, per client B2R-325
LU termination B2R-361
nailed name, displaying B2R-403
nailing statements, displaying B2R-400
PUs
direct configuration B2R-372, B2R-374
displaying B2R-385, B2R-404, B2R-430
DLUR, configuring B2R-376
response-time group
client subnet configuration B2R-319
configuration B2R-379
displaying B2R-415, B2R-418, B2R-420
SAP configuration B2R-357
security
certificates, location of B2R-384
disabling B2R-332, B2R-383
enabling B2R-338, B2R-383
session disconnection idle time configuration B2R-342
session encryption key B2R-351
session maximum configuration B2R-363
session termination B2R-359, B2R-361
shutting down B2R-432
SNA session switch
configuration B2R-439
displaying B2R-395, B2R-398
SNA session switch configuration B2R-333
starting B2R-437
TCP port configuration B2R-434
Telnet nops configuration B2R-348
timing marks configuration B2R-348, B2R-435
UNBIND request configuration B2R-438
tn3270-server command B2R-437
Token Ring, SNA service point
defining B2R-66
enabling B2R-59
txconn destination command B2R-196
txconn license command B2R-198
txconn ping command B2R-200
txconn route command B2R-201
txconn server command B2R-202

U

UDP listener sockets, CMCC adapter B2R-256
UDP stack, CMCC adapter B2R-257
unbind-action command B2R-438
UNBIND request, TN3270 server configuration B2R-361
UNBIND response, TN3270 server configuration B2R-438
user EXEC mode, summary of xiv

V

VDLC (Virtual Data Link Control)
DSPU
defining B2R-45
SAP, enabling B2R-47, B2R-49
starting B2R-51
SNA service point
defining B2R-66, B2R-72
SAP, enabling B2R-74
starting B2R-75
vrn command B2R-439