Router Products Command Summary

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

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

Digital Equipment Corporation makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

THESE MANUALS AND THE SOFTWARE OF THE ABOVE-LISTED SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. DIGITAL AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL DIGITAL 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 DIGITAL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Notice of Restricted Rights:

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

TABLE OF CONTENTS

vines access-list *access-list-number* {**deny** | **permit**} *protocol source-address source-mask* [*source-port source-port-mask*] *destination-address destination-mask* [*destination-port destination-port-mask*]
no vines access-list *access-list-number 285*

vines access-list *access-list-number* {**deny** | **permit**} *source-address source-mask*
no vines access-list *access-list-number 288*

[no] vines arp-enable [dynamic] 288

[no] vines decimal 289

vines encapsulation [arpa | snap | vines-tr]
no vines encapsulation 289

vines host *name address*
no vines host *name 289*

vines **input-network-filter** *access-list-number*
no vines **input-network-filter 290**

vines **input-router-filter** *access-list-number*
no vines **input-router-filter 290**

vines metric [*whole* [fractional]]
no vines metric 290

vines neighbor *address mac-address encapsulation* [*whole* [*fractional*]]
no vines neighbor *address mac-address 291*

vines **output-network-filter** *access-list-number*
no vines **output-network-filter 292**

[no] vines propagate [dynamic] 292

vines redirect [*seconds*]
no vines redirect 293

[no] vines route *number address* [*whole* [*fractional*]] 293

[no] vines route-cache 293

vines routing [*address* | **recompute**]
no vines routing 294

[no] vines serverless [dynamic | broadcast] 294

[no] vines split-horizon 294

[no] vines srtp-enabled 294

vines time access-group *access-list-number*
no vines time access-group 295

vines time destination *address*
no vines time destination 295

[no] vines time participate 295

[no] vines time set-system 295

[no] default-information originate [always] [metric *metric-value*]
[metric-type *type-value*] {level-1 | level-1-2 | level-2}
[route-map *map-name*] 368

[no] default-metric *number 370*

[no] default-metric *bandwidth delay reliability loading mtu 370*

[no] distance *weight* [*address mask* [*access-list-number*]] [ip] 371

distance bgp *external-distance internal-distance local-distance*
no distance bgp 372

distance eigrp *internal-distance external-distance*
no distance eigrp 373

[no] distribute-list *access-list-number* in [*interface-name*] 373

[no] distribute-list *access-list-number* out [*interface-name* |
routing-process | *autonomous-system-number*] 374

[no] domain-password [*password*] 374

[no] ip address address *mask* [secondary] 374

[no] ip as-path access-list *access-list-number* {permit | deny}
as-regular-expression 375

ip community-list *community-list-number* {permit | deny}
community-number
no ip community-list *community-list-number 375*

[no] ip default-network *network-number 376*

[no] ip dvmrp accept-filter *access-list-number* [*distance*] 376

ip dvmrp default-information {originate | only}
no ip dvmrp default-information {originate | only} 377

[no] ip dvmrp metric *metric* [*access-list-number*] [*protocol process-id*] 377

ip gdp [priority *number* | reporttime *seconds* | holdtime *seconds*]
no ip gdp 378

[no] ip hello-interval eigrp *autonomous-system-number seconds 379*

[no] ip hold-time eigrp *autonomous-system-number seconds 379*

[no] ip igmp access-group *access-list-number 379*

[no] ip igmp join-group *group-address 380*

ip igmp query-interval *seconds*
no ip igmp query-interval 380

ip irdp [multicast | holdtime *seconds* | maxadvertinterval *seconds* |
minadvertinterval *seconds* | preference *number* | address *addres*s
[*number*]]
no ip irdp 380

[no] ip multicast-routing 381

[no] clns cluster-alias 434

clns configuration-time *seconds*
no clns configuration-time 434

clns congestion-threshold *number*
no clns congestion-threshold 434

[no] clns dec-compatible 434

[no] clns enable 435

[no] clns erpdu-interval *milliseconds 435*

[no] clns esct-time *seconds 435*

clns es-neighbor *nsap snpa*
no clns es-neighbor *nsap 435*

clns filter-expr ename term
clns filter-expr ename not term
clns filter-expr ename term or term
clns filter-expr ename term and term
clns filter-expr ename term xor term
no clns filter-expr ename 436

clns filter-set sname [permit | deny] template
no clns filter-set sname 437

clns holding-time *seconds*
no clns holding-time 437

clns host *name nsap 438*

clns is-neighbor *nsap snpa*
no clns is-neighbor *nsap 438*

clns mtu *size*
no clns mtu 438

[no] clns net {*net-address* | *name*} 439

[no] clns net {*nsap-address* | *name*} 439

clns packet-lifetime *seconds*
no clns packet-lifetime 439

[no] clns rdpdu-interval *milliseconds 440*

clns route *nsap-prefix type number* [*snpa-address*]
no clns route *nsap-prefix 440*

clns route *nsap-prefix* {*next-hop-net* | *name*}
no clns route *nsap-prefix 441*

clns route default *nsap-prefix type number*
no clns route default 441

clns route *nsap-prefix* discard
no clns route *nsap-prefix 442*

[no] clns route-cache 442

[no] ipx hold-time eigrp *autonomous-system-number seconds 480*

[no] ipx input-network-filter *access-list-number 481*

[no] ipx input-sap-filter *access-list-number 481*

ipx internal-network *network-number*
no internal-network [*network-number*] 481

ipx ipxwan [*local-node* {*network-number* | unnumbered}
local-server-name retry-interval retry-limit]
no ipxwan 482

[no] ipx ipxwan error [shutdown | reset | resume] 483

[no] ipxwan static 484

[no] ipx link-delay *microseconds 484*

[no] ipx maximum-hops *hops 484*

ipx maximum-paths *paths*
no ipx maximum-paths 484

[no] ipx netbios input-access-filter {host | bytes} *name 485*

[no] ipx netbios output-access-filter {host | bytes} *name 485*

ipx network *number* [encapsulation *encapsulation-type* [secondary]]
no ipx network *number* [encapsulation *encapsulation-type*] 486

[no] ipx nlsp csnp-interval *seconds 488*

[no] ipx nlsp enable 488

[no] ipx nlsp hello-interval *seconds 488*

[no] ipx nlsp metric *metric-number 489*

[no] ipx nlsp priority *priority-number 489*

[no] ipx nlsp retransmit-interval *seconds 489*

[no] ipx nlsp rip [on | off | auto] 490

[no] ipx nlsp sap [on | off | auto] 490

[no] ipx output-gns-filter *access-list-number 491*

[no] ipx output-network-filter *access-list-number 491*

ipx output-rip-delay *delay*
no ipx output-rip-delay 492

ipx output-sap-delay delay
no ipx output-sap-delay 492

[no] ipx output-sap-filter *access-list-number 492*

[no] ipx pad-process-switched-packets 493

[no] ipx ping-default {cisco | novell}
To select the ping type that the router transmits, use the **ipx ping-default** global configuration command. To return to the default ping type, use the **no** form of this command. 493

[no] locaddr-priority-list *list-number address-number queue-keyword* [*dsap ds*] [*dmac dm*] 552

mac-address *ieee-address 552*

[no] multiring {*protocol-keyword* | all | other} 553

[no] netbios access-list bytes name {permit | deny} offset pattern 553

[no] netbios access-list host *name* {permit | deny} *pattern 554*

[no] netbios enable-name-cache 555

[no] netbios input-access-filter bytes name 555

[no] netbios input-access-filter host name 555

netbios name-cache mac-address netbios-name {*in*terface-name |
ring-group group-number}
no netbios name-cache *mac-address netbios-name 555*

netbios name-cache name-len length 556

netbios name-cache proxy-datagram seconds 556

netbios name-cache query-timeout *seconds*
no netbios name-cache query-timeout 557

netbios name-cache recognized-timeout *seconds*
no netbios name-cache recognized-timeout 557

[no] netbios name-cache **timeout** *minutes 557*

[no] netbios output-access-filter bytes name 558

[no] netbios output-access-filter host name 558

[no] priority-group *list 558*

priority-list *list-number* protocol *protocol-name queue-keyword*
no priority-list *list-number address-number queue-keyword 558*

rif *mac-address rif-string* {*interface-name* | ring-group *ring*}
no rif *mac-address* {*interface-name* | ring-group *ring*} 559

rif timeout *minutes*
no rif timeout 560

rif validate-age seconds 560

rsrb remote-peer ring-group tcp ip-address lsap-output-list
access-list-number
rsrb remote-peer ring-group fst ip-address lsap-output-list
access-list-number
rsrb remote-peer ring-group interface interface-name lsap-output-list
access-list-number 560

rsrb remote-peer ring-group tcp ip-address netbios-output-list name
rsrb remote-peer ring-group fst ip-address netbios-output-list name
rsrb remote-peer ring-group interface interface-name
netbios-output-list host 561

LLC2 and SDLC Commands 587

Introduction

This document provides a summary of the commands used to configure routers. This book is divided into sections that correspond to the chapters of the *Router Products Command Reference* publication. Within each section the commands are listed in alphabetical order. The table of contents shows the sections in this book; the index lists all the commands in alphabetical order, without regard to the section where they are located. See the *Router Products Command Reference* publication for complete command descriptions and examples.

Conventions

This document uses the following conventions:

- The symbol ^ and the text Ctrl represent the key labeled *Control*.

  For example, the key combination ^*D* or Ctrl-D mean hold down the *Control* key while you press the *D* key.

- A string is defined as a nonquoted set of characters.

  For example, when setting up a community string for SNMP to "public," do not use quotes around the string, or the string will include the quotation marks.

Command descriptions use the following conventions:

- Vertical bars (|) separate alternative, mutually exclusive, elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) indicate a required choice.
- Braces within square brackets ([{ }]) indicate a required choice within an optional element.
- **Boldface** indicates commands and keywords that are entered literally as shown.

- *Italics* indicate arguments for which you supply values; in contexts that do not allow italics, arguments are enclosed in angle brackets (< >).
- If the **no** form of a command has exactly the same keywords and arguments as the command, **no** appears in square brackets at the beginning of the command line. If the **no** form of a command does not have all the same keywords and arguments, the **no** form is displayed separately.
- If the **no** form of a command is not explicitly explained in the description, it negates the command.

EXEC System Use

- Enter commands by typing their names at the EXEC prompt and pressing the Return key.
- There are two EXEC prompt levels. The user-level prompt is the server name followed by an angle bracket (>), as in this example:

  ```
  Router>
  ```

  There is also a privileged-level prompt available to the system administrator by entering a password. It is the server name followed by a pound sign (#), as in this example:

  ```
  Router#
  ```

- Use the following editing commands when typing commands at the EXEC prompt:

  — Delete or Backspace to erase characters

  — Ctrl-U to delete a line

- As a shortcut, you can abbreviate commands to the fewest letters that make them unique. The letters “sho” can be entered for the **show** command, for example.

- Certain EXEC commands display multiple screens with this prompt at the bottom of the screen:

  ```
  --More--
  ```

  Press the space bar to continue the output or press Return to display the next line. Press any other key to return to the prompt.

System Help

You can obtain help when entering commands by using the following methods:

- For a brief description of the context-sensitive help system, type **help**.
- To list all commands for a command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that start with a particular character set, enter an abbreviated command immediately followed by a question mark (?).
- To list a command's keywords or arguments, enter a question mark (?) in place of a keyword or argument on the command line.
- At any time during an active Telnet session, you can list the Telnet commands by typing the following command at the system prompt:

  Ctrl-^ ?

  Press the Ctrl, Shift, and 6 keys simultaneously, let go, and type **?**.

User Interface Commands

This chapter describes the function and displays the syntax of each command used to enter and exit the command modes supported by the Internetwork Operating System (IOS). For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

disable

To exit privileged EXEC mode and return to user EXEC mode, enter the **disable** EXEC command.

[**no**] editing

To enable enhanced editing mode for a particular line, use the **editing** line configuration command. To disable the enhanced editing mode, use the **no** form of this command.

enable

To enter privileged EXEC mode, use the **enable** EXEC command.

end

To exit configuration mode, use the **end** global configuration command.

exit

To exit any command mode or close an active terminal session and terminate the EXEC, use the **exit** command at the system prompt.

full-help

To get help for the full set of user-level commands, use the **full-help** line configuration command.

help

To display a brief description of the help system, enter the **help** command.

[**no**] **history** [**size** *number-of-lines*]

To enable the command history function, or to change the command history buffer size for a particular line, use the **history** line configuration command. To disable the command history feature, use the **no** form of this command.

size *number-of-lines*	Number of command lines that the system will record in its history buffer. The range is 0 to 256.

show history

To list the commands you have entered in the current EXEC session, use the **show history** EXEC command.

User Interface Commands

9

System Image, Microcode Image, and Configuration File Load Commands

This chapter describes the function and displays the syntax of each command used to load and copy system images, microcode images, and configuration files. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

boot
boot *filename* [*ip-address*]
boot flash [*filename*]
boot flash [*device***:**]*partition-number***:**[*filename*]

To boot the router manually, use the **boot** ROM monitor command.

filename — Name of the system image you want to netboot.

ip-address — (Optional) IP address of the TFTP server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

flash *filename* — (Optional) Boots the router from Flash memory with the optional filename of the image you want loaded. The filename is case sensitive. Without a filename, the first valid file in Flash memory is loaded.

*device***:** — (Optional) Valid value is **flash**.

*partition-number***:** — Boots the router from Flash memory with the optional filename of the image you want loaded from the specified Flash partition. If you do not specify a filename, the first valid file in the specified partition of Flash memory is loaded.

[**no**] **boot bootstrap flash** [*filename*]
[**no**] **boot bootstrap mop** *filename* [*mac-address*] [*interface*]
[**no**] **boot bootstrap** [**tftp**] *filename* [*ip-address*]

To configure the filename that is used to boot a secondary bootstrap image, use the **boot bootstrap** global configuration command. Use the **no** form of this command to disable booting from a secondary bootstrap image.

flash Indicates that the router will be booted from Flash memory.

mop Indicates that the router will be netbooted from a system image stored on a Digital MOP server.

tftp (Optional) Indicates that the router will be netbooted from a system image stored on a TFTP server.

filename (Optional with **flash**) Name of the system image from which you want to netboot. If you omit the filename when booting from Flash, the router uses the first system image stored in Flash memory.

ip-address (Optional) IP address of the TFTP server on which the system image resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

mac-address (Optional) MAC address of the MOP server on which the file resides. If the MAC address argument is not included, a broadcast message is sent to all MOP boot servers. The first MOP server to indicate that it has the file will be the server from which the router gets the boot image.

interface (Optional) Interface out which the router should send MOP requests to reach the MOP server. The interface options are **async**, **dialer**, **ethernet**, **loopback**, **null**, **serial**, and **tunnel**. If the interface argument is not specified, a request will be sent on all interfaces that have MOP enabled, and the interface out which the first response is received will be used to load the software.

boot buffersize *bytes*
no boot buffersize

To modify the buffer size used to load configuration files, use the **boot buffersize** global configuration command. Use the **no** form of this command to return to the default setting.

bytes Specifies the size of the buffer to be used. There is no minimum or maximum buffer size.

[**no**] **boot host mop** *filename* [*mac-address*] [*interface*]
[**no**] **boot host** [**tftp | rcp**] *filename* [*ip-address*]

To change the default name of the host configuration filename from which you want to load configuration commands, use the **boot host** global configuration command. Use the **no** form of this command to restore the host configuration filename to the default.

mop Indicates that the router will be configured from a configuration file stored on a Digital MOP server.

tftp (Optional) Indicates that the router will be configured from a configuration file stored on a TFTP server.

rcp (Optional) Indicates that the router will be configured from a configuration file stored on a rcp server.

filename Name of the file from which you want to load configuration commands.

ip-address (Optional) IP address of the TFTP server on which the file resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

mac-address (Optional) MAC address of the MOP server on which the file resides. If the MAC address argument is not included, a broadcast message is sent to all MOP boot servers. The first MOP server to indicate that it has the file is the server from which the router gets the boot image.

interface (Optional) Interface out which the router should send MOP requests to reach the MOP server. The interface options are **async**, **dialer**, **ethernet**, **serial**, and **tunnel**. If the interface argument is not specified, a request is sent on all interfaces that have MOP enabled, and the interface out which the first response is received is used to load the software.

[**no**] **boot network mop** *filename* [*mac-address*] [*interface*]
[**no**] **boot network** [**tftp** | **rcp**] *filename* [*ip-address*]

To change the default name of the network configuration file from which you want to load configuration commands, use the **boot network** global configuration command. Use the **no** form of this command to restore the network configuration filename to the default.

mop Configures the router to download the configuration file from a network server using the Digital MOP protocol.

rcp (Optional) Configures the router to download the configuration file from a network server using rcp. If omitted, defaults to **tftp**.

tftp (Optional) Configures the router to download the configuration file from a network server using TFTP. If omitted and **rcp** is not specified, defaults to **tftp**.

filename Name of the file from which you want to load configuration commands. The default filename is *network-config*.

ip-address (Optional) If **rcp** or **tftp** is specified, the IP address of the network server on which the compressed image file resides. If omitted, this value defaults to the IP broadcast address of 255.255.255.255.

mac-address (Optional) If **MOP** is specified, the MAC address of the network server on which the file resides. If the MAC address argument is not included, a broadcast message is sent to all MOP boot servers. The first server to indicate that it has the file will be the server from which the router gets the boot image.

interface (Optional) If MOP is specified, interface out which the router should send MOP requests to reach the server. The interface options are **async**, **dialer**, **ethernet**, **serial**, and **tunnel**. If the interface argument is not specified, a request will be sent on all interfaces that have MOP enabled, and the interface out which the first response is received will be used to load the software.

boot system flash [*device***:**][*partition-number***:**][*filename*]
[**no**] **boot system mop** *filename* [*mac-address*] [*interface*]
[**no**] **boot system rom**
[**no**] **boot system** [**tftp** | **rcp**] *filename* [*ip-address*]

no boot system flash [*filename*]
no boot system

To change the filename of the system image that is loaded onto the router at reboot time, use the **boot system** global configuration command. Use the **no boot system** command to remove the name.

flash Boots the router from Flash memory.

mop Boots the router from a system image stored on a Digital MOP server.

rom Boots the router from ROM.

rcp (Optional) Boots the router from a system image stored on a network server using rcp. If you omit this keyword, the transport mechanism defaults to **tftp**.

tftp (Optional) Boots the router from a system image stored on a TFTP server. If omitted and **rcp** is not specified, the transport mechanism defaults to **tftp**.

filename (Optional with **flash**.) Name of the configuration file from which you want to netboot. It is case sensitive. If you do not specify a system image file with the **boot system** command, the router uses the configuration register settings to determine the default system image filename to boot from the network server. The router forms the default boot filename by starting with the word *cisco* and then appending the octal equivalent of the boot field number in the configuration register, followed by a hyphen, and the processor type name (cisco *nn-cpu*).

ip-address (Optional) IP address of the rcp or TFTP server on which the image file resides. Defaults to the IP broadcast address of 255.255.255.255.

mac-address (Optional) If MOP is used, the MAC address of the server on which the file resides. If the MAC address argument is not included, a broadcast message is sent to all MOP boot servers. The first server to indicate that it has the file will be the server from which the router gets the boot image.

interface (Optional) Interface out which the router should send MOP requests to reach the server. The interface options are **async**, **dialer**, **ethernet**, **serial**, and **tunnel**. If the interface argument is not specified, a request will be sent on all interfaces that have MOP enabled, and the interface out which the first response is received will be used to load the software.

*device***:** (Optional) Valid value is **flash**.

*partition-number***:**	(Optional) Boots the router from Flash memory with the optional filename of the image you want loaded from the specified Flash partition. If you do not specify a filename, the first valid file in the specified partition of Flash memory is loaded.

config-register *value*

To change the router configuration register settings, use the **config-register** global configuration command.

value	Hexadecimal or decimal value that represents the 16-bit configuration register value you want to use the next time the router is restarted. The value range is from 0x0 to 0xFFFF (0 to 65535 in decimal). The default is 0x101 for the router models without Flash memory; default is 0x10F for router models with Flash memory.

configure {**terminal** | **memory** | **network**}

To enter global configuration mode, use the **configure** privileged EXEC command.

terminal	Executes configuration commands from the terminal.
memory	Executes the configuration commands stored in nonvolatile random-access memory (NVRAM).
network	Retrieves the configuration commands stored in a file on a server.

configure overwrite-network

To load a configuration file directly into NVRAM, use the **configure overwrite-network** privileged EXEC command.

copy bootflash rcp

To use rcp to copy a bootstrap image from Flash memory on a Cisco 4500 router to a network server, use the **copy bootflash rcp** EXEC command.

copy bootflash tftp

To copy a boot image from Flash memory to a TFTP server, use the **copy bootflash tftp** EXEC command.

copy flash rcp

To copy a system image from Flash memory to a network server using rcp, use the **copy flash rcp** EXEC command.

copy flash tftp

To copy a system image from Flash memory to a TFTP server, use the **copy flash tftp** EXEC command.

copy mop bootflash

To copy a boot image from a MOP server to Flash memory on the Cisco 4500, use the **copy mop bootflash** EXEC command.

copy mop flash

To use MOP to copy a system image to Flash memory, use the **copy mop flash** EXEC command.

copy rcp bootflash

To copy a bootstrap image from a network server to Flash memory on a Cisco 4500 router using rcp, use the **copy rcp bootflash** EXEC command.

copy rcp flash

To copy a system image from a network server into Flash memory using rcp, use the **copy rcp flash** EXEC command.

copy rcp running-config

To copy a configuration file from a network server to the router using rcp and run that configuration, use the **copy rcp running-config** EXEC command.

copy rcp startup-config

To copy a configuration file from a network server to the router's NVRAM using rcp, use the **copy rcp startup-config** EXEC command.

copy running-config {rcp | tftp}

To copy the running configuration file from the router to a network server using rcp or TFTP, use the **copy running-config** EXEC command.

copy startup-config {rcp | tftp}

To copy a startup configuration file to a network server using rcp or TFTP, use the **copy startup-config rcp** EXEC command.

copy tftp bootflash

To copy a boot image from a TFTP server to Flash memory on the Cisco 4500, use the **copy tftp bootflash** EXEC command.

copy tftp flash

To copy a system image using TFTP into Flash memory, use the **copy tftp flash** EXEC command.

copy verify

To verify the checksum of a system image in Flash memory, use the **copy verify** EXEC command.

copy verify bootflash

To verify the checksum of a boot image in Flash memory, use the **copy verify bootflash** EXEC command.

erase bootflash

To erase the boot image in Flash memory on the Cisco 4500, use the **erase bootflash** EXEC command.

erase flash

To erase Flash memory, use the **erase flash** EXEC command.

[**no**] **ip rarp-server** *ip-address*

Use the **ip rarp-server** interface configuration command to allow the router to act as a Reverse Address Resolution Protocol (RARP) server. Use the **no** form of this command to restore the interface to the default of no RARP server support.

ip-address	IP address to be provided in the source protocol address field of the RARP response packet. Normally, this is set to the address you configure as the primary address for the interface.

[**no**] **ip rcmd domain-lookup**

Use the **ip rcmd domain-lookup** global configuration command to enable DNS security for rcp and rsh. To bypass DNS security for rcp and rsh, use the **no** form of this command.

[**no**] **ip rcmd rcp-enable**

To configure the router to allow remote users to copy files to and from the router, use the **ip rcmd rcp-enable** global configuration command. Use the **no rcp-enable** command to disable a router that is enabled for rcp.

[**no**] **ip rcmd remote-host** *local-username* {*ip-address* | *host*} *remote-username* [**enable**]

To allow remote users to execute commands on the router using rsh or rcp, use the **ip rcmd remote-host** global configuration command to create an entry for the remote user in a local authentication database. Use the **no** form of this command to remove an entry for a remote user from the local authentication database.

local-username	Name of the user on the local router. You can specify the router host name as the username. This name needs to be communicated to the network administrator or the user on the remote system. To be allowed to remotely execute commands on the router, the remote user must specify this value correctly.
ip-address	IP address of the remote host from which the local router will accept remotely executed commands. Either the IP address or the host name is required.
host	Name of the remote host from which the local router will accept remotely executed commands. Either the host name or the IP address is required.
remote-username	Name of the user on the remote host from which the router will accept remotely executed commands.
enable	(Optional) Enables the remote user to execute privileged EXEC commands using rsh. This keyword does not apply to rcp.

[**no**] **ip rcmd remote-username** *username*

To configure the remote username to be used when requesting a remote copy using rcp, use the **ip rcmd remote-username** global configuration command. To remove the remote username form the configuration, use the **no** form of this command.

username	Name of the remote user on the server. This name is used for rcp copy requests. All files and images to be copied are searched for or written relative to the directory of the remote user's account.

[**no**] **ip rcmd rsh-enable**

To configure the router to allow remote users to execute commands on the router using rsh, use the **ip rcmd rsh-enable** global configuration command. Use the **no** form of this command to disable a router that is enabled for rsh.

[**no**] **microcode** *interface* [**flash** | **rom** | **system**] [**flash** *filename*]

To specify the location of the microcode you want to download from Flash memory into the writable control store (WCS) on a Cisco 7000 series router, use the **microcode** interface configuration command.

interface	One of the following interface processor names: **aip**, **fip**, **fsip**, **hip**, **mip**, **trip**, **eip**, or **sp**.
flash	(Optional) If the **flash** keyword is specified, a *filename* argument is required, unless you are using the **no microcode** *interface-type* **flash** command.

rom (Optional) If the **rom** keyword is specified, no further arguments are necessary. For example, the command **microcode fip rom** specifies that all FDDI Interface Processors (FIPs) should be loaded from their onboard ROM microcode. This onboard ROM microcode is not the same as the eight ROMs on the RP that contain the system image.

system (Optional) If specified, the router loads the microcode from the microcode bundled into the system image you are running for that interface type.

filename (Optional) Filename of the microcode in Flash memory you want to download. This argument is used only with the **flash** keyword. If you use the **flash** keyword, the name of the microcode file in Flash is required unless the command is **no microcode** *interface* **flash**. (This command results in the same default condition as the command **microcode** *interface* **rom**, which indicates that the card should be loaded from its onboard ROM microcode.)

microcode reload

To signal to the Cisco 7000 series router that all microcode configuration commands have been entered and the processor cards should be reloaded, use the **microcode reload** interface configuration command.

[**no**] **mop device-code** {**cisco** | **ds200**}

To identify the type of device sending MOP sysid messages and request program messages, use the **mop device-code** global configuration command. Use the **no** form of this command to set the identity to the default value.

cisco Denotes a Cisco device code.

ds200 Denotes a DECserver 200 device code.

mop retransmit-timer *seconds*
no mop retransmit-timer

To configure the length of time the router waits before retransmitting boot requests to a MOP server, use the **mop retransmit-timer** global configuration command. Use the **no** form of this command to reinstate the default value.

seconds Sets the length of time, in seconds, that the router waits before retransmitting a message. The value is a number from 1 to 20.

mop retries *count*
no mop retries

To configure the number of times a router will retransmit boot requests to a MOP server, use the **mop retries** global configuration command. Use the **no** form of this command to reinstate the default value.

count Indicates the number of times a router will retransmit a MOP boot request. The value is a number from 3 to 24.

o
o/r

To list the value of the boot field (bits 0-3) in the configuration register, use the ROM monitor **o** command. To reset the value of the boot field so that the router boots from ROM, use the ROM monitor **o/r** command.

partition flash *partitions* [*size1 size2*]
no partition flash

To separate Flash memory into two partitions, use the **partition flash** global configuration command. Use the **no** form of this command to undo partitioning, and restore Flash memory to one partition.

partitions	Number of partitions in Flash memory. Can be 1 or 2.
size1	(Optional) Size of the first partition in megabytes.
size2	(Optional) Size of the second partition in megabytes.

reload

To reload the operating system, use the **reload** EXEC command.

rsh {*ip-address* | *host*} [**/user** *username*] *remote-command*

To execute a command remotely on a remote rsh host, use the **rsh** EXEC command.

ip-address	IP address of the remote host on which to execute the rsh command. Either the IP address or the host name is required.

host	Name of the remote host on which to execute the command. Either the host name or the IP address is required.
/**user** *username*	(Optional) Remote username. If you do not specify a remote username, the router software uses the configured remote username, if one exists. Otherwise, the router software uses the username associated with the current TTY, if it is a valid name. If this name is invalid, the router software uses the host name as the username.
remote-command	Command to be executed remotely. This is a required parameter. Unlike UNIX, the router software does not default to a remote login. Instead, the router provides Telnet and connect services.

[**no**] service compress-config

To compress configuration files on the Cisco 7000 series, Cisco 4000, Cisco 3000, and AGS+ routers, which have NVRAM, use the **service compress-config** global configuration command. To disable compression, use the **no** form of this command.

[**no**] service config

To enable autoloading of configuration files from a network server, use the **service config** global configuration command. Use the **no** form of this command to restore the default.

show async-bootp

Use the **show async-bootp** privileged EXEC command to display the parameters that have been configured for SLIP extended BOOTP requests.

show bootflash

To verify boot Flash memory, use the **show bootflash** EXEC command.

show configuration

Use the **show configuration** EXEC command to display the contents of NVRAM, if present and valid.

NVRAM stores the configuration information in the network server in text form as configuration commands. The **show configuration** command shows the version number of the software used when you last executed the **write memory** command.

show flash [all | chips | detailed | err | partition *number* [all | chips | detailed | err] | summary]

Use the **show flash** EXEC command to verify Flash memory. The **show flash** command displays the type of Flash memory present, any files that might currently exist in Flash memory, and the amounts of Flash memory used and remaining.

all (Optional) Shows complete information about Flash memory, including information about the individual ROM devices in Flash memory and the names and sizes of all system image files stored in Flash, including those that are invalidated.

chips (Optional) Shows information per partition and per chip, including which bank the chip is in, its code, size, and name.

detailed (Optional) Shows detailed file directory information per partition, including file length, address, name, Flash checksum, computer checksum, bytes used, bytes available, total bytes, and bytes of system Flash memory.

err (Optional) Shows write or erase failures in the form of number of retries.

partition *number*

(Optional) Shows output for the specified partition number. If you specify the **partition** keyword, you must specify a partition number. You can use this keyword only when Flash memory has multiple partitions.

summary

(Optional) Shows summary information per partition, including the partition size, bank size, state, and method by which files can be copied into a particular partition. You can use this keyword only when Flash memory has multiple partitions.

show flh-log

To view the system console output generated during the Flash load helper operation, use the **show flh-log** privileged EXEC command.

show microcode

To show the microcode bundled into a Cisco 7000 series system, use the **show microcode** EXEC command.

show version

Use the **show version** EXEC command to display the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

tftp-server system [**flash:**][*partition-number***:**]*filename* [*access-list-number*]
no tftp-server system [**flash:**] *filename* [*access-list-number*]

To specify TFTP server operation for a router, use the **tftp-server system** global configuration command. To remove a previously defined filename, use the **no** form of this command with the appropriate filename and, optionally, access-list number.

filename	Name you give the router ROM file.
access-list-number	(Optional) IP access list number.
flash:	(Optional) Specifies TFTP server operation from the file in the first partition of Flash memory.
*partition-number***:**	(Optional) Specifies TFTP server operation from the file in the specified partition of Flash memory. If the partition number is not specified, the file in the first partition is used.

verify flash

To verify the checksums of files in Flash memory, use the **verify flash** EXEC command.

write erase

To erase the configuration information in NVRAM, use the **write erase** EXEC command.

write memory

To copy the current configuration information to NVRAM, use the **write memory** EXEC command.

write network

To copy the current configuration information to a network server, use the **write network** EXEC command.

write terminal

To display the current configuration information on the terminal, use the **write terminal** EXEC command.

Line Configuration and Terminal Setting Commands

This chapter describes the function and displays the syntax of each terminal line and modem support command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

absolute-timeout *minutes*

To set the interval for closing the connection, use the **absolute-timeout** line configuration command. Use the **no** form of this command to restore the default.

minutes	Number of minutes after which the user's session is terminated.

activation-character *ascii-number*
no activation-character

To set the activation character, use the **activation-character** line configuration command. This command defines the character you type at a vacant terminal to begin a terminal session. Use the **no** form of this command to make any character activate a terminal.

ascii-number	ASCII decimal representation of the activation character. Default is Return (decimal 13).

[**no**] **autobaud**

To set the line for automatic baud detection, use the **autobaud** line configuration command. Use the **no** form of this command to restore the default.

autocommand *command*

To configure the router to automatically execute a command or list of commands automatically when a user connects to a particular line, use the **autocommand** line configuration command.

command	Any appropriate EXEC command, including the host name and any switches associated with the EXEC command.

autohangup

To configure automatic line disconnect, use the **autohangup** line configuration command. The command causes the EXEC to issue the **exit** command when the last connection closes.

autoselect {**arap** | **ppp** | **slip**} | **during-login**
no autoselect

To configure a line to start an ARA, Point-to-Point (PPP), or SLIP session, use the **autoselect** line configuration command. Use the **no** form of this command to disable this function on a line.

arap	Configures the router to allow an ARA session to start up automatically.
ppp	Configures the router to allow a PPP session to start up automatically.
slip	Configures the router to allow a SLIP session to start up automatically.
during-login	(Optional) The user receives a username and/or password prompt without pressing the Return key. After the user logs in, the autoselect function begins.

banner exec *d message d*

To display a message on terminals with an interactive EXEC, use the **banner exec** global configuration command. This command specifies a message to be displayed when an EXEC process is created (line activated, or incoming connection to VTY).

d Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.

message Message text.

banner incoming *d message d*

To specify a message used when you have an incoming connection to a line from a host on the network, use the **banner incoming** global configuration command. An incoming connection is one initiated from the network side of the router. To suppress the EXEC banner on certain lines, use the **no exec-banner** line configuration command. This line should *not* display the EXEC or MOTD banners when an EXEC is created.

d Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.

message 0000000000

banner motd *d message d*

To specify a message-of-the-day (MOTD) banner, use the **banner motd** global configuration command.

d Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.

message Message text.

busy-message *hostname d message d*
no busy-message *hostname*

To create a "host failed" message that displays when a connection fails, use the **busy-message** global configuration command. Use the **no** form of this command to disable the "host failed" message from displaying on the specified host.

hostname	Name of the host that cannot be reached.
d	Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the message.
message	Message text.

databits {**5** \| **6** \| **7** \| **8**}

To set the number of data bits per character that are interpreted and generated by hardware, use the **databits** line configuration command.

5	Five data bits per character.
6	Six data bits per character.
7	Seven data bits per character.
8	Eight data bits per character.

data-character-bits {**7** \| **8**}

To set the number of data bits per character that are interpreted and generated by software, use the **data-character-bits** line configuration command.

7	Seven data bits per character.
8	Eight data bits per character.

default-value exec-character-bits {7 | 8}

To define the EXEC character width for either 7 bits or 8 bits, use the **default-value exec-character-bits** global configuration command.

7	Selects the 7-bit ASCII character set.
8	Selects the full 8-bit ASCII character set.

default-value special-character-bits {7 | 8}

To configure the flow control default value from a 7-bit width to an 8-bit width, use the **default-value special-character-bits** global configuration command.

7	Selects the 7-bit character set.
8	Selects the full 8-bit character set.

disconnect-character *ascii-number*
no disconnect-character

To define a character to disconnect a session, use the **disconnect-character** line configuration command. This command defines the character you enter to end a terminal session. Use the **no** form of this command to remove the disconnect character.

ascii-number	ASCII decimal representation of the session disconnect character.

[**no**] **dispatch-character** *ascii-number1* [*ascii-number2 . . . ascii-number*]

To define a character that causes a packet to be sent, use the **dispatch-character** line configuration command. Use the **no** form of this command to remove the definition of the specified dispatch character.

ascii-number	ASCII decimal representation of the character, such as Return (ASCII decimal 13) for line-at-a-time transmissions.

dispatch-timeout *milliseconds*
no dispatch-timeout

To set the character dispatch timer, use the **dispatch-timeout** line configuration command. Use the **no** form of this command to remove the timeout definition.

milliseconds	Integer that specifies the number of milliseconds the router waits after putting the first character into a packet buffer before sending the packet. During this interval, more characters may be added to the packet, which increases the processing efficiency of the remote host.

escape-character *ascii-number*
no escape-character

To define a system escape character, use the **escape-character** line configuration command. The **no** form of this command sets the escape character to Break.

ascii-number	Either the ASCII decimal representation of the character or a control sequence (Ctrl-E, for example).

[**no**] **exec**

To allow an EXEC process on a line, use the **exec** line configuration command. The **no** form of this command turns off the EXEC process for the line specified.

[**no**] **exec-banner**

To control whether banners are displayed or suppressed, use the **exec-banner** line configuration command. This command determines whether the router will display the EXEC banner or the message-of-the-day (MOTD) banner when an EXEC is created. The **no** form of this command suppresses the banner messages.

exec-character-bits {**7** | **8**}

To configure the character widths of EXEC and configuration command characters, use the **exec-character-bits** line configuration command.

7	Selects the 7-bit character set.
8	Selects the full 8-bit character set for use of international and graphical characters in banner messages, prompts, and so forth.

exec-timeout *minutes* [*seconds*]
no exec-timeout

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** line configuration command. The **no** form of this command removes the timeout definition. It has the same effect as **exec-timeout 0**.

minutes	Integer that specifies the number of minutes.
seconds	(Optional) Additional time intervals in seconds. An interval of zero specifies no time-outs.

[**no**] **flowcontrol** {**none** | **software** [**in** | **out**] | **hardware** [**in** | **out**]}

To set the method of data flow control between the terminal or other serial device and the router, use the **flowcontrol** line configuration command. To disable flow control, use the **no** form of this command.

none	Turns off flow control.
software	Sets software flow control. An optional keyword specifies the direction: in causes the router to listen to flow control from the attached device, and out causes the router to send flow control information to the attached device. If you do not specify a direction, both are assumed.
hardware	Sets hardware flow control. An optional keyword specifies the direction: in causes the router to listen to flow control from the attached device, and out causes the router to send flow control information to the attached device. If you do not specify a direction, both are assumed. For more information about hardware flow control, see the hardware installation and maintenance manual for your router.

hold-character *ascii-number*
no hold-character

To define the local hold character used to pause output to the terminal screen, use the **hold-character** line configuration command. The **no** form of this command restores the default.

ascii-number	Either the ASCII decimal representation of the hold character or a control sequence (for example, Ctrl-P).

length *screen-length*

To set the terminal screen length, use the **length** line configuration command.

screen-length	Number of lines on the screen. A value of zero disables pausing between screens of output.

line [**aux** | **console** | **vty**] *line-number* [*ending-line-number*]

To configure a console port line, auxiliary port line, or virtual terminal lines, use the **line** global configuration command.

aux	(Optional) Enables the auxiliary RS-232 DTE port. Must be addressed as relative line 0. The auxiliary port can be used for modem support and asynchronous connections.
console	(Optional) Specifies the console terminal line. The console port is DCE.
vty	(Optional) Specifies a virtual terminal for remote console access.
line-number	Specifies the relative number of the terminal line (or the first line in a contiguous group) you want to configure when the line type is specified. Numbering begins with zero.
ending-line-number	(Optional) Specifies the relative number of the last line in a contiguous group you want to configure. If you omit the keyword, then *line-number* and *ending-line-number* are absolute rather than relative line numbers.

location *text*
no location

To record the location of a serial device, use the **location** line configuration command. The **no** form of this command removes the description.

text	Location description.

[**no**] **lockable**

To enable the EXEC command **lock**, use the **lockable** global configuration command. The **no** form of this command reinstates the default, which does not allow the terminal to be locked.

login [**local** | **tacacs**]
no login

To enable password checking at login, use the **login** line configuration command. Use the **no** form of this command to disable password checking and allow connections without a password.

local	(Optional) Selects local password checking. Authentication is based on the username specified with the **username** global configuration command.
tacacs	(Optional) Selects the TACACS-style user ID and password-checking mechanism.

[**no**] **login authentication** {**default** | *list-name*}

To enable AAA/TACACS+ authentication for logins, use the **login authentication** line configuration command. Use the **no** form of the command to return to the default.

default	Uses the default list created with the **aaa authentication login** command.
list-name	Uses the indicated list created with the **aaa authentication login** command.

login-string *hostname d message* [**%***sec***p**] [**%***sec***w**] [**%b**] *d*
no login-string *hostname*

To define a string of characters that the router sends to a host after a successful Telnet connection, use the **login-string** global configuration command. This command applies only to rlogin and Telnet sessions. The **no** form of this command removes the login string.

hostname	Specifies the name of the host.
d	Sets a delimiting character of your choice—a pound sign (#) for example. You cannot use the delimiting character in the busy message.
message	Specifies the login string.
%*sec***p**	(Optional) Sets a pause in seconds. To insert pauses into the login string, embed a percent sign (%) followed by the number of seconds to pause and the letter "p."
%*sec***w**	(Optional) Prevents users from issuing commands or keystrokes during a pause.
%b	(Optional) Sends a Break character.

modem answer-timeout *seconds*
no modem answer-timeout

To set the amount of time that the router waits for CTS after raising DTR in response to RING, use the **modem answer-timeout** line configuration command. The **no** form of this command reverts the router to the default value.

seconds	Specifies the timeout interval in seconds.

[**no**] **modem callin**

To support dial-in modems that use DTR to control the off-hook status of the modem, use the **modem callin** line configuration command. In response to RING, the modem raises the DTR signal, which answers the modem. At the end of the session, the router lowers DTR, which disconnects the modem. The **no** form of this command disables this feature.

[**no**] **modem callout**

To configure a line for reverse connections, use the **modem callout** line configuration command. The **no** form of this command disables this feature.

[**no**] **modem cts-required**

To configure a line to require a Clear To Send (CTS) signal, use the **modem cts-required** line configuration command. Use the **no** form of this command to disable this feature.

[**no**] **modem dtr-active**

To configure a line to leave DTR low unless the line has an active incoming connection or an EXEC process, use the **modem dtr-active** line configuration command. The **no** form of this command disables this feature.

[**no**] **modem in-out**

To configure a line for both incoming and outgoing calls, use the **modem in-out** line configuration command. The **no** form of this command disables this feature.

[**no**] **modem ri-is-cd**

To configure a line for a high-speed modem, use the **modem ri-is-cd** line configuration command. The **no** form of this command disables this feature.

[**no**] **notify**

To enable terminal notification about pending output from other connections, use the **notify** line configuration command. The **no** form of this command ends notification.

padding *ascii-number count*
no padding *ascii-number*

To set the padding on a specific output character, use the **padding** line configuration command. To remove padding for the specified output character, use the **no padding** line configuration command.

ascii-number	ASCII decimal representation of the character.
count	Number of NULL bytes sent after that character; the maximum is 255.

parity {**none** \| **even** \| **odd** \| **space** \| **mark**}

To define generation of a parity bit, use the **parity** line configuration command.

none	No parity.
even	Even parity.
odd	Odd parity.
space	Space parity.
mark	Mark parity.

password *password*
no password

To specify a password on a line, use the **password** line configuration command. Use the **no** form of this command to remove the password.

password Case-sensitive character string that specifies the line password. The string can contain any alphanumeric characters, including spaces, up to 80 characters, except that the first character cannot be a number. You cannot specify the password in the format *number-space-anything* because the space after the number causes problems. For example, “hello 21” is a legal password, but “21 hello” is not.

[**no**] **private**

To save user EXEC command changes between terminal sessions, use the **private** line configuration command. Use the **no** form of this command to restore the default condition.

refuse-message *d message d*
no refuse-message

To define a line-in-use message, use the **refuse-message** line configuration command. Use the **no** form of the command to disable the message.

d Delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the message.

message Message text.

rotary *group*
no rotary

To define a group of lines consisting of one or more virtual terminal lines or one auxiliary port line, use the rota**ry** line configuration command. Use the **no** form of this command to remove a line or group of lines from a rotary group.

group Integer between 1 and 100 that you choose to identify the rotary group.

rxspeed *bps*

To set the terminal baud rate receive (from terminal) speed, use the **rxspeed** line configuration command.

bps Baud rate in bits per second (bps); see the line speeds table in the terminal lines chapter of the *Router Products Command Reference* publication for settings.

[**no**] **script activation** *regexp*

To specify that a chat script start on a line any time the line is activated, use the **script activation** line configuration command. The **no** form of this command disables this feature.

regexp Regular expression that specifies the set of modem scripts that might be executed. The first script name that matches the argument *regexp* will be used.

script connection *regexp*
no script connection

To specify that a chat script start on a line any time a remote network connection is made to a line, use the **script connection** line configuration command. The **no** form of this command disables this feature.

regexp Specifies the set of modem scripts that might be executed. The first script name that matches the argument regexp will be used.

script reset *regexp*
no script reset

To specify that a chat script start on a line any time the specified line is reset, use the **script reset** line configuration command. The **no** form of this command disables this feature.

regexp Specifies the set of modem scripts that might be executed. The first script name that matches the argument regexp will be used.

script startup *regexp*
no script startup

To specify that a chat script start on a line any time the router is powered up, use the **script startup** line configuration command. The **no** form of this command disables this feature.

regexp Specifies the set of modem scripts that might be executed. The first script name that matches the argument *regexp* will be used.

[**no**] **service linenumber**

To configure the router to display line number information after the EXEC or incoming banner, use the **service linenumber** global configuration command. To disable this function, use the **no** form of this command.

session-limit *session-number*
no session-limit

To set the maximum number of terminal sessions per line, use the **session-limit** line configuration command. The **no** form of this command removes any specified session limit.

session-number	Specifies the maximum number of sessions.

session-timeout *minutes* [**output**]
no session-timeout

To set the interval for closing the connection when there is no input or output traffic, use the **session-timeout** line configuration command. The no form of this command removes the timeout definition.

minutes	Specifies the time interval in minutes.
output	(Optional) Specifies that when traffic is sent to an asynchronous line from the router (within the specified interval), the connection is retained.

show line [*line-number*]

To display a terminal line's parameters, use the **show line** EXEC command.

line-number	(Optional) Absolute line number of the line for which you want to list parameters.

special-character-bits {**7** | **8**}

To configure the number of data bits per character for special characters such as software flow control characters and escape characters, use the **special-character-bits** line configuration command.

7	Selects the 7-bit ASCII character set.
8	Selects the full 8-bit character set for special characters.

speed *bps*

To set the terminal baud rate, use the **speed** line configuration command. The command sets both the transmit (to terminal) and receive (from terminal) speeds.

bps	Baud rate in bits per second (bps); see the lines speeds table in the terminal lines chapter of the *Router Products Command Reference* publication for settings.

start-character *ascii-number*
no start-character

To define the character that signals the start of data transmission when software flow control is in effect, use the **start-character** line configuration command. The **no** form of this command removes the character.

ascii-number	ASCII decimal representation of the start character.

start-chat *regexp* [**aux 0** [*dialer-string*]]
no start-chat

To manually start a chat script, use the **start-chat** privileged EXEC command. The **no** form of the command stops the chat script.

regexp	Specifies the name of a regular expression or modem script to be executed. If there is more than one script with a name that matches the argument *regexp*, the first script found will be used.
aux 0	(Optional) Indicates the line number on which to execute the chat script. If you do not specify a line number, the current line number is chosen. If the specified line is busy, the script is not executed and an error message appears. If the *dialer-string* argument is specified, the line number (aux 0) must be entered; it is not optional if you specify a dialer string. This command functions only on physical terminal (tty) lines. It does not function on virtual terminal (vty) lines.
dialer-string	String of characters (often a telephone number) to be sent to a DCE. If you enter a dialer string, you must also specify the line number (aux 0), or the chat script *regexp* will not start.

stopbits {**1** | **1.5** | **2**}

To set the number of the stop bits transmitted per byte, use the **stopbits** line configuration command.

1	One stop bit.
1.5	One and one-half stop bits.
2	Two stop bits.

stop-character *ascii-number*
no stop-character

To set the flow control stop character, use the **stop-character** line configuration command. The **no** form of this command removes the character.

ascii-number	ASCII decimal representation of the stop character.

telnet break-on-ip

To configure the router to generate a hardware Break signal upon receiving an Interrupt Process (IP) command, use the **telnet break-on-ip** line configuration command.

telnet refuse-negotiations

To configure a line using Telnet to refuse to negotiate full-duplex, remote echo options on incoming connections, use the **telnet refuse-negotiations** line configuration command.

telnet speed *default-speed maximum-speed*

To allow the router to negotiate transmission speed of the line to a connected device, use the **telnet speed** line configuration command.

default-speed	Line speed (in bps) that the router will use if the device on the other end of the connection has not specified a speed.
maximum-speed	Maximum speed (in bps) that the device on the port will use.

telnet sync-on-break

To configure the router to cause an incoming connection to send a Telnet synchronize signal when it receives a Telnet Break signal, use the **telnet sync-on-break** line configuration command.

telnet transparent

To configure the router to send a carriage return (CR) as a CR followed by a NULL instead of a CR followed by a line feed (LF), use the **telnet transparent** line configuration command.

terminal-type *terminal-name*
no terminal-type

Use the **terminal-type** line configuration command to specify the type of terminal connected to a line. Use the **no** form of this command to remove any information about the type of terminal and reset the line to the default terminal emulation.

terminal-name	Terminal name and type.

transport input {mop | telnet | none}

To allow the system administrator to define which protocols to use to connect to a specific line of the router, use the **transport input** line configuration command.

mop	Selects the MOP protocol.
telnet	Specifies all types of incoming TCP/IP connections.
none	Prevents any protocol selection on the line. This makes the port unusable by incoming connections.

transport output {telnet | none}

To determine the protocols that can be used for outgoing connections from a line, use the **transport output** line configuration command.

telnet	Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.

none	Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to **none**, the system no longer makes that assumption. No connection will be attempted if the command is not recognized.

transport preferred {**telnet** | **none**}

To specify the transport protocol the router uses if the user does not specify one when initiating a connection, use the **transport preferred** line configuration command.

telnet	Selects the TCP/IP Telnet protocol. It allows a user at one site to establish a TCP connection to a login server at another site.
none	Prevents any protocol selection on the line. The system normally assumes that any unrecognized command is a host name. If the protocol is set to **none**, the system no longer makes that assumption. No connection will be attempted if the command is not recognized.

txspeed *bps*

To set the terminal transmit baud rate (to terminal), use the **txspeed** line configuration command.

bps	Baud rate in bits per second (bps); see the line speeds table in the terminal lines chapter of the *Router Products Command Reference* publication for settings.

vacant-message [*d message d*]
no vacant-message

To display an idle terminal message, use the **vacant-message** line configuration command. The command enables the banner to be displayed on the screen of an idle terminal. The **vacant-message** command without any arguments restores the default message. The **no** form of this command removes the default vacant message or any other vacant message that might have been set.

d	(Optional) A delimiting character of your choice—a pound sign (#), for example. You cannot use the delimiting character in the banner message.
message	(Optional) Vacant terminal message.

width *characters*

To set the terminal screen width, use the **width** line configuration command. This command sets the number of character columns displayed on the attached terminal.

characters	Integer that specifies the number of character columns displayed on the terminal.

System Management Commands

This chapter describes the function and displays the syntax of commands used to manage the router system and its performance on the network. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

a**aa accounting** {**system** | **network** | **connection** | **exec** | **command** *level*} {**start-stop** |
  wait-start | **stop-only**} **tacacs+**
no aaa accounting {**system** | **network** | **connection** | **exec** | **command** *level*}

To enable AAA accounting of requested services for billing or security purposes when using TACACS+, use the **aaa accounting** global configuration command. Use the **no** form of this command to disable accounting.

system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.
connection	Runs accounting for outbound Telnet and rlogin.
exec	Runs accounting for Execs (user shells). This keyword might return user profile information such as **autocommand** information.
command	Runs accounting for all commands at the specified privilege level.

level

Command level that should be accounted. Valid entries are 0 through 15.

start-stop

Sends a start record accounting notice at the beginning of a process and a stop record is sent at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting record was received by the accounting server.

wait-start

As in **start-stop**, sends both a start and a stop accounting record to the accounting server. However, if you use the **wait-start** keyword, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.

stop-only

Sends a stop record accounting notice at the end of the requested user process.

aaa authentication arap {**default** | *list-name*} *method1* [...[*method4*]]
no aaa authentication arap {**default** | *list-name*} *method1* [...[*method4*]]

To enable an AAA authentication method for ARA users using TACACS+, use the **aaa authentication arap** global configuration command. Use the **no** form of the command to disable this authentication.

default	Uses the listed methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the following list of authentication methods tried when a user logs in.
method	One of the keywords described in the table "AAA Authentication ARAP Method Descriptions."

[**no**] **aaa authentication enable default** *method1* [...[*method4*]]

To enable AAA authentication to determine if a user can access the privileged command level with TACACS+, use the **aaa authentication enable default** global configuration command. Use the **no** form of the command to disable this authorization method.

method	At least one and up to four of the keywords described in the table "AAA Authentication Enable Default Method Descriptions."

[**no**] **aaa authentication local-override**

To have the router check the local user database for authentication before attempting another form of authentication, use the **aaa authentication local-override** global configuration command. Use the **no** form of the command to disable the override.

[**no**] **aaa authentication login** {**default** | *list-name*} *method1* [...[*method4*]]

To set AAA authentication at login when using TACACS+, use the **aaa authentication login** global configuration command. Use the **no** form of the command to disable AAA authentication.

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the following list of authentication methods tried when a user logs in.
method	At least one and up to four of the methods described in the table "AAA Authentication Login Method Descriptions."

[**no**] **aaa authentication ppp** {**default** | *list-name*} *method1* [...[*method4*]]

To specify one or more AAA authentication methods for use on serial interfaces running PPP when using TACACS+, use the **aaa authentication ppp** global configuration command. Use the **no** form of the command to disable authentication.

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string used to name the following list of authentication methods tried when a user logs in.
method	At least one and up to four of the methods described in the table "AAA Authentication PPP Method Descriptions."

aaa authorization {**network** | **connection** | **exec** | **command** *level*}
methods
no aaa authorization {**network** | **connection** | **exec** | **command** *level*}

To set parameters that restrict a user's network access based on TACACS+ authorization, use the **aaa authorization** global configuration command. To disable authorization for a function, use the **no** form of the command.

network	Performs authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.
connection	Runs authorization for outbound Telnet and rlogin.
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This keyword might return user profile information such as **autocommand** information.
command	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
methods	The table "AAA Authorization Method Descriptions" lists the *methods* keywords.

[**no**] **aaa new-model**

To enable the AAA access control model that includes TACACS+, issue the **aaa new-model** global configuration command. Use the **no** form of the command to disable this functionality.

alias *mode alias-name alias-command-line*
no alias *mode* [*alias-name*]

To create a command alias, use the **alias** global configuration command. Use the **no** form of this command to delete all aliases in a command mode or to delete a specific alias, and to revert to the original command syntax.

mode	Command mode of the original and alias commands. See the "Mode Argument Options" table in the *Router Products Command Reference* publication for a list of options for this argument.
alias-name	Command alias.
alias-command-line	Original command syntax.

[**no**] **arap authentication** {**default** \| *list-name*}

To enable TACACS+ authentication for ARA on a line, use the **arap authentication** line configuration command. Use the **no** form of the command to disable authentication for an ARA line.

default	Use the default list created with the **aaa authentication arap** command.
list-name	Use the indicated list created with the **aaa authentication arap** command.

[**no**] **buffers** {**small** | **middle** | **big** | **large** | **verylarge** | **huge** | *type number*}{**permanent** | **max-free** | **min-free** | **initial** } *number*

Use the **buffers** global configuration command to make adjustments to initial buffer pool settings and to the limits at which temporary buffers are created and destroyed. Use the **no** form of this command to return the buffers to their default size.

small — Buffer size of this public buffer pool is 104 bytes.

middle — Buffer size of this public buffer pool is 600 bytes.

big — Buffer size of this public buffer pool is 1524 bytes.

large — Buffer size of this public buffer pool is 5024 bytes.

verylarge — Buffer size is of this public buffer pool 8188 bytes.

huge — Default buffer size of this public buffer pool is 18024 bytes. This value can be configured with the **buffers huge size** command.

type — Interface type of the interface buffer pool. Value cannot be **fddi**.

number — Interface number of the interface buffer pool.

permanent — Number of permanent buffers that the system tries to create and keep. Permanent buffers are normally not trimmed by the system.

max-free — Maximum number of free or unallocated buffers in a buffer pool.

min-free	Minimum number of free or unallocated buffers in a buffer pool.
initial	Number of additional temporary buffers that are to be allocated when the system is reloaded. This keyword can be used to ensure that the system has necessary buffers immediately after reloading in a high-traffic environment.
number	Number of buffers to be allocated.

[**no**] **buffers huge size** *number*

Use the **buffers huge size** global configuration command to dynamically resize all huge buffers to the value you specify. Use the **no** form of this command to restore the default buffer values.

number	Number of buffers to be allocated

calendar set *hh:mm:ss day month year*
calendar set *hh:mm:ss month day year*

To set the Cisco 7000 series or Cisco 4500 series system calendar, use the **calendar set** EXEC command.

hh:mm:ss	Current time in hours (military format), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

cdp enable

To enable CDP on an interface, use the **cdp enable** interface configuration command. Use the **no** form of this command to disable CDP on an interface.

cdp holdtime *seconds*
no cdp holdtime

To specify the amount of time the receiving device should hold a CDP packet from your router before discarding it, use the **cdp holdtime** global configuration command. Use the **no** form of this command to revert to the default setting.

seconds	Specifies the hold time to be sent in the CDP update packets.

cdp run

To enable CDP on your router, use the **cdp run** global configuration command. Use the **no** form of this command to disable CDP.

cdp timer *seconds*
no cdp timer

To specify how often your router will send CDP updates, use the **cdp timer** global configuration command. Use the **no** form of this command to revert to the default setting.

seconds	Specifies how often your router will send CDP updates.

clear cdp counters

To reset CDP traffic counters to zero (0) on your router, use the **clear cdp counters** privileged EXEC command.

clear cdp table

To clear the table that contains CDP information about neighbors, use the **clear cdp table** privileged EXEC command.

[**no**] **clock calendar-valid**

To configure the Cisco 7000 series or Cisco 4500 series router as a time source for a network based on its calendar, use the **clock calendar-valid** global configuration command. Use the **no** form of this command to set the router so that the calendar is not an authoritative time source.

clock read-calendar

To manually read the calendar into the Cisco 7000 series or Cisco 4500 series system clock, use the **clock read-calendar** EXEC command.

clock set *hh:mm:ss day month year*
clock set *hh:mm:ss month day year*

To manually set the system clock, use the **clock set** EXEC command.

hh:mm:ss	Current time in hours (military format), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

clock summer-time *zone* **recurring** [*week day month hh:mm week day month hh:mm* [*offset*]]
clock summer-time *zone* **date** *date month year hh:mm date month year hh:mm* [*offset*]
clock summer-time *zone* **date** *month date year hh:mm month date year hh:mm* [*offset*]
no clock summer-time

To configure the system to automatically switch to summer time (daylight savings time), use one of the formats of the **clock summer-time** configuration command. Use the **no** form of this command to configure the router not to automatically switch to summer time.

zone	Name of the time zone (PDT, ...) to be displayed when summer time is in effect.
week	Week of the month (1 to 5 or **last**).
day	Day of the week (Sunday, Monday, ...).
date	Date of the month (1 to 31).
month	Month (January, February, ...).
year	Year (1993 to 2035).
hh:mm	Time (military format) in hours and minutes.
offset	(Optional) Number of minutes to add during daylight savings time (default is 60).

clock timezone *zone hours* [*minutes*]
no clock timezone

To set the time zone for display purposes, use the **clock timezone** global configuration command. To set the time to Coordinated Universal Time (UTC), use the **no** form of this command.

zone	Name of the time zone to be displayed when standard time is in effect.
hours	Hours offset from UTC.
minutes	(Optional) Minutes offset from UTC.

clock update-calendar

To set the Cisco 7000 series or Cisco 4500 series calendar from the system clock, use the **clock update-calendar** EXEC command.

custom-queue-list *list*
no custom-queue-list [*list*]

To assign a custom queue list to an interface, use the **custom-queue-list** interface configuration command. To remove a specific list or all list assignments, use the **no** form of this command.

list — Number of the custom queue list you want to assign to the interface. An integer from 1 to 10.

[**no**] **enable last-resort** {**password** | **succeed**}

To specify what happens if the TACACS servers used by the **enable** command do not respond, use the **enable last-resort** global configuration command. The **no** form of this command restores the default.

password — Allows you to enable by entering the privileged command level password.

succeed — Allows you to enable without further question.

enable password [**level** *level*] [*encryption-type*] *password*
no enable password [**level** *level*]

To assign a password for the privileged command level, use the **enable password** global configuration command. The commands **enable password** and **enable-password** are synonymous.

level *level* — (Optional) Level for which the password applies.

encryption-type — (Optional) Type of password encryption. Can be 0 or 7. 0 indicates that the password that follows has not yet been encrypted. 7 indicates that the password has been encrypted using Cisco-proprietary encryption.

password	Case-sensitive character string that specifies the line password prompted for in response to the EXEC command **enable**. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the *password* in the format *number-space-anything*. The space after the number causes problems.

[**no**] **enable use-tacacs**

To enable use of the TACACS to determine whether a user can access the privileged command level, use the **enable use-tacacs** global configuration command. Use the **no** form of this command to disable TACACS verification.

hostname *name*

To specify or modify the host name for the network server, use the **hostname** global configuration command. The host name is used in prompts and default configuration filenames. The **setup** command facility also prompts for a host name at startup.

name	New host name for the network server; the name is case sensitive.

[no] load-interval *seconds*

To change the length of time for which data is used to compute load statistics, use the **load-interval** interface configuration command. Use the **no** form of this command to revert to the default setting.

seconds	Length of time for which data is used to compute load statistics. A value that is a multiple of thirty, between 30 and 600 (30, 60, 90, 120, and so forth).

[**no**] **logging** *host*

To log messages to a syslog server host, use the **logging** global configuration command. The **no** form of this command deletes the syslog server with the specified address from the list of syslogs.

host Name or IP address of the host to be used as a syslog server.

[**no**] **logging buffered**

To log messages to an internal buffer, use the **logging buffered** global configuration command. The **no** form of this command cancels the use of the buffer and writes messages to the console terminal, which is the default.

logging console *level*
no logging console

To limit messages logged to the console based on severity, use the **logging console** global configuration command. The **no** form of this command disables logging to the console terminal.

level Limits the logging of messages displayed on the console terminal to the named level. See the *level* keywords table for this command in the *Router Products Command Reference* publication.

logging facility *facility-type*
no logging facility

To configure the syslog facility in which error messages are sent, use the **logging facility** global configuration command. To revert to the default of local7, use the **no** form of this global configuration command.

facility-type Syslog facility. See the *facility-type* keywords table for this command in the *Router Products Command Reference* publication.

logging monitor *level*
no logging monitor

To limit messages logged to the terminal lines (monitors) based on severity, use the **logging monitor** global configuration command. This command limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above *level*. The **no** form of this command disables logging to terminal lines other than the console line.

level	One of the *level* keywords. See the *level* keywords table for this command in the *Router Products Command Reference* publication.

[**no**] **logging on**

To control logging of error messages, use the **logging on** global configuration command. This command enables message logging to all destinations except the console terminal. The **no** form of this command enables logging to the console terminal only.

[**no**] **logging synchronous** [**level** *severity-level* | **all**] [**limit** *number-of-buffers*]

To synchronize unsolicited messages and debug output with solicited router output and prompts for a specific console port line, auxiliary port line, or virtual terminal line, use the **logging synchronous** line configuration command. The no form of this command disables the synchronizing of messages.

level *severity-level*	(Optional) Message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. When specifying a severity level number, consider that for the logging system, low numbers indicate greater severity and high numbers indicate lesser severity. The default value is 2.

all (Optional) Specifies that all messages are printed asynchronously, regardless of the severity level.

limit *number-of-buffers* (Optional) Number of buffers to be queued for the terminal after which new messages are dropped. The default value is 20.

logging trap *level*
no logging trap

To limit messages logged to the syslog servers based on severity, use the **logging trap** global configuration command. The command limits the logging of error messages sent to syslog servers to only those messages at the specified level. The **no** form of this command disables logging to syslog servers.

level One of the *level* keywords. See the *level* keywords table for this command in the *Router Products Command Reference* publication.

[**no**] **login authentication** {**default** | *list-name*}

To enable TACACS+ authentication for logins, use the **login authentication** line configuration command. Use the **no** form of the command to return to the default.

default Uses the default list created with the **aaa authentication login** command.

list-name Uses the indicated list created with the **aaa authentication login** command.

ntp access-group {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*
no ntp access-group {**query-only** | **serve-only** | **serve** | **peer**}

To control access to the system's Network Time Protocol (NTP) services, use the **ntp access-group** global configuration command. To remove access control to the system's NTP services, use the **no** form of this command.

query-only	Allows only NTP control queries. See RFC 1305 (NTP Version 3).
serve-only	Allows only time requests.
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
access-list-number	Number (1 to 99) of a standard IP access list.

[**no**] **ntp authenticate**

To enable NTP authentication, use the **ntp authenticate** global configuration command. Use the **no** form of this command to disable the feature.

ntp authentication-key *number* **md5** *value*
no ntp authentication-key *number*

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** global configuration command. Use the **no** form of this command to remove the authentication key for NTP.

number	Key number (1 to 4294967295).
value	Key value (an arbitrary string of up to eight characters).

ntp broadcast [**version** *number*]
no ntp broadcast

To specify that a specific interface should send Network Time Protocol (NTP) broadcast packets, use the **ntp broadcast** interface configuration command. Use the **no** form of this command to disable this capability.

version *number*	(Optional) Number from 1 to 3 indicating the NTP version.

ntp broadcast client
no ntp broadcast client

To allow the system to receive NTP broadcast packets on an interface, use the **ntp broadcast client** command. Use the **no** form of this command to disable this capability.

ntp broadcastdelay *microseconds*
no ntp broadcastdelay

To set the estimated round-trip delay between the router and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** global configuration command. Use the **no** form of this command to revert to the default value.

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999. The default is 3000.

ntp clock-period *value*

Do not enter this command; it is documented for informational purposes only. The system automatically generates this command as Network Time Protocol (NTP) determines the clock error and compensates.

As NTP compensates for the error in the system clock, it keeps track of the correction factor for this error. The system automatically saves this value into the system configuration using the **ntp clock-period** global configuration command. The system uses the **no** form of this command to revert to the default.

ntp disable
no ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** interface configuration command. To enable receipt of NTP packets on an interface, use the **no** form of this interface configuration command.

[**no**] **ntp master** [*stratum*]

To configure the router as an NTP master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp maste**r global configuration command. To disable the master clock function, use the **no** form of this command.

stratum	(Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.

ntp peer *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]
no ntp peer *ip-address*

To configure the router's system clock to synchronize a peer or to be synchronized by a peer, use the **ntp peer** global configuration command. To disable this capability, use the **no** form of this command.

ip-address	IP address of the peer providing, or being provided, the clock synchronization.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
keyid	(Optional) Authentication key to use when sending packets to this peer.

source (Optional) Identifies the interface from which to pick the IP source address.

interface (Optional) Name of the interface from which to pick the IP source address.

prefer (Optional) Makes this peer the preferred peer that provides synchronization.

ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*]
[**prefer**]
no ntp server *ip-address*

To allow the router's system clock to be synchronized by a time server, use the **ntp server** global configuration command. To disable this capability, use the **no** form of this command.

ip-address IP address of the time server providing the clock synchronization.

version (Optional) Defines the Network Time Protocol (NTP) version number.

number (Optional) NTP version number (1 to 3).

key (Optional) Defines the authentication key.

keyid (Optional) Authentication key to use when sending packets to this peer.

source (Optional) Identifies the interface from which to pick the IP source address.

interface (Optional) Name of the interface from which to pick the IP source address.

prefer (Optional) Makes this server the preferred server that provides synchronization.

ntp source *interface*
no ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** global configuration command. Use the **no** form of this command to remove the specified source address.

interface	Any valid system interface name.

[**no**] **ntp trusted-key** *key-number*

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** global configuration command. Use the **no** form of this command to disable authentication of the identity of the system.

key-number	Key number of authentication key to be trusted.

[**no**] **ntp update-calendar**

To periodically update the Cisco 7000 series calendar from Network Time Protocol (NTP), use the **ntp update-calendar** global configuration command. Use the **no** form of this command to disable this feature.

ping [*protocol*] {*host* | *address*}

Use the **ping** (packet internet groper) user or privileged EXEC or user command to diagnose basic network connectivity on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

protocol	(Optional) Protocol keyword—one of **apollo**, **appletalk**, **clns**, **decnet**, **ip**, **ipx**, **vines**, or **xns.**
host	Host name of system to ping.
address	Address of system to ping.

ppp authentication {**chap** | **pap**} [**if-needed**] [*list-name*]
no ppp authentication

To enable Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and to enable an AAA authentication method on an interface, use the **ppp authentication** interface configuration command. Use the **no** form of the command to disable this authentication.

chap	Enables CHAP on a serial interface.
pap	Enables PAP on a serial interface.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
list-name	(Optional) Used with AAA/TACACS+. Specifies the name of a list of AAA methods of authentication to use. If no listname is specified, the system uses the default. Lists and default are created with the **aaa authentication ppp** command.

ppp use-tacacs [**single-line**]
no ppp use-tacacs

To enable TACACS for PPP authentication, use the **ppp use-tacacs** interface configuration command. Use the **no** form of this command to disable TACACS for PPP authentication.

single-line	(Optional) Accept the username and password in the username field. This option applies only when using CHAP authentication.

priority-group *list*
no priority-group

To assign the specified priority list to an interface, use the **priority-group** interface configuration command. Use the **no** form of this command to remove the specified **priority-group** assignment.

list	Priority list number assigned to the interface.

[**no**] **priority-list** *list-number* **default** {**high** | **medium** | **normal** | **low**}

To assign a priority queue for those packets that do not match any other rule in the priority list, use the **priority-list default** global configuration command. Use the **no** form of this command to return to the default or assign **normal** as the default.

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
high | **medium** | **normal** | **low**	Priority queue level.

[**no**] **priority-list** *list-number* **interface** *interface-type interface-number*
{**high** | **medium** | **normal** | **low**}

To establish queuing priorities on packets entering from a given interface, use the **priority-list interface** global configuration command. Use the **no** form of this command with the appropriate arguments to remove an entry from the list.

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
interface-type	Name of the interface.
interface-number	Number of the specified interface.
high | **medium** | **normal** | **low**	Priority queue level.

priority-list *list-number* **protocol** *protocol-name* {**high** | **medium** |
normal | **low**} *queue-keyword keyword-value*
no priority-list *list-number* **protocol**

To establish queuing priorities based upon the protocol type, use the **priority-list protocol** global configuration command. Use the **no** form of this command with the appropriate list number to remove an entry from the list.

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
protocol-name	Specifies the protocol type: **aarp**, **arp**, **apollo**, **appletalk**, **bridge** (transparent), **clns**, **clns_es**, **clns_is**, **compressedtcp**, **cmns**, **decnet**, **decnet_node**,**decnet_router-l1**, **decnet_router-l2**, **ip**, **ipx**, **pad**, **rsrb**, **stun**, **vines**, **xns**, and **x25**.
high | **medium** | **normal** | **low**	Priority queue level.
queue-keyword keyword-value	Possible queue keywords are **fragments**, **gt**, **lt**, **list**, **tcp**, and **udp**. See the queue keywords table for this command in the *Router Products Command Reference* publication.

priority-list *list-number* **queue-limit** *high-limit medium-limit normal-limit low-limit*
no priority-list *list-number* **queue-limit**

To specify the maximum number of packets that can be waiting in each of the priority queues, use the **priority-list queue-limit** global configuration command. The **no** form of this command selects the normal queue.

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
high-limit medium-limit normal-limit low-limit	Priority queue maximum length. A value of 0 for any of the four arguments means that the queue can be of unlimited size for that particular queue.

[**no**] **priority-list** *list-number* **stun** {**high** \| **medium** \| **normal** \| **low**} **address** *group-number address*

To establish queuing priorities based on the address of the serial link on a STUN connection, use the **priority-list stun** global configuration command. Use the **no** form of this command with the appropriate arguments to remove an entry from the list.

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
high | **medium** | **normal** | **low**	Priority queue level.
address	Required keyword.
group-number	Group number used in the **stun group** command.

address	Address of the serial link. The format of the address is either a 1-byte hex value (for example, C1) for an SDLC link or one that is specified by the **stun schema** global configuration command.

[**no**] **privilege** *mode* **level** *level command*

To set the privilege level for a command, use the **privilege level** global configuration command. Use the no form of this command to revert to default privileges for a given command.

mode	Configuration mode. See the mode argument options table in the description of the **alias** command in the *Router Products Command Reference* publication for a list of acceptable options.
level	Privilege level to be associated with the specified command. You can specify up to sixteen privilege levels, using numbers 0 through 15.
command	Command to which privilege level is associated.

[**no**] **privilege level** *level*

To set the default privilege level for a line, use the **privilege level** line configuration command. Use the **no** form of this command to restore the default user privilege level to the line.

level	Privilege level to be associated with the specified line.

[**no**] **prompt** *string*

To customize the router prompt, use the **prompt** global configuration command. To revert to the default router prompt, use the **no** form of this command.

string	Router prompt. It can consist of all printing characters and the escape sequences listed in the "Custom Router Prompt Escape Sequences" table in the *Router Products Command Reference* publication.

[**no**] **queue-list** *list-number* **default** *queue-number*

To assign a priority queue for those packets that do not match any other rule in the queue list, use the **queue-list default** global configuration command. To restore the default value, use the **no** form of this command.

list-number	Number of the queue list. An integer from 1 to 10.
queue-number	Number of the queue. An integer from 1 to 10.

queue-list *list-number* **interface** *interface-type interface-number*
queue-number
no queue-list *list-number* **interface** *queue-number*

To establish queuing priorities on packets entering on an interface, use the **queue-list interface** global configuration command. To remove an entry from the list, use the **no** form of this command.

list-number	Number of the queue list. An integer from 1 to 10.
interface-type	Required argument that specifies the name of the interface.
interface-number	Number of the specified interface.
queue-number	Number of the queue. An integer from 1 to 10.

queue-list *list-number* **protocol** *protocol-name queue-number*
queue-keyword keyword-value
no queue-list *list-number* **protocol** *protocol-name*

To establish queuing priority based upon the protocol type, use the **queue-list protocol** global configuration command. Use the **no** form of this command with the appropriate list number to remove an entry from the list.

list-number	Number of the queue list. An integer from 1 to 10.
protocol-name	Required argument that specifies the protocol type: **aarp**, **arp**, **apollo**, **appletalk**, **bridge** (transparent), **clns**, **clns_es**, **clns_is**, **compressedtcp**, **cmns**, **decnet**, **decnet_node**, **decnet_router-l1**, **decnet_router-l2**, **ip**, **ipx**, **pad**, **rsrb**, **stun**, **vines**, **xns**, and **x25**.
queue-number	Number of the queue. An integer from 1 to 10.
queue-keyword keyword-value	Possible keywords are **gt**, **lt**, **list**, **tcp**, and **udp**. See the queue keywords table for this command in the *Router Products Command Reference* publication.

[**no**] **queue-list** *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

To designate the byte size allowed per queue, use the **queue-list queue byte-count** global configuration command. To return the byte size to the default value, use the **no** form of this command.

list-number	Number of the queue list. An integer from 1 to 10.
queue-number	Number of the queue. An integer from 1 to 10.
byte-count-number	Specifies the lower boundary on how many bytes the system allows to be delivered from a given queue during a particular cycle.

[**no**] **queue-list** *list-number* **queue** *queue-number* **limit** *limit-number*

To designate the queue length limit for a queue, use the **queue-list queue limit** global configuration command. To return the queue length to the default value, use the **no** form of this command.

list-number	Number of the queue list. An integer from 1 to 10.
queue-number	Number of the queue. An integer from 1 to 10.
limit-number	Maximum number of packets which can be queued at any time. Range is 0 to 32767 queue entries.

[**no**] **queue-list** *list-number* **stun** *queue-number* **address** *group-number address-number*

To establish queuing priorities based on the address of the serial link on a STUN connection, use the **queue-list stun** global configuration command. Use the **no** form of this command with the appropriate arguments to remove an entry from the list.

list-number	Number of the queue list. An integer from 1 to 10.
queue-number	Queue number in the range from 1 to 10.
address	Required keyword.
group-number	Group number used in the **stun group** command.
address-number	Address of the serial link. The format of the address is either a 1-byte hex value (for example, C1) for an SDLC link or one that is specified by the **stun schema** configuration command.

scheduler-interval *milliseconds*
no scheduler-interval

To control the maximum amount of time that can elapse without running the lowest-priority system processes, use the **scheduler-interval** global configuration command. The **no** form of this command restores the default.

milliseconds	Integer that specifies the interval, in milliseconds. The minimum interval that you can specify is 500 milliseconds; there is no maximum value.

[**no**] **service exec-wait**

To delay the startup of the EXEC on noisy lines, use the **service exec-wait** global configuration command. Use the **no** form of this command to disable this feature.

[**no**] **service nagle**

To enable the Nagle congestion control algorithm, use the **service nagle** global configuration command. Use the **no** form of this command to disable this feature.

[**no**] **service password-encryption**

To encrypt passwords, use the **service password-encryption** global configuration command. Use the **no** form of this command to disable this service.

[**no**] **service tcp-keepalives** {**in** | **out**}

To generate keepalive packets on idle network connections, use the **service tcp-keepalives** global configuration command. The **no** form of this command with the appropriate keyword disables the keepalives.

in	Generates keepalives on incoming connections (initiated by remote host).
out	Generates keepalives on outgoing connections (initiated by a user).

[**no**] **service telnet-zero-idle**

To set the TCP window to zero (0) when the Telnet connection is idle, use the **service telnet-zero-idle** global configuration command. Use the **no** form of this command to disable this feature.

service timestamps [*type* **uptime**]
service timestamps *type* **datetime** [**msec**] [**localtime**] [**show-timezone**]
no service timestamps [*type*]

To configure the system to timestamp debugging or logging messages, use one of the **service timestamps** global configuration commands. Use the **no** form of this command to disable this service.

type	(Optional) Type of message to timestamp: debug or log.
uptime	(Optional) Timestamp with time since the system was rebooted.
datetime	Timestamp with the date and time.
msec	(Optional) Include milliseconds with the date and time.
localtime	(Optional) Timestamp relative to the local time zone.
show-timezone	(Optional) Include the time zone name in the timestamp.

show aliases [*mode*]

To display all alias commands, or the alias commands in a specified mode, use the **show aliases** EXEC command.

mode	(Optional) Command mode. See the mode argument options table in the description of the **alias** command for acceptable options for the *mode* argument.

show buffers [**all** | **alloc** [**dump**]]
show buffers interface [*type number* [**alloc** [**dump**]]]

Use the **show buffers** EXEC command to display statistics for the buffer pools on the network server.

all	(Optional) Displays all public and interface pool information.
alloc	(Optional) Displays a brief listing of all allocated buffers. When **alloc** is specified after **interface** *type number*, displays a brief listing of buffers allocated for that interface.
dump	(Optional) Dumps all allocated buffers. This keyword must be used with the **alloc** keyword, not by itself. When **alloc dump** is specified after **interface** *type number*, dumps buffers allocated for that interface.
interface [*type number*]	(Optional) Displays all interface pool information. If the specified interface *type* and *number* has its own buffer pool, displays information for that pool. Value of *type* can be **ethernet**, **serial**, or **tokenring**.

show calendar

To display the calendar hardware setting for the Cisco 7000 series or Cisco 4500 series, use the **show calendar** EXEC command.

show cdp

To display global CDP information, including timer and hold-time information, use the **show cdp** privileged EXEC command.

show cdp entry *entry-name* [**protocol** | **version**]

To display information about a neighbor device listed in the CDP table, use the **show cdp entry** privileged EXEC command.

entry-name	Name of neighbor about which you want information.
protocol	(Optional) Limits the display to information about the protocols enabled on a device.
version	(Optional) Limits the display to information about the version of software running on the device.

show cdp interface [*type number*]

To display information about the interfaces on which CDP is enabled, use the **show cdp interface** command.

type	(Optional) Type of interface about which you want information.
number	(Optional) Number of the interface about which you want information.

show cdp neighbors [*interface-type interface-number*] [**detail**]

To display information about neighbors, use the **show cdp neighbors** privileged EXEC command.

interface-type	(Optional) Type of the interface connected to the neighbors about which you want information.
interface-number	(Optional) Number of the interface connected to the neighbors about which you want information.
detail	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

show cdp traffic

To display traffic information from the CDP table, use the **show cdp traffic** privileged EXEC command.

show clock [detail]

To display the system clock, use the **show clock** EXEC command.

detail	(Optional) Indicates the clock source (NTP, VINES, 7000 calendar, and so forth) and the current summertime setting (if any).

show environment

Use the **show environment** EXEC command to display temperature and voltage information on the AGS+ and Cisco 7000 series console.

show environment all

Use the **show environment all** EXEC command to display temperature and voltage information on the Cisco 7000 series console.

show environment last

After a shutdown occurs due to detection of fatal environmental margins, use the **show environment last** EXEC command to display the last measured value from each of six test points on the CSC-ENVM (on the AGS+) or the route processor (RP) (on the Cisco 7000 series).

show environment table

Use the **show environment table** EXEC command to display environmental measurements and a table that lists the ranges of environment measurement that are within specification. This command is available on the Cisco 7000 series only.

show logging

Use the **show logging** EXEC command to display the state of syslog error and event logging, including host addresses, and whether console logging is enabled, and also to display Simple Network Management Protocol (SNMP) configuration parameters and protocol activity.

show memory [*type*] [**free**]

Use the **show memory** EXEC command to show statistics about the router's memory, including memory free pool statistics.

type (Optional) Memory type to display (processor, multibus, io, sram). If type is not specified, statistics for all memory types present in the router will be displayed.

free (Optional) Displays free memory statistics.

show ntp associations [**detail**]

To show the status of Network Time Protocol (NTP) associations, use the **show ntp associations** EXEC command.

detail (Optional) Shows detailed information about each NTP association.

show ntp status

To show the status of Network Time Protocol (NTP), use the **show ntp status** EXEC command.

show privilege

To display your current level of privilege, use the **show privilege** EXEC command.

show processes [cpu]

Use the **show processes** EXEC command to display information about the active processes.

cpu	(Optional) Displays detailed CPU utilization statistics.

show processes memory

Use the **show processes memory** EXEC command to show memory utilization.

show protocols

Use the **show protocols** EXEC command to display the global and interface-specific status of any configured Level 3 protocol; for example, IP, DECnet, IPX, AppleTalk, and so forth.

show queueing [custom | priority]

To list the current state of the queue lists, use the **show queueing** privileged EXEC command.

custom	(Optional) Shows status of custom queue lists.
priority	(Optional) Shows status of priority lists.

show snmp

To check the status of communications between the SNMP agent and SNMP manager, use the **show snmp** EXEC command.

show stacks

Use the **show stacks** EXEC command to monitor the stack utilization of processes and interrupt routines, including the reason for the last system reboot; if the system was reloaded because of a system failure, a saved system stack trace is displayed.

[**no**] **snmp-server access-list** *list-number*

To set up an access list that determines which hosts can send requests to the network server, use the **snmp-server access-list** global configuration command. Use the **no** form of this command to remove the specified access list.

list-number	Integer from 1 to 99 that specifies an IP access list number.

snmp-server access-policy *destination-party source-party context privileges*
no snmp-server access-policy *destination-party source-party context*

To create or update an access policy, use the **snmp-server access-policy** global configuration command. To remove the specified access policy, use the **no** form of this command.

destination-party	Name of a previously defined party identified as the destination party or target for this access policy. This name serves as a label used to reference a record defined for this party through the **snmp-server party** command. A destination party performs management operations that are requested by a source party.
source-party	Name of a previously defined party identified as the source party or subject for this access policy. This name serves as a label used to reference a record defined for this party through the **snmp-server party** command. A source party sends communications to a destination party requesting the destination party to perform management operations.

context — Name of a previously defined context that defines the resources for the access policy. This name serves as a label used to reference a record defined for this context through the **snmp-server context** command. A context identifies object resources accessible to a party.

privileges — Bit mask representing the access privileges that govern the management operations that the source party can ask the destination party to perform. Use decimal or hexadecimal format to specify privileges as a sum of values in which each value specifies an SNMP PDU type that the source party can use to request an operation. The decimal values are defined as follows:

- Get =1
- GetNext = 2
- Response = 4
- Set = 8
- SNMPv1-Trap = 16
- GetBulk = 32
- SNMPv2-Trap = 128

snmp-server chassis-id *text*
no snmp-server chassis-id

To provide a message line identifying the SNMP server serial number, use the **snmp-server chassis-id** global configuration command. Use the **no** form of this command to remove the message line.

text — Message you want to enter to identify the chassis serial number.

snmp-server community *string* [**RO** | **RW**] [*number*]
no snmp-server community *string*

To set up the community access string to permit access to the SNMPv1 protocol, use the **snmp-server community** global configuration command. The **no** form of this command removes the specified community string. The **no snmp-server** command disables both versions of SNMP (SNMPv1 and SNMPv2).

string	Community string that acts like a password and permits access to the SNMP protocol.
RO	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects. The default is **RO**.
RW	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.The default is **RO**.
number	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that may use the community string to gain access to the SNMPv1 agent.

snmp-server contact *text*
no snmp-server contact

To set the system contact (syscontact) string, use the **snmp-server contact** global configuration command. Use the **no** form of this command to remove the system contact information.

text	String that describes the system contact information.

snmp-server context *context-name context-oid view-name*
no snmp-server context *context-name*

To create or update a context record, use the **snmp-server context** global configuration command. To remove a specific context entry, use the **no** form of this command.

context-name	Name of the context to be created or updated. This name serves as a label used to reference a record for this context.
context-oid	Object identifier to assign to the context. Specify this value in dotted decimal notation, with an optional text identifier; for example, 1.3.6.1.6.3.3.1.4.131.108.45.11.1(== initialContextId.131.108.45.11.1).
view-name	Name of a previously defined view. The view defines the objects available to the context.

snmp-server host *address community-string* [**snmp**] [**tty**]
no snmp-server host *address community-string*

To specify the recipient of an SNMP trap operation, use the **snmp-server host** global configuration command. The **no** form of this command removes the specified host.

address	Name or IP address of the host.
community-string	Password-like community string to send with the trap operation.
snmp	(Optional) Enables the SNMP traps defined in RFC 1157.
tty	(Optional) Enables Cisco enterprise-specific traps when a TCP connection closes.

snmp-server location *text*
no snmp-server location

To set the system location string, use the **snmp-server location** global configuration command. Use the **no** form of this command to remove the location string.

text String that describes the system location information.

snmp-server packetsize *byte-count*
no snmp-server packetsize

To specify the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply, use the **snmp-server packetsize** global configuration command. Use the **no** form of this command to restore the default value.

byte-count Integer byte count from 484 to 8192.

snmp-server party *party-name party-oid* [*protocol-address*]
[**packetsize** *size*] [**local | remote**] [**authentication**
{**md5** *key* [**clock** *clock*] [**lifetime** *lifetime*] | **snmpv1** *string*}]
no snmp-server party *partyname*

To create or update a party record, use the **snmp-server party** global configuration command. To remove a specific party entry, use the **no** form of this command.

party-name Name of the party characterized by the contents of the record. This name serves as a label used to reference the party record that you are creating or modifying.

party-oid Object identifier to assign to the party. Specify this value in dotted decimal notation, with an optional text identifier; for example, 1.3.6.1.6.3.3.1.3.131.108.34.54.1 (= initialPartyId.131.108.34.54.1) *protocol-address* (Optional) Address of the protocol that the party record pertains to. Currently the only supported protocol is UDP, so this value specifies a UDP address in the format *a.b.c.d port*. In future releases, additional protocols will be supported. This value is used to specify the destination of trap messages.

packetsize *size* (Optional) Maximum size in bytes of a message that this party is able to receive. By default, the packet size set through the **snmp-server packetsize** command is used.

local | **remote** (Optional) Indicates that the party is local or remote. If neither **local** nor **remote** is specified, a default value of **local** is assumed.

authentication (Optional) Indicates that the party uses an authentication protocol. If specified, either **md5** or **snmpv1** is required.

md5 *key* (Optional) Indicates that the party uses the Message Digest algorithm MD5 for message authentication. If **md5** is specified, you must also specify a 16-byte hexadecimal ASCII string representing the MD5 authentication key for the party.

clock *clock* (Optional) Initial value of the authentication clock.

lifetime *lifetime* (Optional) Lifetime, in seconds, that represents the upper bound on acceptable delivery delay for messages generated by the party.

snmpv1 *string* (Optional) Community string. The keyword **snmpv1** indicates that the party uses community-based authentication.

All messages sent to this party will be authenticated using the SNMPv1 community string specified by *string* instead of MD5.

snmp-server queue-length *length*

To establish the message queue length for each trap host, use the **snmp-server queue-length** global configuration command.

length	Integer that specifies the number of trap events that can be held before the queue must be emptied.

[**no**] **snmp-server system-shutdown**

To use the SNMP message reload feature, use the **snmp-server system-shutdown** global configuration command. The **no** form of this command prevents an SNMP system-shutdown request (from an SNMP manager) from resetting the Cisco agent.

[**no**] **snmp-server trap-authentication** [**snmpv1 | snmpv2**]

To establish trap message authentication, use the **snmp-server trap-authentication** global configuration command. To remove message authentication, use the **no snmp-server trap-authentication** command.

snmpv1	(Optional) Indicates that SNMP authentication traps will be sent to SNMPv1 management stations only. If no keyword is specified, trap message authentication is turned on by default. In this case, messages are sent to the host that is specified though the **snmp-server host** command and to any SNMP stations configured through access policies to receive trap messages.
snmpv2	(Optional) Indicates that SNMP authentication traps will be sent to SNMPv2 management stations only. If no keyword is specified, trap message authentication is turned on by default. In this case, messages are sent to the host that is specified though the **snmp-server host** command and to any SNMP stations configured through access policies to receive trap messages.

snmp-server trap-source *interface*
no snmp-server trap-source

To specify the interface (and hence the corresponding IP address) that an SNMP trap should originate from, use the **snmp-server trap-source** global configuration command. Use the **no** form of this command to remove the source designation.

interface	Interface from which the SNMP trap originates. The argument includes the interface type and number in platform-specific syntax.

snmp-server trap-timeout *seconds*

To define how often to try resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** global configuration command.

seconds	Integer that sets the interval, in seconds, for resending the messages.

snmp-server userid *user-id* [**view** *view-name*] [**RO** | **RW**]
[**password** *password*]
no snmp-server userid *user-id*

To create or update an SNMPv2 security context using the simplified security conventions method, use the **snmp-server userid** global configuration command. The **no** form of this command removes the specified security context.

user-id	User ID name that identifies an approved SNMPv2 user. The user ID represents a set of security information for this user. This value can identify a particular user of the system or a background process.

view *view-name*	(Optional) View to be used for this security context. The argument *view-name* must be the name of a predefined view. For authenticated users, defaults to the predefined view *everything.* For users who are not authenticated, defaults to the predefined view *restricted.*
RO	(Optional) Specifies read-only access.This is the default for unauthenticated users.
RW	(Optional) Specifies read-write access. This is the default for authenticated users.
password *password*	(Optional) If specified, indicates that this is an authenticated user, and defines the password used to authenticate the user. The password must be at least eight characters long.

snmp-server view *view-name oid-tree* {**included** | **excluded**}
no snmp-server view *view-name*

To create or update a view entry, use the **snmp-server view** global configuration command. To remove the specified SNMP server view entry, use the **no** form of this command.

view-name	Label for the view record that you are updating or creating. The name is used to reference the record.
oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as *1.3.6.2.4*, or a word, such as *system*. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
included | **excluded**	Type of view. Either **included** or **excluded** is required.

tacacs-server attempts *count*
no tacacs-server attempts

To control the number of login attempts that can be made on a line set up for TACACS verification, use the **tacacs-server attempts** global configuration command. Use the **no** form of this command to remove this feature and restore the default.

count	Integer that sets the number of attempts.

tacacs-server authenticate {**connection** [**always**] | **enable** | **slip** [**always**] [**access-lists**]}

To specify that the network or router must respond indicating whether the user may perform an action when the user attempts to perform the action, use the **tacacs-server authenticate** global configuration command.

connection	Configures a required response when a user makes a TCP connection.
always	(Optional) Performs authentication even when a user is not logged in. This option only applies to the **connection** or **slip** keywords.
enable	Configures a required response when a user enters the **enable** command.
slip	Configures a required response when a user starts a SLIP or PPP session.
access-lists	(Optional) Requests and installs access lists. This option only applies to the **slip** keyword.

[**no**] **tacacs-server extended**

To enable an extended TACACS mode, use the **tacacs-server extended** global configuration command. Use the **no** form of this command to disable the mode.

[**no**] **tacacs-server host** *name*

To specify a TACACS host, use the **tacacs-server host** global configuration command. You can use multiple **tacacs-server host** commands to specify multiple hosts. The software searches for the hosts in the order you specify them. The **no** form of this command deletes the specified name or address.

name	Name or IP address of the host.

[**no**] **tacacs-server last-resort** {**password** \| **succeed**}

To cause the network server to request the privileged password as verification, or to force successful login without further input from the user, use the **tacacs-server last-resort** global configuration command. The **no** form of this command restores the system to the default behavior.

password	Allows the user to access the EXEC command mode by entering the password set by the **enable** command.
succeed	Allows the user to access the EXEC command mode without further question.

tacacs-server notify {**connection** [**always**] \| **enable** \| **logout** [**always**] \| **slip** [**always**]}

Use the **tacacs-server notify** global configuration command to cause a message to be transmitted to the TACACS server, with retransmission being performed by a background process for up to 5 minutes.

connection	Specifies that a message be transmitted when a user makes a TCP connection.
always	(Optional) Sends a message even when a user is not logged in. This option applies only to SLIP or PPP sessions and can be used with the **connection**, **logout**, or **slip** keywords.

enable	Specifies that a message be transmitted when a user enters the **enable** command.
logout	Specifies that a message be transmitted when a user logs out.
slip	Specifies that a message be transmitted when a user starts a SLIP or PPP session.

[**no**] **tacacs-server optional-passwords**

To specify that the first TACACS request to a TACACS server be made *without* password verification, use the **tacacs-server optional-passwords** global configuration command. Use the **no** form of this command to restore the default.

tacacs-server retransmit *retries*
no tacacs-server retransmit

To specify the number of times the router software will search the list of TACACS server hosts before giving up, use the **tacacs-server retransmit** global configuration command. The **no** form of this command restores the default.

retries	Integer that specifies the retransmit count. The router software will try all servers, allowing each one to time out before increasing the *retries* count.

tacacs-server timeout *seconds*
no tacacs-server timeout

To set the interval that the server waits for a server host to reply, use the **tacacs-server timeout** global configuration command. The **no** form of this command restores the default.

seconds	Integer that specifies the timeout interval in seconds.

test flash

To test Flash memory on MCI and ENVM Flash EPROM interfaces, use the **test flash** EXEC command.

test interfaces

To test the system interfaces on the modular router, use the **test interfaces** EXEC command.

test memory

To perform a test of Multibus memory (including nonvolatile memory) on the AGS+ router, use the **test memory** EXEC command.

trace [*protocol*] [*destination*]

Use the **trace** privileged EXEC command to discover the routes the router's packets will actually take when traveling to their destination.

protocol	(Optional) Protocols that can be used are **appletalk**, **clns**, **ip** and **vines**.
destination	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

trace [*protocol*] [*destination*]

Use the **trace** EXEC command to discover the IP routes the router's packets will actually take when traveling to their destination.

protocol	(Optional) Protocols that can be used are **appletalk**, **clns**, **ip** and **vines**.
destination	(Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

username *name* [**nopassword** | **password** *encryption-type password*]
username *name* **password** *secret*
username *name* [**access-class** *number*]
username *name* [**autocommand** *command*]
username *name* [**noescape**] [**nohangup**]

To establish a username-based authentication system at login, even though your network cannot support a TACACS service, use the **username** global configuration command.

name Host name, server name, user ID, or command name.

nopassword (Optional) Specifies that no password is required for this user to log in. This is usually most useful in combination with the **autocommand** keyword.

password (Optional) Specifies a possibly encrypted password for this username.

encryption-type (Optional) A single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Currently defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.

password (Optional) A password can contain embedded spaces and must be the last option specified in the **username** command.

secret For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. This prevents the secret from being stolen. The secret can consist of any string of up to 11 printable ASCII characters. There is no limit to the number of username/password combinations that can be specified, allowing any number of remote devices to be authenticated.

access-class (Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** line configuration command. It is used for the duration of the user's session.

number (Optional) The access list number.

autocommand (Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. As the command can be any length and contain imbedded spaces, commands using the **autocommand** keyword must be the last option on the line.

command (Optional) The command string.

noescape (Optional) Prevents a user from using an escape character on the host to which that user is connected.

nohangup (Optional) Prevents the router from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another login prompt.

Interface Commands

This chapter describes the function and displays the syntax of each interface command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

async default ip address *ip-address*
no async default ip address

To assign the interface address that is used by the device connecting to the router via PPP or SLIP, unless you override the address at the command line, use the **async default ip address** interface configuration command. Use the **no** form of the command to remove the address from your configuration.

ip-address	Address of the client interface.

[**no**] **async dynamic address**

To specify an address on an asynchronous interface (rather than using the default address), use the **async dynamic address** interface configuration command. Use the **no** form of this command to disable dynamic addressing.

[**no**] **async dynamic routing**

To implement asynchronous routing on an interface, use the **async dynamic routing** interface configuration command. The **no** form of this command disables use of routing protocols; static routing will still be used.

async mode dedicated
no async mode

To place a line into network mode using SLIP or PPP encapsulation, use the **async mode dedicated** interface configuration command. The **no** form of this command returns the line to interactive mode.

async mode interactive
no async mode

To enable the **slip** and **ppp** EXEC commands, use the **async mode interactive** line configuration command. Use the **no** form of this command to prevent users from implementing SLIP and PPP at the EXEC level.

atm-dxi map *protocol address vpi vci* [**broadcast**]
no atm-dxi map *protocol address*

To map a given VPI and VCI to a DXI frame address, use the **atm-dxi map** interface configuration command. Use the **no** form of this command to remove the definition.

protocol	Specifies the protocol: **apollo**, **appletalk**, **bridge**, **clns**, **decnet**, **ip**, **ipx**, **vines**, **xns**.
address	Protocol-specific address.
vpi	Specifies the Virtual Path Identifier in the range 0 to 15.
vci	Specifies the Virtual Circuit Identifier in the range 0 to 63.
broadcast	(Optional) Broadcasts should be forwarded to this address.

[**no**] **auto-polarity**

To enable automatic receiver polarity reversal on a hub port connected to an Ethernet interface of a Cisco 2505 or Cisco 2507, use the **auto-polarity** hub configuration command. To disable this feature, use the **no** form of this command.

[**no**] **backup delay** {*enable-delay* | **never**} {*disable-delay* | **never**}

To define how much time should elapse before a secondary line is set up or taken down after a primary line transition, use the **backup delay** interface configuration command. Use the **no** form of this command to remove the definition.

enable-delay Integer that specifies the delay in seconds after the primary line goes down before the secondary line is activated.

never Prevents the secondary line from being activated.

disable-delay Integer that specifies the delay in seconds after the primary line goes up before the secondary line is deactivated.

never Prevents the secondary line from being deactivated.

[**no**] **backup interface** *interface-name*
[**no**] **backup interface** *interface-name slot/port*
(for the Cisco 7000 series)

To configure the serial interface as a secondary, or dial backup line, use the **backup interface** interface configuration command. Use the **no** form of this command with the appropriate serial port designation to disable this feature.

interface-name Serial port to be set as the secondary interface line.

slot On the Cisco 7000 series, specifies the slot number.

port On the Cisco 7000 series, specifies the port number.

[**no**] **backup load** {*enable-threshold* | **never**} {*disable-load* | **never**}

To set the traffic load thresholds for dial backup service, use the **backup load** interface configuration command. Use the **no** form of this command to remove the setting.

enable-threshold	Integer that specifies a percentage of the primary line’s available bandwidth.
never	Sets the secondary line to never be activated due to load.
disable-load	Integer that specifies a percentage of the primary line’s available bandwidth.
never	Sets the secondary line to never be deactivated due to load.

bandwidth *kilobits*
no bandwidth

To set a bandwidth value for an interface, use the **bandwidth** interface configuration command. Use the **no** form of this command to restore the default values.

kilobits	Intended bandwidth in kilobits per second. For a full bandwidth DS3, enter the value **44736**.

channel-group *number* **timeslots** *range* [**speed** {**48** | **56** | **64**}]

Use the **channel-group** controller configuration command to define the timeslots that belong to each T1 circuit.

number	Channel-group number. When configuring a T1 data line, channel-group numbers can be a value from 0 to 23. When configuring an E1 data line, channel-group numbers can be a value from 0 to 29.
timeslots *range*	Timeslot or range of timeslots belonging to the channel-group. The first timeslot is numbered 1. For a T1 controller, the timeslot range is from 1 to 24. For an E1 controller, the timeslot range is from 1 to 31.
speed {**48** | **56** | **64**}	(Optional) Specifies the line speed (in kilobits per second) of the T1 or E1 link.

clear controller lex *number* [**prom**]
clear controller lex *slot*/*port* [**prom**] (for the Cisco 7000 series)

To reboot the LAN Extender and restart its operating software, use the **clear controller lex** privileged EXEC command.

number	Number of the LAN Extender interface corresponding to the LAN Extender to be rebooted.
prom	(Optional) Forces a reload of the PROM image, regardless of any Flash image.
slot	On the Cisco 7000 series, specifies the backplane slot number. On the Cisco 7000, the value can be 0, 1, 2, 3, or 4. On the Cisco 7010, the value can be 0, 1, or 2.
port	On the Cisco 7000 series, specifies the port number of the interface. The value can be 0, 1, 2, or 3 for the serial interface.

clear controller t1 *slot/port*

Use the **clear controller t1** EXEC command to reset the T1 controller interface on the Cisco 7000.

slot	Backplane slot number; can be 0, 1, 2, 3, or 4. The slots are numbered from left to right.
port	Port number of the interface. It can be 0 or1 for the MIP (MultiChannel Interface Processor). Ports on each interface processor are numbered from the top down.

clear counters [*type number*] [**ethernet** | **serial**]
clear counters [*type slot/port*] [**ethernet** | **serial**] (for the Cisco 7000 series)

To clear the interface counters, use the **clear counters** EXEC command.

type	(Optional) Specifies the interface type; it is one of the keywords listed in the "Clear Counters Interface Type Keywords" table.
number	(Optional) Specifies the interface counter displayed with the **show interfaces** command.
ethernet	(Optional) If the *type* is **lex**, you can clear the interface counters on the Ethernet interface.
serial	(Optional) If the *type* is **lex**, you can clear the interface counters on the serial interface.
slot	(Optional) On the Cisco 7000 series, specifies the backplane slot number. On the 7000, value can be 0, 1, 2, 3, or 4. On the 7010, value can be 0, 1, or 2.
port	(Optional) On the Cisco 7000 series, specifies the port number of the interface. Value can be 0, 1, 2, or 3 for the serial interface.

clear hub ethernet *number*

To reset and reinitialize the hub hardware connected to an interface of a Cisco 2505 or Cisco 2507, use the **clear hub** EXEC command.

ethernet	Indicates the hub in front of an Ethernet interface.
number	Hub number to clear, starting with 0. Since there is currently only one hub, this number is 0.

clear hub counters [**ether** *number* [*port* [*end-port*]]]

To set to zero the hub counters on an interface of a Cisco 2505 or Cisco 2507, use the **clear hub counters** EXEC command.

ether	(Optional) Indicates the hub in front of an Ethernet interface.
number	(Optional) Hub number for which to clear counters. Since there is currently only one hub, this number is 0. If the keyword **ether** is specified, the *number* is required.
port	(Optional) Port number on the hub. On the Cisco 2505, port numbers range from 1 through 8. On the Cisco 2507, port numbers range from 1 through 16. If a second port number follows, then this port number indicates the beginning of a port range. If no port number is specified, counters for all ports are cleared.
end-port	(Optional) Ending port number of a range.

clear interface *type number*
clear interface *type slot*/*port* (on a Cisco 7000 series)
clear interface *type slot*/*port* [**:***channel-group*] (on a Cisco 7000 series MIP T1 interface)

To reset the hardware logic on an interface, use the **clear interface** EXEC command.

type	Specifies the interface type; it is one of the keywords listed in the “Interface Type Keywords” table of the *Router Products Command Reference* publication.
number	Specifies the port, connector, or interface card number.
slot	In a Cisco 7000, specifies the backplane slot number and can be 0, 1, 2, 3, or 4. In a Cisco 7010, the value can be 0, 1, or 2.
port	On a Cisco 7000 series, specifies the port number of the interface and can be 0, 1, 2, 3, 4 or 5 depending on the type of interface, as follows: **AIP** (ATM Interface Processor)—0 **EIP** (Ethernet Interface Processor)—0, 1, 2, 3, 4, or 5 **FIP** (FDDI Interface Processor)—0 **HIP** (HSSI Interface Processor)—0 **TRIP** (Token Ring Interface Processor)—0, 1, 2, or 3
:*channel-group*	(Optional) On the Cisco 7000 series supporting Channelized T1, specifies the channel in the range of 0 to 23.

clear rif-cache

To clear entries from the Routing Information Field (RIF) cache, use the **clear rif-cache** EXEC command.

clock rate *bps*
no clock rate

To configure the clock rate for appliques (connector hardware) on the serial interface of the MCI and SCI cards to an acceptable bit rate, use the **clock rate** interface configuration command. Use the **no clock rate** command to remove the clock rate if you change the interface from a DCE to a DTE device.

bps	Desired clock rate in bits per second: 1200, 2400, 4800, 9600, 19200, 34800, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, or 4000000.

clock source {**line** | **internal**}

Use the **clock source** controller configuration command to set the T1-line clock-source for the MIP in the Cisco 7000 series.

line	Specifies the T1 line as the clock source.
internal	Specifies the MIP as the clock source.

clock source {**line** | **internal**}
no clock source

To control which clock a G.703-E1 interface will use to clock its transmitted data from, use the **clock source** interface configuration command. The **no** form of this command restores the default value.

line	Specifies that the interface will clock its transmitted data from a clock recovered from the line's receive data stream (default).
internal	Specifies that the interface will clock its transmitted data from its internal clock.

cmt connect [*interface-name* [**phy-a** | **phy-b**]]

To start the processes that perform the connection management (CMT) function and allow the ring on one fiber to be started, use the **cmt connect** EXEC command.

interface-name	(Optional) Specifies the FDDI interface.
phy-a	(Optional) Selects Physical Sublayer A.
phy-b	(Optional) Selects Physical Sublayer B.

cmt disconnect [*interface-name* [**phy-a | phy-b**]]

To stop the processes that perform the connection management (CMT) function and allow the ring on one fiber to be stopped, use the **cmt disconnect** EXEC command.

interface-name	(Optional) Specifies the FDDI interface.
phy-a	(Optional) Selects Physical Sublayer A.
phy-b	(Optional) Selects Physical Sublayer B.

[**no**] **compress** [**predictor** | **stac]**

To configure point-to-point software compression for LAPB, HDLC, or PPP, use the **compress** interface configuration command. To disable compression, use the **no** form of this command.

predictor	(Optional) Specifies that a predictor compression algorithm will be used on LAPB and PPP encapsulation.
stac	(Optional) Specifies that a Stacker (LZS) compression algorithm will be used on HDLC and PPP encapsulation.

controller [**t1** | **e1**] *slot*/*port* (on the Cisco 7000)

To configure a T1 or E1 controller and enter controller configuration mode, use the **controller** global configuration command. This command is used only on a Cisco 7000.

t1	T1 controller.
e1	E1 controller.
slot	Backplane slot number; can be 0, 1, 2, 3, or 4. On the 7010, the slot number can be 0, 1, or 2. The slots are numbered from left to right.
port	Port number of the interface. It can be **0** or **1** for the MIP (MultiChannel Interface Processor). Ports on each interface processor are numbered from the top down.

copy flash lex *number*

To download an executable image from Flash memory on the core router to the LAN Extender, use the **copy flash lex** privileged EXEC command.

number	Number of the LAN Extender interface to which to download an image from Flash.

copy tftp lex *number*

To download an executable image from a TFTP server to the LAN Extender, use the **copy tftp lex** privileged EXEC command.

number	Number of the LAN Extender interface to which to download an image.

crc *size*
no crc

To set the length of the cyclic redundancy check (CRC) on a Fast Serial Interface Processor (FSIP) of the Cisco 7000 series, use the **crc** interface configuration command. To set the CRC length to 16 bits, use the **no** form of this command.

size	CRC size (16 or 32 bits); the default is 16 bits.

[**no**] **crc4**

To enable generation of the G.703-E1 CRC4, use the **crc4** interface configuration command. To disable this feature, use the **no** form of this command.

[**no**] **dce-terminal-timing enable**

When running a line at high speeds and long distances, use the **dce-terminal-timing enable** interface configuration command to prevent phase shifting of the data with respect to the clock. If SCTE is not available from the DTE, use the **no** form of this command, which causes the DCE to use its own clock instead of SCTE from the DTE.

delay *tens-of-microseconds*
no delay

To set a delay value for an interface, use the **delay** interface configuration command. Use the **no** form of this command to restore the default delay value.

tens-of-microseconds	Integer that specifies the delay in tens of microseconds for an interface or network segment.

description *string* (controller configuration)
no description

To add a description to a T1 or E1 controller on a Cisco 7000 series router, use the **description controller** configuration command. Use the **no** form of this command to remove the description.

string	Comment or a description to help you remember what is attached to the interface.

description *string* (interface configuration)
no description

To add a description to an interface configuration, use the **description** interface configuration command. Use the **no** form of this command to remove the description.

string	Comment or a description to help you remember what is attached to this interface.

down-when-looped

To configure an interface to inform the system it is down when loopback is detected, use the **down-when-looped** interface configuration command.

[**no**] **dte-invert-txc**

On the Cisco 4000 platform, you can specify the serial Network Interface Module timing signal configuration. When the board is operating as a DTE, the **dte-invert-txc** command inverts the TXC clock signal it gets from the DCE that the DTE uses to transmit data. Use the **no** form of this command if the DCE accepts SCTE from the DTE.

[**no**] **early-token-release**

To enable early token release, a method whereby the Token Ring interfaces can release the token back onto the ring immediately after transmitting rather than waiting for the frame to return, use the **early-token-release** interface configuration command. This feature helps increase the total bandwidth of the Token Ring.

The CSC-C2CTR, CSC-R16 (or CSC-R16M),CSC-2R, and CSC-1R cards and the Token Ring Interface Processor (TRIP) on the Cisco 7000 all support early token release. Once enabled, use the **no** form of this command to disable this feature.

encapsulation *encapsulation-type*

To set the encapsulation method used by the interface, use the **encapsulation** interface configuration command.

encapsulation-type	Encapsulation type. See the Encapsulation Types table of the *Router Products Command Reference* publication for a list of supported encapsulation types.

[**no**] **encapsulation atm-dxi**

Use the **encapsulation atm-dxi** interface configuration command to enable ATM-DXI encapsulation. The **no encapsulation atm-dxi** command disables ATM-DXI encapsulation.

fddi burst-count *number*
no fddi burst-count

To allow the FCI card to preallocate buffers to handle bursty FDDI traffic (for example, NFS bursty traffic), use the **fddi burst-count** interface configuration command. Use the **no** form of this command to revert to the default value.

number	Number of preallocated buffers. Valid values are in the range from 1 to 10; the default is 3 buffers.

fddi c-min *microseconds*
no fddi c-min

To set the C-Min timer on the PCM, use the **fddi c-min** interface configuration command. Use the **no** form of this command to revert to the default value.

microseconds Sets the timer value in microseconds.

fddi cmt-signal-bits *signal-bits* [**phy-a** | **phy-b**]

To control the information transmitted during the connection management (CMT) signaling phase, use the **fddi cmt-signal-bits** interface configuration command. If neither the **phy-a** nor **phy-b** keyword is specified, the signal bits apply to both physical connections.

signal-bits A hexadecimal number preceded by 0x; for example, 0x208. The FDDI standard defines ten bits of signaling information that must be transmitted, as follows:

- **bit 0**—Escape bit. Reserved for future assignment by the FDDI standards committee.
- **bits 1 and 2**—Physical type, as defined in “FDDI Physical Type Bit Specifications” table of the *Router Products Command Reference* publication.
- **bit 3**—Physical compatibility. Set if topology rules include the connection of a physical-to-physical type at the end of the connection.
- **bits 4 and 5**—Link Confidence test duration; set as defined in the “FDDI Link Confidence Test Duration Bit Specification” table of the *Router Products Command Reference* publication.

signal-bits (continued)	• **bit 6**—Media Access Control (MAC) available for link confidence test. • **bit 7**—Link confidence test failed. The setting of bit 7 indicates that the link confidence was failed by the Cisco end of the connection. • **bit 8**—MAC for local loop. • **bit 9**—MAC on physical output.
phy-a	(Optional) Selects Physical Sublayer A.
phy-b	(Optional) Selects Physical Sublayer B.

[**no**] **fddi duplicate-address-check**

To enable the duplicate address detection capability on the FDDI, use the **fddi duplicate-address-check** interface configuration command. Use the **no** form of this command to disable this feature.

[**no**] **fddi encapsulate**

To specify encapsulating bridge mode on the CSC-C2/FCIT interface card, use the **fddi encapsulate** interface configuration command. Use the **no** form of this command to turn off encapsulation bridging and return the FCIT interface to its translational, nonencapsulating mode.

[**no**] **fddi smt-frames**

To enable the SMT frame processing capability on the FDDI, use the **fddi smt-frames** interface configuration command. Use the **no** form of this command to disable this feature, in which case the router will not generate or respond to SMT frames.

fddi tb-min *milliseconds*
no fddi tb-min

To set the TB-Min timer in the physical connection management (PCM), use the **fddi tb-min** interface configuration command. Use the **no** form of this command to revert to the default value.

milliseconds	Sets the TM-Min timer value in milliseconds. The default is 100 milliseconds.

fddi tl-min-time *microseconds*

To control the TL-Min time (the minimum time to transmit a Physical Sublayer, or PHY line state, before advancing to the next physical connection management (PCM) state, as defined by the X3T9.5 specification), use the **fddi tl-min-time** interface configuration command.

microseconds	Integer that specifies the time used during the connection management (CMT) phase to ensure that signals are maintained for at least the value of TL-Min so the remote station can acquire the signal. The default is 30 microseconds.

fddi token-rotation-time *microseconds*

To control ring scheduling during normal operation and to detect and recover from serious ring error situations, use the **fddi token-rotation-time** interface configuration command.

microseconds	Integer that specifies the token rotation time (TRT). The default is 5000 microseconds.

fddi t-out *milliseconds*
no fddi t-out

To set the timeout timer in the physical connection management (PCM), use the **fddi t-out** interface configuration command. Use the **no** form of this command to revert to the default value.

milliseconds	Sets the timeout timer. The default is 100 milliseconds.

fddi valid-transmission-time *microseconds*

To recover from a transient ring error, use the **fddi valid-transmission-time** interface configuration command.

microseconds	Integer that specifies the transmission valid timer (TVX) interval. The default is 2500 microseconds.

framing {**sf** | **esf** | **crc4** | **no-crc4**}

Use the **framing** controller configuration command to select the frame type for the T1 or E1 data line.

sf	Specifies super frame as the T1 frame type.
esf	Specifies extended super frame as the T1 frame type.
crc4	Specifies CRC4 frame as the E1 frame type.
no-crc4	Specifies no CRC4 frame as the E1 frame type.

hold-queue *length* {**in** | **out**}
no hold-queue {**in** | **out**}

To specify the hold-queue limit of an interface, use the **hold-queue** interface configuration command. Use the **no** form of this command with the appropriate keyword to restore the default values for an interface.

length	Integer that specifies the maximum number of packets in the queue. Default input hold-queue limit is 75 packets. Default output hold-queue limit is 40 packets.
in	Specifies the input queue.
out	Specifies the output queue.

[**no**] **hssi external-loop-request**

To allow the router to support a CSU/DSU that uses the LC signal to request a loopback from the router, use the **hssi external-loop-request** interface configuration command. Use the **no** form of this command to disable the feature.

[**no**] **hssi internal-clock**

To convert the HSSI interface into a 45-MHz clock master, use the **hssi internal-clock** interface configuration command. Use the **no** form of this command to disable the clock master mode.

hub ethernet *number port* [*end-port*]

To enable and configure a port on an Ethernet hub of a Cisco 2505 or Cisco 2507, use the **hub** global configuration command.

ethernet	Indicates that the hub is in front of an Ethernet interface.
number	Hub number, starting with 0. Since there is currently only one hub, this number is 0.
port	Port number on the hub. On the Cisco 2505, port numbers range from 1 through 8. On the Cisco 2507, port numbers range from 1 through 16. If a second port number follows, then the first port number indicates the beginning of a port range.
end-port	(Optional) Last port number of a range.

interface *type number*
interface *type slot*/*port* (for the Cisco 7000 series)
interface *type slot*/*port*:*channel-group*
(for channelized T1 on the Cisco 7000 series)

interface *type number*.*subinterface-number* [**multipoint** |
point-to-point]
interface *type slot*/*port*.*subinterface-number* [**multipoint** |
point-to-point] (for the Cisco 7000 series)

To configure an interface or subinterface type and enter interface configuration mode, use the **interface** global configuration command.

type	Type of interface to be configured. See the "Interface Type Keywords" table of the *Router Products Command Reference* publication.
number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.

slot	On the Cisco 7000 series, specifies the backplane slot number; can be 0, 1, 2, 3, or 4 on the Cisco 7000. On the Cisco 7010, can be 0, 1, or 2. The slots are numbered from left to right.
port	On the Cisco 7000 series, specifies the port number of the interface. It can be **0**, **1**, **2**, **3**, **4**, or **5** depending on the type of interface, as follows: **AIP** (ATM Interface Processor)—0 **EIP** (Ethernet Interface Processor)—**0**, **1**, **2**, **3**, **4**, or **5** **FIP** (FDDI Interface Processor)—**0** **FSIP** (Fast Serial Interface Processor)—**0**, **1**, **2**, or **3** **HIP** (HSSI Interface Processor)—**0** **TRIP** (Token Ring Interface Processor)—**0**, **1**, **2**, or **3** Ports on each interface processor are numbered from the top down.
channel-group	On the Cisco 7000, specifies the T1 circuit number in the range of 0 to 23 defined with the **channel-group** controller configuration command.
.*subinterface-number*	Subinterface number in the range 1 to 4294967293. The *number* that precedes the period (.) must match the *number* this subinterface belongs to.
multipoint | **point-to-point**	(Optional) Specifies a multipoint or point-to-point subinterface. The default is **multipoint**.

[**no**] **invert-transmit-clock**

Delays between the SCTE clock and data transmission indicate that the transmit clock signal might not be appropriate for the interface rate and length of cable being used. Different ends of the wire may have variances that differ slightly. To invert the clock signal to compensate for these factors, use the **invert-transmit-clock** interface configuration command. This command applies to the Cisco 7000 series.

ip address-pool dhcp-proxy-client
no ip address-pool dhcp-proxy-client

To make temporary IP addresses available for dial-in asynchronous clients using Serial Line Internet Protocol (SLIP)/PPP, use the **ip address-pool** global configuration command. Use the **no** form of the command to disable IP address pooling on all interfaces.

ip dhcp-server [*ip-address* | *name*]
no ip dhcp-server [*ip-address* | *name*]

To specify which Dynamic Host Configuration Protocol (DHCP) servers to use on your network, specify the IP address of one or more DHCP servers available on the network by using the **ip dhcp-server** global configuration command. Use the **no** form of the command to remove a DHCP server's IP address.

[**no**] **keepalive** [*seconds*]

Use the **keepalive** interface configuration command to set the keepalive timer for a specific interface. The **no** form of this command turns off keepalives entirely.

seconds	(Optional) Unsigned integer value greater than 0. The default is 10 seconds.

lex burned-in-address *ieee-address*
no lex burned-in-address

To set the burned-in MAC address for a LAN Extender interface, use the **lex burned-in-address** interface configuration command. To clear the burned-in MAC address, use the **no** form of this command.

ieee-address	48-bit IEEE MAC address written as a dotted triplet of four-digit hexadecimal numbers

lex input-address-list *access-list-number*
no lex input-address-list

To assign an access list that filters on MAC addresses, use the **lex input-address-list** interface configuration command. To remove an access list from the interface, use the **no** form of this command.

access-list-number	Number of the access list you assigned with the **access-list** global configuration command. It can be a number from 700 to 799.

lex input-type-list *access-list-number*
no lex input-type-list

To assign an access list that filters Ethernet packets by type code, use the **lex input-type-list** interface configuration command. To remove an access list from the interface, use the **no** form of this command.

access-list-number	Number of the access list you assigned with the **access-list** global configuration command. It can be a number in the range 200 to 299.

lex priority-group *group*
no lex priority-group

To activate priority output queuing on the LAN Extender, use the **lex priority-group** interface configuration command. To disable priority output queuing, use the **no** form of this command.

group Number of the priority group. It can be a number in the range 1 to 10.

lex retry-count *number*
no lex retry-count [*number*]

To define the number of times to resend commands to the LAN Extender, use the **lex retry-count** interface configuration command. To return to the default value, use the **no** form of this command.

number Number of times to retry sending commands to the LAN Extender. It can be a number in the range 0 to 100. The default is 10 times.

lex timeout *milliseconds*
no lex timeout [*milliseconds*]

To define the amount of time to wait for a response from the LAN Extender, use the **lex timeout** interface configuration command. To return to the default time, use the **no** form of this command.

milliseconds Time, in milliseconds, to wait for a response from the LAN Extender before resending the command. It can be a number in the range 500 to 60000. The default is 2000 milliseconds (2 seconds).

linecode {**ami** | **b8zs** | **hdb3**}

Use the **linecode** controller configuration command to select the line-code type for the T1 or E1 line.

ami	Specifies alternate mark inversion (AMI) as the line-code type. Valid for T1 or E1 controllers.
b8zs	Specifies B8ZS as the line-code type. Valid for T1 controller only.
hdb3	Specifies high-density bipolar 3 (hdb3) as the line-code type. Valid for E1 controller only.

[**no**] **link-test**

To re-enable the link test function on a port on an Ethernet hub of a Cisco 2505 or Cisco 2507, use the **link-test** hub configuration command. Disable this feature if a pre-10BaseT twisted-pair device not implementing link test is connected to the hub port with the **no** form of this command.

[**no**] **local-lnm**

To enable Lanoptics Hub Networking Management of a PCbus Token Ring interface, use the **local-lnm** command. Use the no form of this command to disable management.

[**no**] **loopback**

To diagnose equipment malfunctions between interface and device, use the **loopback** interface configuration command. The **no** form of this command disables the test.

[**no**] **loopback applique**

To configure an internal loop on the HSSI applique, use the **loopback applique** interface configuration command. To remove the loop, use the **no** form of this command.

[**no**] **loopback dte**

To loop packets to DTE internally within the CSU/DSU at the DTE interface, when the device supports this feature, use the **loopback dte** interface configuration command. To remove the loop, use the **no** form of this command.

[**no**] **loopback line**

To loop packets completely through the CSU/DSU to configure the CSU loop, when the device supports this feature, use the **loopback line** interface configuration command. To remove the loop, use the **no** form of this command.

[**no**] **loopback local**

To loop packets at the router physical interface on a T1 line, use the **loopback local** controller configuration command. To remove the loop, use the **no** form of this command.

[**no**] **loopback remote**

To loop packets completely through the CSU/DSU, over the DS3 link, to the remote CSU/DSU and back, use the **loopback remote** controller configuration command. To remove the loop, use the **no** form of this command.

[**no**] **media-type** [**aui** | **10baset**]

To specify the Ethernet Network Interface Module configuration on the Cisco 4000 series, use the **media-type** interface configuration command.

aui	(Optional) Selects a 15-pin physical connection.
10baset	(Optional) Selects an RJ45 10BaseT physical connection.

[**no**] **mop enabled**

To enable an interface to support the Maintenance Operation Protocol (MOP), use the **mop enabled** interface configuration command. To disable MOP on an interface, use the **no** form of this command.

[**no**] **mop sysid**

To enable an interface to send out periodic Maintenance Operation Protocol (MOP) system identification messages, use the **mop sysid** interface configuration command. To disable MOP message support on an interface, use the **no** form of this command.

mtu *bytes*
no mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** interface configuration command. Use the **no** form of this command to restore the MTU value to its original default value.

bytes	Desired size in bytes.

[**no**] **nrzi-encoding**

To enable non-return to zero inverted (NRZI) line coding format, use the **nrzi-encoding** interface configuration command. Use the **no** form of this command to disable this capability.

peer default ip address pool
no peer default ip address pool

You can selectively disable DHCP proxy-client status on an individual asynchronous interface on a router by using the **no peer default ip address pool** interface configuration command. You can turn a single interface back on by issuing the standard command after it is turned off.

ppp [**default** | *client* [**@***tacacs-server*]] [**/routing**]

To make an asynchronous connection from the auxiliary port using the Point-to-Point Protocol (PPP), enter the **ppp** EXEC command.

default (Optional) Makes PPP connection when a default address has been configured.

client (Optional) IP address or the name of the client workstation or PC.

@*tacacs-server* (Optional) IP address or IP host name of the TACACS server to which the user's TACACS authentication request is to be sent.

/routing (Optional) Indicates asynchronous routing is enabled.

ppp authentication {**chap** | **pap**} [**if-needed**] [*listname*]
no ppp authentication

To enable Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP), and to enable a TACACS+ authorization method on a serial interface, use the **ppp authentication** interface configuration command. Use the **no** form of the command to disable this authentication.

chap Enables CHAP on a serial interface.

pap Enables PAP on a serial interface.

if-needed (Optional) Used with TACACS and XTACACS. Do not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.

list-name (Optional) Used with AAA/TACACS+. Specify the name of a list of TACACS+ methods of authentication to use. If no listname is specified, the system uses the default. Lists and default are created with the **aaa authentication ppp** command.

ppp authentication chap [**if-needed**]
no ppp authentication chap

To enable Challenge Handshake Authentication Protocol (CHAP) on a serial interface, use the **ppp authentication chap** interface configuration command. Use the **no** form of this command to disable this encapsulation.

if-needed	(Optional) Indicates that the system will not perform CHAP authentication if the user has already been authenticated. This option applies only to asynchronous and virtual asynchronous interfaces.

ppp authentication pap [**if-needed**]
no ppp authentication pap

To enable Password Authentication Protocol (PAP) on a serial interface, use the **ppp authenticate pap** interface configuration command. To disable this feature, use the **no** form of this command.

if-needed	(Optional) Indicates that the system will not perform PAP authentication if the user has already been authenticated. This option applies only to asynchronous and virtual asynchronous interfaces.

ppp quality *percentage*
no ppp quality

To enable Link Quality Monitoring (LQM) on a serial interface, use the **ppp quality** interface configuration command. Use the **no** form of this command to disable LQM.

percentage	Specifies the link quality threshold. Range is 1 to 100.

pri-group [**timeslots** *range*]
no pri-group

To specify ISDN Primary Rate Interface (PRI) on a channelized T1 card on the Cisco 7000 series, use the **pri-group** controller configuration command. Use the **no pri-group** command to remove the ISDN PRI.

timeslots *range*	(Optional) Specifies a single range of values from 1 to 23.

pulse-time *seconds*
no pulse-time

To enable pulsing DTR signal intervals on the serial interfaces, use the **pulse-time** interface configuration command. Use the **no** form of this command to restore the default interval.

seconds	Integer that specifies the DTR signal interval in seconds. The default is 0 seconds.

ring-speed *speed*

To set the ring speed for the CSC-1R, CSC-2R, and IGS/TR Token Ring interfaces, use the **ring-speed** interface configuration command.

speed	Integer that specifies the ring speed, either 4 for 4-Mbps or 16 for 16-Mbps operation. The default is 16-Mbps operation.

show async status

To list the status of the asynchronous interface 1 associated with the router auxiliary port, use the **show async status** user EXEC command.

show compress

To display compression statistics, use the **show compress** EXEC command.

show controllers cbus

Use the **show controllers cbus** privileged EXEC command on the AGS+ to display all information under the ciscoBus controller card. This command also shows the capabilities of the card and reports controller-related failures.

show controllers cxbus

Use the **show controllers cxbus** privileged EXEC command to display information about the switch processor (SP) CxBus controller on the Cisco 7000 series. 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 controllers e1 [*slot*/*port*]

Use the **show controllers e1** privileged EXEC command on the Cisco 7000 to display information about the E1 links supported by the MultiChannel Interface Processor (MIP). This command displays controller status that is specific to the controller hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

slot	Specifies the backplane slot number and can be 0, 1, 2, 3, or 4.
port	Specifies the port number of the controller and can be 0 or 1.

show controllers ethernet *interface-number*

Use the **show controllers ethernet** EXEC command to display information on the Cisco 2500, Cisco 3000, or Cisco 4000.

interface-number	Interface number of the Ethernet interface.

show controllers fddi

Use the **show controllers fddi** user EXEC command to display all information under the FDDI controller card on the AGS+ or FDDI Interface Processor (FIP) on the Cisco 7000 series.

show controllers lex [*number*]
show controllers lex [*slot*/*port*] (for the Cisco 7000 series)

To show hardware and software information about the LAN Extender, use the **show controllers lex** EXEC command.

number	(Optional) Number of the LAN Extender interface about which to display information.
slot	(Optional) Specifies the backplane slot number on the Cisco 7000 series, and can be 0, 1, 2, 3, or 4.
port	(Optional) Specifies the port number of the controller and can be 0 or 1.

show controllers mci

Use the **show controllers mci** privileged EXEC command to display all information under the Multiport Communications Interface card or the SCI. This command displays information the system uses for bridging and routing that is specific to the interface hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

show controllers serial

Use the **show controllers serial** privileged EXEC command to display information specific to the interface hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

show controllers t1 [*slot*/*port*]

Use the **show controllers t1** privileged EXEC command on the Cisco 7000 to display information about the T1 links supported by the MultiChannel Interface Processor (MIP). This command displays controller status information that is specific to the controller hardware. The information displayed is generally useful for diagnostic tasks performed by technical support personnel only.

slot	(Optional) Specifies the backplane slot number and can be 0, 1, 2, 3, or 4.
port	(Optional) Specifies the port number of the controller and can be 0, 1, 2, or 3.

show controllers token

Use the **show controllers token** privileged EXEC command to display information about memory management, error counters, and the CSC-R, CSC-1R, CSC-2R, C2CTR, and CSC-R16 (or CSC-R16M) Token Ring interface cards or Token Ring Interface Processor (TRIP), in the case of the Cisco 7000 series.

show hub [**ether** *number* [*port* [*end-port*]]]

To display information about the hub on an Ethernet interface of a Cisco 2505 or Cisco 2507, use the **show hub** EXEC command.

ether	(Optional) Indicates that this is an Ethernet hub.
number	(Optional) Hub number, starting with 0. Since there is currently only one hub, this number is 0.
port	(Optional) Port number on the hub. On the Cisco 2505, port numbers range from 1 through 8. On the Cisco 2507, port numbers range from 1 through 16. If a second port number follows, then this port number indicates the beginning of a port range.
end-port	(Optional) Ending port number of a range.

show interfaces [*type number*] [*first*] [*last*] [**accounting**]
show interfaces [*type* [*slot*/*port*] [**accounting**] (for the Cisco 7000)

Use the **show interfaces** EXEC command to display statistics for all interfaces configured on the router. The resulting output varies, depending on the network for which an interface has been configured.

type number — (Optional) Specify that information for a particular interface controller be displayed. Allowed values for *type* include **async**, **bri0**, **ethernet**, **fddi**, **hssi**, **loopback**, **null**, **serial**, **tokenring**, and **tunnel**. For the Cisco 7000 series, *type* can be **atm**, **ethernet**, **fddi**, **serial**, or **tokenring**.

The argument *number* must match a port number on the selected interface controller.

first last — (Optional) The Cisco 2500 and Cisco 3000 support the ISDN Basic Rate Interface (BRI). The argument *first* can be either 1 or 2. The argument *last* can only be 2, indicating B channels 1 and 2. D-channel information is obtained by using the command without the optional arguments.

accounting — (Optional) Displays the number of packets of each protocol type that has been sent through the interface. You can show these numbers for all interfaces, or you can specify a specific *type* and *number*.

slot — Specifies the backplane slot number and can be 0, 1, 2, 3, or 4.

port Specifies the port number of the interface and can be 0, 1, 2, 3, 4, or 5 depending on the type of interface, as follows:

AIP (ATM Interface Processor)—0

EIP (Ethernet Interface Processor)—0, 1, 2, 3, 4, or 5

FIP (FDDI Interface Processor)—0

FSIP (Fast Serial Interface Processor)—0, 1, 2, or 3

HIP (HSSI Interface Processor) 0

TRIP (Token Ring Interface Processor)—0, 1, 2, or 3

show interfaces async [*number*] [**accounting**]

Use the **show interfaces async** privileged EXEC command to display information about the serial interface.

number (Optional) Must be 1.

accounting (Optional) Displays the number of packets of each protocol type that have been sent through the interface.

show interfaces atm [*slot*/*port*]

Use the **show interfaces atm** EXEC command to display information about the ATM interface.

slot/*port* (Optional) In the Cisco 7000, *slot* can be 0, 1, 2, 3, or 4. In the Cisco 7010, *slot* can be 0, 1, or 2. Port must be 0.

show interfaces bri *number* [*first*] [*last*] [**accounting**]

Use the **show interfaces bri** privileged EXEC command to display information about the BRI D and B channels.

number — Interface number. The value is 0 through 7 if the router has one BRI NIM or 0 through 15 if the router has two BRI NIMs. Specifying just the *interface-number* will display the D channel and both B channels for that BRI interface. (On the Cisco 2500 or Cisco 3000, only the D channel would be displayed.)

first last — (Optional) The argument *first* can be either 1 or 2. The argument *last* can only be 2, indicating B channels 1 and 2. D-channel information is obtained by using the command without the optional arguments.

accounting — (Optional) Displays the number of packets of each protocol type that have been sent through the interface.

show interfaces ethernet *number* [**accounting**]
show interfaces ethernet [*slot*/*port*] [**accounting**] (for the Cisco 7000 series)

Use the **show interfaces ethernet** privileged EXEC command to display information about an Ethernet interface on the router.

number — Must match a port number on the selected interface.

accounting — (Optional) Displays the number of packets of each protocol type that have been sent through the interface.

slot — (Optional) On a Cisco 7000 **series**, slot location of the interface processor.

port — (Optional) On a Cisco 7000 **series**, port number on the interface.

show interfaces fddi *number* [**accounting**]
show interfaces fddi [*slot*/*port*] [**accounting**] (for the Cisco 7000 series)

Use the **show interfaces fddi** user EXEC command to display information about the FDDI interface.

number	Must match a port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
slot	(Optional) On a Cisco 7000 series, slot location of the interface processor.
port	(Optional) On a Cisco 7000 series, port number on the interface.

show interfaces hssi *number* [**accounting**]
show interfaces hssi [*slot*/*port*] [**accounting**] (for the Cisco 7000 series)

Use the **show interfaces hssi** privileged EXEC command to display information about the HSSI interface.

number	Must match a port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
slot	(Optional) On a Cisco 7000 series, slot location of the interface processor.
port	(Optional) On a Cisco 7000 series, port number on the interface.

show interfaces lex *number* [**ethernet** | **serial**]

To display statistics about a LAN Extender interface, use the **show interface lex** EXEC command.

number — Number of the LAN Extender interface that resides on the core router about which to display statistics.

ethernet — (Optional) Displays statistics about the Ethernet interface that resides on the LAN Extender.

serial — (Optional) Displays statistcs about the serial interface that resides on the LAN Extender.

show interfaces loopback [*number*] [**accounting**]

Use the **show interfaces loopback** privileged EXEC command to display information about the dialer interface.

number — (Optional) Must match a port number on the selected interface.

accounting — (Optional) Displays the number of packets of each protocol type that have been sent through the interface.

show interfaces serial [*number*] [**accounting**]
show interfaces serial [*slot*/*port*] [**accounting**] (for the Cisco 7000 series)

Use the **show interfaces serial** privileged EXEC command to display information about a serial interface.

number — (Optional) Must match an interface port number.

accounting — (Optional) Displays the number of packets of each protocol type that have been sent through the interface.

slot — (Optional) On a Cisco 7000 series, slot location of the interface processor.

port (Optional) On a Cisco 7000 series, port number on interface.

show interfaces tokenring [*number*] [**accounting**]
show interfaces tokenring [*slot*/*port*] [**accounting**] (for the Cisco 7000 series)

Use the **show interfaces tokenring** privileged EXEC command to display information about the Token Ring interface and the state of source route bridging.

number (Optional) Must match an interface port line number.

accounting (Optional) Displays the number of packets of each protocol type that have been sent through the interface.

slot On a Cisco 7000 series, optional slot location of the interface processor. Value can be 0, 1, 2, 3, or 4 in the Cisco 7000. In the Cisco 7010, value can be 0, 1, or 2.

port On a Cisco 7000 series, optional port number on interface. Value can be 0, 1, 2, or 3.

show interfaces tunnel *number* [**accounting**]

To list tunnel interface information, use the **show interfaces tunnel** privileged EXEC command.

number Must match the interface port line number.

accounting (Optional) Displays the number of packets of each protocol type that have been sent through the interface.

show ip interface [**brief**] [*type*] [*number*]

To list a summary of an interface’s IP information and status, use the **show ip interface** privileged EXEC command.

brief (Optional) Displays a brief summary of IP status and configuration.

type (Optional) Specifies that information be displayed about that interface type only. The possible value depends on the type of interfaces the system has. For example, it could be **ethernet**, **null**, **serial**, **tokenring**, etc.

number (Optional) Interface number.

show interfaces vty *number*

Use the **show interfaces vty** EXEC command to display information about virtual asynchronous interfaces.

number Number of the virtual terminal (VTY) that has been configured for asynchronous protocol features (vty-async).

show rif

Use the **show rif** EXEC command to display the current contents of the RIF cache.

[**no**] **shutdown**

To disable an interface, use the **shutdown** interface configuration command. To restart a disabled interface, use the **no** form of this command.

slip [**default** | *client* [**@***tacacs-server*]] [**/routing**] [**/compressed**]

To make a SLIP connection on the auxiliary port, use the **slip** user EXEC command.

default	(Optional) Makes a SLIP connection when a default address has been configured.
client	(Optional) IP address or the name of the client workstation or PC.
@*tacacs-server*	(Optional) IP address or IP hostname of the TACACS server to which the user's TACACS authentication request is sent.
/routing	(Optional) Indicates routing is enabled. Asynchronous interface 1 must be configured for **async dynamic routing**.
/compressed	(Optional) Indicates IP header compression should be used on the link.

smt-queue-threshold *number*
no smt-queue-threshold

To set the maximum number of unprocessed FDDI station management (SMT) frames that will be held for processing, use the **smt-queue-threshold** global configuration command. Use the **no** form of this command to restore the queue to the default.

number	Number of buffers used to store unprocessed SMT messages that are to be queued for processing. Acceptable values are positive integers.The default threshold value is equal to the number of FDDI interfaces installed in the router.

source-address [*mac-address*]
no source-address

To configure source address control on a port on an Ethernet hub (repeater) of a Cisco 2505 or Cisco 2507, use the **source-address** hub configuration command. To remove a previously defined source address, use the **no** form of this command.

mac-address	(Optional) MAC address in the packets that the hub will allow to access the network.

[**no**] **squelch** {**normal** | **reduced**}

To extend the Ethernet twisted-pair 10BaseT capability beyond the standard 100 meters on the Cisco 4000 platform, use the **squelch** interface configuration command. To restore the default, use the **no** form of this command.

normal	Allows normal capability. The default value is normal range.
reduced	Allows extended 10BaseT capability.

timeslot *start-slot – stop-slot*
no timeslot

To enable framed mode on a G.703-E1 interface, use the **timeslot** interface configuration command. To restore the default, use the **no** form of this command or set the start-slot to 0.

start-slot	The first subframe in the major frame. Range is 1 to 31 and must be less than or equal to *stop-slot*.
stop-slot	The last subframe in the major frame. Range is 1 to 31 and must be greater than or equal to *start-slot.*

[**no**] **transmit-clock-internal**

When a DTE does not return a transmit clock, use the **transmit-clock-internal** interface command to enable the internally generated clock on a serial interface on a Cisco 7000. Use the **no** form of this command to disable the feature.

transmitter-delay {*microseconds* | *hdlc-flags*}
no transmitter-delay

To specify a minimum dead-time after transmitting a packet, use the **transmitter-delay** interface configuration command. The **no** form of this command restores the default.

microseconds	Approximate number of microseconds of minimum delay after transmitting a packet on the MCI and SCI interface cards. The default is 0 microseconds.
hdlc-flags	Minimum number of HDLC flags to be sent between each packet on the HIP, HSCI, FSIP, or HSSI. The valid range on the HSSI is 2 to 128000.

[**no**] **ts16**

To control the use of time slot 16 for data on a G.703-E1 interface, use the **ts16** interface configuration command. To restore the default, use the **no** form of this command.

[**no**] **tunnel checksum**

To enable encapsulator-to-decapsulator checksumming of packets on a tunnel interface, use the **tunnel checksum** interface configuration command. To disable checksumming, use the **no** form of this command.

tunnel destination {*hostname* | *ip-address*}
no tunnel destination

To specify a tunnel interface's destination, use the **tunnel destination** interface configuration command. To remove the destination, use the **no** form of this command.

hostname	Name of the host destination.
ip-address	IP address of the host destination expressed in decimal in four-part, dotted notation.

tunnel key *key-number*
no tunnel key

To enable an ID key for a tunnel interface, use the **tunnel key** interface configuration command. To remove the ID key, use the **no** form of this command.

key-number	Integer from 0 to 4294967295.

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre ip** | **nos**}
no tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** interface configuration command. To set to the default, use the **no** form of this command.

aurp	AppleTalk Update Routing Protocol (AURP).
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible CLNS tunnel.
gre ip	Generic route encapsulation GRE) protocol over IP.
nos	KA9Q/NOS compatible IP over IP.

[**no**] **tunnel sequence-datagrams**

To configure a tunnel interface to drop datagrams that arrive out of order, use the **tunnel sequence-datagrams** interface configuration command. To disable this function, use the **no** form of this command.

tunnel source {*ip-address* | *interface-type interface-number*}
no tunnel source

To set a tunnel interface's source address, use the **tunnel source** interface configuration command. To remove the source address, use the **no** form of this command.

ip-address	IP address to use as the source address for packets in the tunnel.
interface-type	All types.
interface-number	Specifies the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.

tx-queue-limit *number*

To control the number of transmit buffers available to a specified interface on the MCI and SCI cards, use the **tx-queue-limit** interface configuration command.

number	Maximum number of transmit buffers that the specified interface can subscribe. Defaults and specified limits are displayed with the **show controllers mci** EXEC command.

ATM Commands

This chapter describes the function and displays the syntax of each ATM command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

atm aal aal3/4

To enable a subinterface supporting ATM adaptation layer 3/4 (AAL3/4) on an ATM interface, use the **atm aal aal3/4** interface configuration command.

atm backward-max-burst-size-clp0 *cell-count*
no atm backward-max-burst-size-clp0

To change the maximum number of high-priority cells coming from the destination router to the source router at the burst level on the switched virtual circuit (SVC), use the **atm backward-max-burst-size-clp0** map-class configuration command. The **no** form of this command restores the default.

cell-count	Maximum number of high-priority cells coming from the destination router at the burst level. The default is –1.

atm backward-max-burst-size-clp1 *cell-count*
no atm backward-max-burst-size-clp1

To change the maximum number of low-priority cells coming from the destination router to the source router at the burst level on the SVC, use the **atm backward-max-burst-size-clp1** map-class configuration command. The **no** form of this command restores the default value.

cell-count	Maximum number of low-priority cells coming from the destination router at the burst level. The default is –1.

atm backward-peak-cell-rate-clp0 *rate*
no atm backward-peak-cell-rate-clp0

To change the peak rate of high-priority cells coming from the destination router to the source router on the SVC, use the **atm backward-peak-cell-rate-clp0** map-class configuration command. The **no** form of this command restores the default.

rate	Maximum rate in kilobits per second (kbps) that this SVC can receive high-priority cells from the destination router. The default is –1. Maximum value is 155,000 kbps.

atm backward-peak-cell-rate-clp1 *rate*
no atm backward-peak-cell-rate-clp1

To change the peak rate of low-priority cells coming from the destination router to the source router on the SVC, use the **atm backward-peak-cell-rate-clp1** map-class configuration command. The **no** form of this command restores the default.

rate	Maximum rate in kilobits per second (kbps) that this SVC can receive low-priority cells from the destination router. The default is –1. Maximum value is 155,000 kbps.

atm backward-sustainable-cell-rate-clp0 *rate*
no atm backward-sustainable-cell-rate-clp0

To change the sustainable rate of high-priority cells coming from the destination router to the source router on the SVC, use the **atm backward-sustainable-cell-rate-clp0** map-class configuration command. The **no** form of this command restores the default.

rate	Sustainable rate in kilobits per second (kbps) that this SVC can receive high-priority cells from the destination router. The default is –1. Maximum value is 155,000 kbps.

atm backward-sustainable-cell-rate-clp1 *rate*
no atm backward-sustainable-cell-rate-clp1

To change the sustainable rate of low-priority cells coming from the destination router to the source router on the SVC, use the **atm backward-sustainable-cell-rate-clp1** map-class configuration command. The **no** form of this command restores the default value.

rate	Sustainable rate in kilobits per second (kbps) that this SVC can receive low-priority cells from the destination router. The default is –1. Maximum value is 155,000 kbps.

[**no**] **atm clock internal**

To cause the AIP to generate the transmit clock internally, use the **atm clock internal** interface configuration command. The **no** form of this command restores the default value.

atm exception-queue *number*
no atm exception-queue

To set the exception-queue length, use the **atm exception-queue** interface configuration command. The **no** form of this command restores the default value.

number	Number of entries, in the range of 8 to 256. The default is 32 entries.

atm forward-max-burst-size-clp0 *cell-count*
no atm forward-max-burst-size-clp0

To change the maximum number of high-priority cells going from the source router to the destination router at the burst level on the SVC, use the **atm forward-max-burst-size-clp0** map-class configuration command. The **no** form of this command restores the default value.

cell-count	Maximum number of high-priority cells going from the source router at the burst level. The default is –1.

atm forward-max-burst-size-clp1 *cell-count*
no atm forward-max-burst-size-clp1

To change the maximum number of low-priority cells going from the source router to the destination router at the burst level on the SVC, use the **atm forward-max-burst-size-clp1** map-class configuration command. The **no** form of this command restores the default value.

cell-count	Maximum number of low-priority cells going from the source router at the burst level. The default is –1.

atm forward-peak-cell-rate-clp0 *rate*
no atm forward-peak-cell-rate-clp0

To change the peak rate of high-priority cells going from the source router to the destination router on the SVC, use the **atm forward-peak-cell-rate-clp0** map-class configuration command. The **no** form of this command restores the default value.

rate	Maximum rate in kilobits per second (kbps) that this SVC can send high-priority cells from the source router. The default is –1. The maximum value is 155,000 kbps.

atm forward-peak-cell-rate-clp1 *rate*
no atm forward-peak-cell-rate-clp1

To change the peak rate of low-priority cells coming from the source router to the destination router on the SVC, use the **atm forward-peak-cell-rate-clp1** map-class configuration command. The **no** form of this command restores the default value.

rate	Maximum rate in kilobits per second (kbps) that this SVC can send low-priority cells from the source router. The default is –1. The maximum value is 155,000 kbps.

atm forward-sustainable-cell-rate-clp0 *rate*
no atm forward-sustainable-cell-rate-clp0

To change the sustainable rate of high-priority cells coming from the source router to the destination router on the SVC, use the **atm forward-sustainable-cell-rate-clp0** map-class configuration command. The **no** form of this command restores the default value.

rate	Sustainable rate in kilobits per second (kbps) that this SVC can send high-priority cells from the source router. The default is –1. The maximum value is 155,000 kbps.

atm forward-sustainable-cell-rate-clp1 *rate*
no atm forward-sustainable-cell-rate-clp1

To change the sustainable rate of low-priority cells coming from the source router to the destination router on the SVC, use the **atm forward-sustainable-cell-rate-clp1** map-class configuration command. The **no** form of this command restores the default value.

rate	Sustainable rate in kilobits per second (kbps) that this SVC can send low-priority cells from the source router. The default is –1. Maximum value is 155,000 kbps.

atm maxvc *number*
no atm maxvc

To set the ceiling value of the virtual circuit descriptor (VCD) on the AIP card, use the **atm maxvc** interface configuration command. The **no** form of this command restores the default value.

number	Maximum number of supported virtual circuits. Valid values are 256, 512, 1024, 2048, or 4096. The default is 4096.

atm mid-per-vc *maximum*

To limit the number of message identifier (MID) numbers allowed on each virtual circuit, use the **atm mid-per-vc** interface configuration command.

maximum Number of MIDs allowed per virtual circuit on this interface. The values allowed are 16, 32, 64, 128, 256, 512, and 1024. The default is 16 MIDs per virtual circuit.

atm multicast *address*

To assign an SMDS E.164 multicast address to the ATM subinterface that supports AAL3/4 and SMDS encapsulation, use the **atm multicast** interface configuration command.

address Multicast E.164 address assigned to the subinterface.

atm nsap-address *nsap-address*
no atm nsap-address

To set the NSAP address for an ATM interface using SVC mode, use the **atm nsap-address** interface configuration command. The **no** form of this command removes any configured address for the interface.

nsap-address 40-digit (hexadecimal) NSAP address of this interface (the source address).

[**no**] **atm pvc** *vcd vpi vci aal-encap* [[*midlow midhigh*] [*peak average burst*]]

To create a permanent virtual circuit (PVC) on the AIP interface, use the **atm pvc** interface configuration command. The **no** form of this command removes the specified PVC.

vcd — Virtual circuit descriptor. Unique number per AIP that identifies to the AIP which VPI/VCI to use for a particular packet. Valid values range from 1 to the value set with the **atm maxvc** command. The AIP requires this feature to manage packet transmission. The *vcd* is not associated with the VPI/VCI used for the ATM network cells.

vpi — ATM network virtual path identifier (VPI) of this PVC, in the range from 0 through 255. The VPI is an 8-bit field in the header of the ATM cell. The VPI value is unique only on a single interface, not throughout the ATM network (it has local significance only).

Both *vpi* and *vci* cannot be specified as 0; if one is 0, the other cannot be 0.

vci — ATM network virtual channel identifier (VCI) of this PVC, in the range of 0 through 65535. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single interface, not throughout the ATM network (it has local significance only).

Both *vpi* and *vci* cannot be specified as 0; if one is 0, the other cannot be 0.

aal-encap ATM adaptation layer (AAL) and encapsulation type. When **aal5mux** is specified, a protocol is also required. Possible values are as follows:

- **aal34smds** (encapsulation for SMDS networks)
- **aal5nlpid** (encapsulation that allows ATM interfaces to interoperate with HSSI interfaces that are using an ADSU and running ATM-DXI)
- **aal5mux decnet** (a MUX-type virtual circuit)
- **aal5mux ip** (a MUX-type virtual circuit)
- **aal5mux novell** (a MUX-type virtual circuit)
- **aal5mux vines** (a MUX-type virtual circuit)
- **aal5mux xns** (a MUX-type virtual circuit)
- **aal5snap** (LLC/SNAP precedes the protocol datagram)
- **qsaal** (a signaling-type PVC used for setting up or tearing down SVCs)

midlow (Optional) Starting message identifier (MID) number for this PVC. The default is 0. If you set the *peak*, *average*, and *burst* values, you must also set the *midlow* and *midhigh* values.

midhigh (Optional) Ending MID number for this PVC. The default is 0. If you set the *peak*, *average*, and *burst* values, you must also set the *midlow* and *midhigh* values.

peak (Optional) Maximum rate (in kbps) at which this virtual circuit can transmit. Valid values are in the range from 1 to the maximum rate set for a rate queue. If you set this value, you must also specify a value for the *average*, *burst*, *midlow* and *midhigh* arguments.

average (Optional) Average rate (in kbps) at which this virtual circuit will transmit. Valid values are in the range from 1 to the maximum rate set for a rate queue. If you set this value, you must also specify a value for the *peak*, *burst*, *midlow* and *midhigh* arguments.

burst (Optional) Value (in the range 1 through 2047) that relates to the maximum number of ATM cells the virtual circuit can transmit to the network at the *peak* rate of the PVC. The actual burst cells equals *burst* * 32 cells, thereby allowing for a burst size of 32 cells to 65504 cells. The largest practical value of *burst* is the MTU size of the AIP card. If you set this value, you must also specify a value for the *average*, *peak*, *midlow* and *midhigh* arguments.

atm rate-queue *queue-number speed*
no atm rate-queue

To create a permanent rate queue for the AIP, use the **atm rate-queue** interface configuration command. The **no** form of this command removes the rate queue.

queue-number Queue number in the range 0 through 7.

speed Speed in Mbps in the range from 1 through 155. The maximum speed is determined by the detected PLIM type on the AIP:

- 34 Mbps for E3
- 45 Mbps for DS3 (when available)
- 100 Mbps for TAXI
- 155 Mbps for SONET

atm rawq-size *number*
no atm rawq-size

To define the AIP raw queue size, use the **atm rawq-size** interface configuration command. The **no** form of this command restores the default value.

number	Maximum number of cells in the raw queue simultaneously, in the range 8 through 256. The default is 32.

atm rxbuff *number*
no atm rxbuff

To set the maximum number of Receive buffers for simultaneous packet reassembly, use the **atm rxbuff** interface configuration command. The **no** form of this command restores the default value.

number	Maximum number of packet reassemblies that the AIP can perform simultaneously, in the range 0 through 512. The default is 256.

atm smds-address *address*

To assign a unicast E.164 address to the ATM subinterface that supports AAL3/4 and SMDS encapsulation, use the **atm smds-address** interface configuration command.

address	Unicast E.164 address assigned to the subinterface.

[**no**] **atm sonet stm-1**

To set the proper mode of operation for the SONET PLIM, use the **atm sonet stm-1** interface configuration command. The **no** form of this command restores the default (STS-3C).

atm txbuff *number*
no atm txbuff

To set the maximum number of Transmit buffers for simultaneous packet fragmentation, use the **atm txbuff** interface configuration command. The **no** form of this command restores the default value.

number	Maximum number of packet fragmentations that the AIP can perform simultaneously, in the range 0 through 512. The default is 256.

atm vc-per-vp *number*
no atm vc-per-vp

To set the maximum number of VCIs to support per VPI, use the **atm vc-per-vp** interface configuration command. The **no** form of this command restores the default value.

number	Maximum number of VCIs to support per VPI. Valid values are 32, 64, 128, 256, 512, 1024, 2048, or 4096. The default is 1024.

atm vp-filter *hexvalue*
no atm vp-filter

To set the AIP filter register, use the **atm vp-filter** interface configuration command. The **no** form of this command restores the default value.

hexvalue	Value in hexadecimal format. The default is 0x7B.

[**no**] *protocol protocol-address* **atm-nsap** *atm-nsap-address*
[**class** *class-name*] [**broadcast**]

To define an ATM map statement for an SVC, use the **atm-nsap** map-list configuration command in conjunction with the **map-list** global configuration command. The **no** form of this command removes the address.

protocol	One of the following keywords: **appletalk**, **apollo**, **bridge**, **clns**, **decnet**, **ip**, **ipx**, **vines**, **xns**.
protocol-address	Destination address that is being mapped to this SVC.
atm-nsap-address	Destination ATM NSAP address. Must be exactly 40 hexadecimal digits long and in the correct dotted format.
class	(Optional) Keyword.
class-name	(Optional) Name of a table that contains encapsulation-specific parameters. Such a table can be shared between maps that have the same encapsulation.
broadcast	(Optional) Indicates this map entry is to be used when the corresponding *protocol* sends broadcast packets to the interface (for example, IGRP updates).

[**no**] *protocol protocol-address* **atm-vc** *vcd* [**broadcast**]

To define an ATM map statement for a PVC, use the **atm-vc** map-list configuration command in conjunction with the **map-list** global configuration command. The **no** form of this command removes the address.

protocol	One of the following keywords: **appletalk**, **apollo**, **bridge**, **clns**, **decnet**, **ip**, **ipx, vines**, **xns**.
protocol-address	Destination address that is being mapped to this PVC.
vcd	Virtual circuit descriptor of the PVC.
broadcast	(Optional) Keyword that indicates this map entry is to be used when the corresponding *protocol* wants to send broadcast packets (such as IGRP updates) to the interface. Provides pseudo-broadcasting support.

atmsig close atm *slot*/**0** *vcd*

To disconnect an SVC, use the **atmsig close atm** EXEC command.

slot	Slot of the SVC to close.
vcd	Virtual circuit descriptor of the signaling PVC to close.

dxi map *protocol protocol-address vpi vci* [**broadcast**]
no dxi map *protocol protocol-address*

To map a protocol address to a given VPI and VCI, use the **dxi map** interface configuration command. Use the **no** form of this command to remove the mapping for that protocol and protocol address.

protocol	The bridging or protocol keyword: **apollo**, **appletalk**, **bridge**, **clns**, **decnet**, **ip**, **novell**, **vines**, or **xns**.
protocol-address	Protocol-specific address.

vpi Virtual path identifier in the range 0 to 15.

vci Virtual circuit identifier in the range 0 to 63.

broadcast (Optional) Broadcasts should be forwarded to this address.

[**no**] **dxi pvc** *vpi vci* [**snap** | **nlpid** | **mux**]

Use the **dxi pvc** interface configuration command to configure multiprotocol or single protocol ATM-DXI encapsulation. The **no** form of this command disables multiprotocol ATM-DXI encapsulation.

vpi ATM network virtual path identifier (VPI) of this PVC, in the range from 0 through 255. The VPI is an 8-bit field in the header of the ATM cell. The VPI value is unique only on a single interface, not throughout the ATM network (it has local significance only).

Both *vpi* and *vci* cannot be specified as 0; if one is 0, the other cannot be 0.

vci ATM network virtual channel identifier (VCI) of this PVC, in the range of 0 through 65535. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single interface, not throughout the ATM network (it has local significance only).

Both *vpi* and *vci* cannot be specified as 0; if one is 0, the other cannot be 0.

snap (Optional) LLC/SNAP encapsulation based on the protocol used in the packet. This keyword defines a PVC that can carry multiple network protocols. This is the default.

nlpid (Optional) RFC 1294/1490 encapsulation. This option is provided for backward compatibility with the default encapsulation in earlier versions of the Cisco IOS.

vpi ATM network virtual path identifier (VPI) of this PVC, in the range from 0 through 255. The VPI is an 8-bit field in the header of the ATM cell. The VPI value is unique only on a single interface, not throughout the ATM network (it has local significance only).

Both *vpi* and *vci* cannot be specified as 0; if one is 0, the other cannot be 0.

vci ATM network virtual channel identifier (VCI) of this PVC, in the range of 0 through 65535. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single interface, not throughout the ATM network (it has local significance only).

Both *vpi* and *vci* cannot be specified as 0; if one is 0, the other cannot be 0.

snap (Optional) LLC/SNAP encapsulation based on the protocol used in the packet. This keyword defines a PVC that can carry multiple network protocols. This is the default.

mux (Optional) MUX encapsulation; the carried protocol is defined by the **dxi map** command when the PVC is set up. This keyword defines a PVC that carries only one network protocol.

[**no**] **loopback plim**

To place the AIP into loopback mode, use the **loopback plim** interface configuration command. The **no** form of this command removes the loopback.

[**no**] **map-class** *encapsulation class-name*

To define quality of service (QOS) parameters that are associated with a static map for an SVC, use the **map-class** global configuration command. The **no** form of this command deletes this class.

encapsulation	Encapsulation type. One of the following: **atm**, **dialer**, **frame-relay**, **smds**, or **x25**.
class-name	User-assigned name of the QOS parameters table.

[**no**] **map-group** *name*

To associate an ATM map list to an interface or subinterface for either a PVC or SVC, use the **map-group** interface configuration command. The **no** form of this command removes the reference to the map list.

name	Name of the map list identified by a **map-list** command.

[**no**] **map-list** *name*

To define an ATM map statement for either a PVC or SVC, use the **map-list** global configuration command. The **no** form of this command deletes this list and all associated map statements.

name	Name of the map list.

show atm interface atm *slot*/**0**

To display ATM-specific information about an interface, use the **show atm interface atm** privileged EXEC command.

slot	Slot number of the AIP.

show atm map

To display the list of all configured ATM static maps to remote hosts on an ATM network, use the **show atm map** EXEC command.

show atm traffic

To display current, global ATM traffic information to and from all ATM networks connected to the router, use the **show atm traffic** EXEC command.

show atm vc [*vcd*]

To display all active ATM virtual circuits (PVCs and SVCs) and traffic information, use the **show atm vc** privileged EXEC command.

vcd	(Optional) Number of the virtual circuit to display information about.

show dxi map

To display all the protocol addresses mapped to a serial interface, use the **show dxi map** EXEC command.

show dxi pvc

To display the PVC statistics for a serial interface, use the **show dxi pvc** EXEC command.

show sscop

To show SSCOP details for all ATM interfaces, use the **show sscop** EXEC command.

sscop cc-timer *seconds*
no sscop cc-timer

To change the connection control timer, use the **sscop cc-timer** interface configuration command. The **no** form of this command restores the default value.

seconds	Number of seconds between BGN messages. The default is 10 seconds.

[**no**] **sscop keepalive-timer** *seconds*

To change the keepalive timer, use the **sscop keepalive-timer** interface configuration command. The **no** form of this command restores the default value.

seconds Number of seconds the router waits between transmission of POLL PDUs when no SD or SDP PDUs are queued for transmission or are outstanding pending acknowledgments. The default is 30 seconds.

sscop max-cc *retries*
no sscop max-cc

To change the retry count of connection control, use the **sscop max-cc** interface configuration command. The **no** form of this command restores the default value.

retries Number of times that SSCOP will retry to transmit BGN, END, or RS PDUs as long as an acknowledgment has not been received. Valid range is 1 to 6000. The default is 10 retries.

sscop poll-timer *seconds*
no sscop poll-timer

To change the poll timer, use the **sscop poll-timer** interface configuration command. The **no** form of this command restores the default value.

seconds Number of seconds the router waits between transmissions of POLL PDUs. The default is 10 seconds.

sscop rcv-window *packets*
no sscop rcv-window

To change the receiver window, use the **sscop rcv-window** interface configuration command. The **no** form of this command restores the default value.

packets Number of packets the interface can receive before it must send an acknowledgment to the ATM switch. Valid range is 1 to 6000. The default is 7 packets.

sscop send-window *packets*
no sscop send-window

To change the transmitter window, use the **sscop send-window** interface configuration command. The **no** form of this command restores the default value.

packets Number of packets the interface can send before it must receive an acknowledgment from the ATM switch. Valid range is 1 to 6000. The default is 7 packets.

DDR Commands

This chapter describes the function and displays the syntax of each dial-on-demand routing command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **backup delay** {*enable-delay* | **never**} {*disable-delay* | **never**}

To define how much time should elapse before a secondary line status changes after a primary line status has changed, use the **backup delay** interface configuration command. To return to the default, which means as soon as the primary fails, the secondary is brought up without delay, use the **no** form of this command.

enable-delay	Number of seconds that elapse after the primary line goes down before the router activates the secondary line. The default is 0 seconds.
disable-delay	Number of seconds that elapse after the primary line goes up before the router deactivates the secondary line. The default is 0 seconds.
never	Prevents the secondary line from being activated or deactivated.

[**no**] **backup interface** *type number*

To configure the serial interface as a secondary or dial backup line, use the **backup interface** interface configuration command. To disable this feature, use the **no** form of this command.

type	Interface type. It must be **serial**.
number	Serial port to be set as the secondary line.

[**no**] **backup load** {*enable-threshold* | **never**} {*disable-load* | **never**}

To set traffic load threshold for dial backup service, use the **backup load** interface configuration command. To return to the default value, use the **no** form of this command.

enable-threshold	Percentage of the primary line's available bandwidth.
disable-load	Percentage of the primary line's available bandwidth.
never	Sets the secondary line to never be activated due to traffic load.

[**no**] **chat-script** *script-name expect-send*

Use the **chat-script** global configuration command to create a script that will place a call over a modem. Use the **no** form of this command to disable the specified chat script.

script-name	Name of the chat script.
expect-send	Content of the chat script.

clear dialer [**interface** *type number*]
clear dialer [**interface serial** *slot*/*port*]   (Cisco 7000 series only)

To clear the values of dialer statistics for one or more serial or BRI interfaces configured for DDR, use the **clear dialer** privileged EXEC command.

interface	(Optional) Indicates that one interface will be specified.
type	Interface type, either **serial** or **bri**.
number	Interface number.
slot/*port*	On the Cisco 7000 series, specifies the slot and port numbers.

clear snapshot quiet-time *interface*

To end the quiet period on a client router within two minutes, use the **clear snapshot quiet-time** EXEC command.

interface	Interface type and number.

[**no**] **dialer caller** *number*

To configure caller ID screening, use the **dialer caller** interface configuration command. To disable this feature, use the **no** form of this command.

number	Telephone number for which to screen. Specify an x to represent a single "don't-care" character. The maximum length of each number is 25 characters.

[**no**] **dialer dtr**

To enable DDR on an interface and specify that the serial line is connected by non-V.25bis modems using EIA signaling only (the data terminal ready [DTR] signal), use the **dialer dtr** interface configuration command. To disable dial-on-demand routing for the interface, use the **no** form of this command.

dialer enable-timeout *seconds*
no dialer enable-timeout

Use the **dialer enable-timeout** interface configuration command to set the length of time an interface stays down after a call has completed or failed before it is available to dial again. Use the **no** form of this command to reset the enable timeout value to the default.

seconds	Time in seconds that the router waits before the next call can occur on the specific interface. Acceptable values are positive, nonzero integers. The default is 15 seconds.

dialer fast-idle *seconds*
no dialer fast-idle

Use the **dialer fast-idle** interface configuration command to specify the amount of time that a line for which there is contention will stay idle before the line is disconnected and the competing call is placed. Use the **no** form of this command to return to the default value.

seconds	Idle time, in seconds, that must occur on an interface before the line is disconnected. Acceptable values are positive, nonzero integers. The default is 20 seconds.

dialer hold-queue *packets*
no dialer hold-queue [*packets*]

To allow "interesting" outgoing packets to be queued until a modem connection is established, use the **dialer hold-queue** interface configuration command. To disable a dialer hold queue, use the **no** form of this command.

packets	Number of packets, in the range 0 to 100 packets, to hold in the queue. This argument is optional with the **no** form of this command.

dialer idle-timeout *seconds*
no dialer idle-timeout

Use the **dialer idle-timeout** interface configuration command to specify the idle time before the line is disconnected. Use the **no** form of this command to reset the idle timeout to the default value.

seconds	Idle time, in seconds, that must occur on an interface before the line is disconnected. Acceptable values are positive, nonzero integers. The default is 120 seconds.

dialer in-band [**no-parity** | **odd-parity**]
no dialer in-band

Use the **dialer in-band** interface configuration command to specify that DDR is to be supported. Use the **no** form of this command to disable dial-on-demand routing for the interface.

no-parity	(Optional) Indicates that no parity is to be applied to the dialer string that is sent out to the modem on synchronous interfaces.
odd-parity	(Optional) Indicates that the dialed number has odd parity (7-bit ASCII characters with the eighth bit the parity bit) on synchronous interfaces.

dialer load-threshold *load*
no dialer load-threshold

To configure bandwidth on demand by setting the maximum load before the dialer places another call to a destination, use the **dialer load-threshold** interface configuration command. To disable the setting, use the **no** form of this command.

load	Interface load beyond which the dialer will initiate another call to the destination. This argument is a number between 1 and 255.

[**no**]**dialer map** *protocol next-hop-address* [**name** *hostname*] [**spc**]
[**speed 56** | **64**] [**broadcast**]
[**modem-script** *modem-regexp*] [**system-script** *system-regexp*]
[*dial-string*[**:***isdn-subaddress*]]

[**no**] **dialer map** *protocol next-hop-address* [**name** *hostname*] [**spc**]
[**speed 56** | **64**] [**broadcast**] [*dial-string*[**:***isdn-subaddress*]]

[**no**] **dialer map bridge** [**name** *hostname*] [**spc**] [**broadcast**]
[*dial-string*[**:***isdn-subaddress*]]

[**no**] **dialer map** *protocol next-hop-address dial-string* [**name** *hostname*] [**modem-script** *modem-regexp*] [**system-script** *system-regexp*] [**broadcast**]

To configure a serial interface or Integrated Services Digital Network (ISDN) interface to call one or multiple sites, use a form of the **dialer map** interface configuration command; all options are shown in the first form of the command. To configure a serial interface or ISDN interface to place a call to multiple sites and to authenticate calls from multiple sites, use the second form of the **dialer map** command. To configure a serial interface or ISDN interface to support bridging, use the third form of the command. To configure an asynchronous interface to place a call to a single site that has no modem script assigned or that requires a system script, or to multiple sites on a single line, on multiple lines, or on a dialer rotary group, use the fourth form of the **dialer map** command.To delete a particular dialer map entry, use a **no** form of this command.

protocol Protocol keyword. See the "Dialer Map Command Supported Protocols" table in the *Router Products Command Reference* publication for a list of supported protocols and their keywords.

next-hop-address Protocol address used to match against addresses to which packets are destined. This argument is not used with the **bridge** protocol keyword.

name (Optional) Indicates the remote system with which the local router communicates.

hostname (Optional) Case-sensitive name or ID of the remote device (usually the host name). For routers with ISDN interfaces, if calling line identification (CLI/ANI/caller ID) is provided, the *hostname* field can contain the number that the calling line ID provides.

spc Specifies a semipermanent connection between customer equipment and the exchange; used only in Germany to configure connections between an ISDN BRI and a 1TR6 ISDN switch type.

speed 56 | 64 Keyword and value indicating the line speed to use. Used for ISDN only. The default is 64.

broadcast Indicates that broadcasts should be forwarded to this protocol address.

modem-script (Optional) Indicates the modem script to be used for the connection (for asynchronous interfaces).

modem-regexp (Optional) Regular expression to which a modem script will be matched (for asynchronous interfaces). No default scripts are defined for placing calls.

system-script (Optional) Indicates the system script to be used for the connection (for asynchronous interfaces).

system-regexp (Optional) Regular expression to which a system script will be matched (for asynchronous interfaces).

dial-string Telephone number sent to the dialing device when it recognizes packets with the specified *next-hop-address* that matches the access lists defined.
The dial string must be the last item in the command line.

:*isdn-subaddress* (Optional) Subaddress number used for ISDN multipoint connections.

dialer map snapshot *sequence-number dial-string*
no dialer map snapshot [*sequence-number*]

To define a dialer map for Cisco's snapshot routing protocol on a client router connected to a DDR interface, use the **dialer map snapshot** interface configuration command. To delete one or more previously defined snapshot routing dialer maps, use the **no** form of this command.

sequence-number	Number in the range from 1 to 254, inclusive, that uniquely identifies a dialer map.
dial-string	Telephone number of a remote snapshot server to be called during an active period.

dialer priority *number*
no dialer priority

To set the priority of an interface in a dialer rotary group use the **dialer priority** interface configuration command. Use the **no** form of this command to revert to the default setting.

number	Specifies the priority of an interface in a dialer rotary group; the highest number indicates the highest priority. A number from 0 to 255. The default value is 0.

dialer rotary-group *number*

Use the **dialer rotary-group** interface configuration command to include an interface in a dialer rotary group.

number	Number of the dialer interface in whose rotary group you want this interface included. An integer that you select that indicates the dialer rotary group; defined by the **interface dialer** command. A number from 0 to 255.

dialer string *dial-string*
no dialer string

Use the **dialer string** interface configuration command to specify the string (telephone number) to be called for interfaces calling a single site. Use the **no** form of this command to delete the dialer string specified for the interface.

dial-string	String of characters to be sent to a DCE.

dialer wait-for-carrier-time *seconds*
no dialer wait-for-carrier-time

Use the **dialer wait-for-carrier-time** interface configuration command to specify how long to wait for a carrier. Use the **no** form of this command to reset the carrier wait time value to the default.

seconds	Number of seconds that the interface waits for the carrier to come up when a call is placed. Acceptable values are positive, nonzero integers. The default is 30 seconds.

dialer-group *group-number*
no dialer-group

To control access, use the **dialer-group** interface configuration command. To remove an interface from the specified dialer access group, use the **no** form of this command.

group-number	Number of the dialer access group to which the specific interface belongs. This access group is defined using the **dialer-list** command. Acceptable values are nonzero, positive integers between 1 and 10.

[**no**] **dialer-list** *dialer-group* **list** *access-list-number*

To group access lists, use the **dialer-list list** global configuration command. To disable automatic dialing, use the **no** form of this command.

dialer-group — Specifies the number of a dialer access group identified in any **dialer-group** interface configuration command.

access-list-number — Specifies the access list number specified in any IP or Novell IPX access lists including Novell IPX extended, Service Access Point (SAP) access lists and bridging type. See the “Dialer-List List Command Access List Types and Numbers” table in the *Router Products Command Reference* publication for the supported access list types and numbers.

dialer-list *dialer-group* **protocol** *protocol-name* {**permit** | **deny** |
list *access-list-number* | *access-group*}
no dialer-list *dialer-group* [**protocol** *protocol-name* [**list**
access-list-number | *access-group*]]

To define a DDR dialer list to control dialing by protocol or by a combination of protocol and access list, use the **dialer-list protocol** global configuration command. To delete a dialer list, use the **no** form of this command.

dialer-group — Number of a dialer access group identified in any **dialer-group** interface configuration command.

protocol-name — One of the following protocol keywords: **appletalk**, **bridge**, **clns**, **clns_es**, **clns_is**, **decnet**, **decnet_router-L1**, **decnet_router-L2**, **decnet_node**, **ip**, **ipx**, **vines**, or **xns**.

permit — (Optional) Permits access to an entire protocol.

deny	(Optional) Denies access to an entire protocol.
list	Specifies that an access list will be used for defining a granularity finer than an entire protocol.
access-list-number	Access list number. Access list numbers include any DECnet, Banyan VINES, IP, Novell IPX, or XNS standard or extended access lists, plus Novell IPX extended, Service Access Point (SAP) access lists and bridging types. See the "Dialer-List Supported Access List Types and Numbers" table in the *Router Products Command Reference* publication.
access-group	Filter list name used in the **clns filter-set** and **clns access-group** commands.

encapsulation ppp

Use the **encapsulation ppp** interface configuration command to configure Point-to-Point Protocol (PPP) encapsulation.

interface dialer *number*

Use the **interface dialer** global configuration command to define a dialer rotary group.

number	Number of the dialer rotary group. It can be number in the range 0 through 255.

ppp authentication chap [if-needed]
no ppp authentication chap

To enable Challenge Handshake Authentication Protocol (CHAP) on a serial interface, use the **ppp authentication chap** interface configuration command. Use the **no** form of this command to disable this feature.

if-needed	(Optional) CHAP authentication is not done on this line if the user has already authenticated.

ppp authentication pap [if-needed]
no ppp authentication pap

To enable Password Authentication Protocol (PAP) on a serial interface, use the **ppp authentication pap** interface configuration command. To disable this encapsulation, use the **no** form of this command.

if-needed	(Optional) PAP authentication is not done on this line if the user has already authenticated.

script dialer *regexp*
no script dialer

To specify a default modem chat script, use the **script dialer** line configuration command. Use the **no** form of this command to disable this feature.

regexp	Specifies the set of modem scripts that might be executed. The first script that matches the argument *regexp* will be used.

show dialer [**interface** *type number*]

To obtain a general diagnostic display for serial interfaces configured for DDR, use th**e show dialer** EXEC command.

interface (Optional) Information for only the interface specified by the arguments *type* and *number* is to be displayed.

type (Optional) Interface type.

number (Optional) Interface unit number.

show snapshot [*interface*]

To display snapshot routing parameters associated with an interface, use the **show snapshot** EXEC command.

interface (Optional) Interface type and number.

[**no**] **snapshot client** *active-time quiet-time*
[**suppress-statechange-updates**] [**dialer**]

To configure a client router for snapshot routing, use the **snapshot client** interface configuration command. To disable a client router, use the **no** form of this command.

active-time Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer in the range 5 to 100. There is no default value. A typical value would be 5 minutes.

quiet-time	Amount of time, in minutes, that routing entries are frozen and remain unchanged between active periods. Routes are not aged during the quiet period, so they remain in the routing table as if they were static entries. This argument can be an integer from 8 to 100000. There is no default value. The minimum quiet time is generally the active time plus 3.
suppress-statechange-updates	(Optional) Disables the exchange of routing updates each time the line protocol goes from "down" to "up" or from "dialer spoofing" to "fully up."
dialer	(Optional) Allows the client router to dial up the remote router in the absence of regular traffic.

[**no**] **snapshot server** *active-time* [**dialer**]

To configure a server router for snapshot routing, use the **snapshot server** interface configuration command. To disable a server router, use the **no** form of this command.

active-time	Amount of time, in minutes, that routing updates are regularly exchanged between the client and server routers. This can be an integer in the range 5 to 100. There is no default value. A typical value would be 5 minutes.
dialer	(Optional) Allows the client router to dial up the remote router in the absence of regular traffic.

username *name* **password** *secret*

Use the **username password** command to specify the password to be used in Challenge Handshake Authentication Protocol (CHAP) caller identification and Password Authentication Protocol (PAP).

name	Host name, server name, user ID, or command name.
secret	For CHAP authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. This prevents the secret from being stolen. The secret can consist of any string of up to 11 printable ASCII characters. There is no limit to the number of username/password combinations that can be specified, allowing any number of remote devices to be authenticated.

Frame Relay Commands

This chapter describes the function and displays the syntax of each Frame Relay command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

clear frame-relay-inarp

To clear dynamically created Frame Relay maps, which are created by the use of Inverse ARP, use the **clear frame-relay-inarp** EXEC command.

[**no**] **encapsulation frame-relay** [**cisco** | **ietf**]

Use the **encapsulation frame-relay** interface configuration command to enable Frame Relay encapsulation. The **no** form of this command disables Frame Relay. If the **ietf** keyword is not specified, this command defaults to using Cisco's encapsulation, which is a four-byte header, with two bytes for the DLCI and two bytes to identify the packet type.

ietf (Optional) Sets the encapsulation method to comply with the IETF standard (RFC 1294). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.

ietf (Optional) Sets the encapsulation method to comply with the IETF standard (RFCs 1294 and 1490). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.

frame-relay broadcast-queue *size byte-rate packet-rate*

To create a special queue for a specified interface to hold broadcast traffic that has been replicated for transmission on multiple DLCIs, use the **frame-relay broadcast-queue** interface configuration command.

size Number of packets to hold in the broadcast queue. The default is 64 packets.

byte-rate Maximum number of bytes to be transmitted per second. The default is 256000 bytes per second.

packet-rate Maximum number of packets to be transmitted per second. The default is 36 packets per second.

frame-relay de-group *group-number dlci*
no frame-relay de-group [*group-number*] [*dlci*]

To specify the discard eligibility (DE) group number to be used for a specified DLCI, use the **frame-relay de-group** interface configuration command. To disable a previously defined group number assigned to a specified DLCI, use the **no** form of this command with the relevant keyword and arguments.

group-number DE group number to apply to the specified DLCI number, in the range from 1 through 10.

dlci DLCI number.

[**no**] **frame-relay de-list** *list-number* {**protocol** *protocol* |
interface *type number*} *characteristic*

To define a discard eligibility (DE) list specifying which packets will have the DE bit set and thus will be eligible for discarding when congestion is experienced on the Frame Relay switch, use the **frame-relay de-list** global configuration command. To delete a portion of a previously defined DE list, use the **no** form of this command.

list-number Number of the DE list.

protocol	One of the following keywords corresponding to a supported protocol or device: **arp**—Address Resolution Protocol. **apollo**—Apollo Domain. **appletalk**—AppleTalk. **bridge**—bridging device. **clns**—ISO Connectionless Network Service. **clns_es**—CLNS end systems. **clns_is**—CLNS intermediate systems. **compressedtcp**—Compressed TCP. **decnet**—DECnet. **decnet_node**—DECnet end node. **decnet_router-L1**—DECnet Level 1 (intra-area) router. **decnet_router-L2**—DECnet Level 2 (interarea) router. **ip**—Internet Protocol. **ipx**—Novell Internet Packet Exchange. **vines**—Banyan VINES. **xns**—Xerox Network Systems.
type	One of the following interface types: **serial**, **null**, or **ethernet**.
number	Interface number.
characteristic	You must supply one of the following:
	fragments—Classify fragmented IP packets. **tcp** *port*—TCP packets to or from a specified port. **udp** *port*—UDP packets to or from a specified port. **list** *access-list-number*—Previously defined access list number. **gt** *bytes*—Packets larger than the specified number of bytes will have the DE bit set. **lt** *bytes*—Packets smaller than the specified number of bytes will have the DE bit set.

[**no**] **frame-relay interface-dlci** *dlci* [*option*]

frame-relay interface-dlci *dlci* [**protocol ip** *ip-address*]

To assign a DLCI to a specified Frame Relay subinterface on the router, use the **frame-relay interface-dlci** interface configuration command. To remove this feature, use the **no** form of this command.

dlci	DLCI number to be used on the specified subinterface.
option	(Optional) Broadcast or encapsulation keyword, as defined in the "Frame Relay Interface-DLCI Option Keywords" table in the *Router Products Command Reference* publication.
protocol ip *ip-address*	Indicates the IP address of the serial interface of a new router onto which a router configuration file is to be autoinstalled over a Frame Relay network. Use this option only when this router will act as the BOOTP server for autoinstallation over Frame Relay.

frame-relay intf-type [**dce** | **dte** | **nni**]
no frame-relay intf-type [**dce** | **dte**]

Use the **frame-relay intf-type** interface configuration command to configure a Frame Relay switch type. Use the **no** form of this command to disable the switch.

dce	(Optional) Router functions as a switch connected to a router.
dte	(Optional) Router is connected to a Frame Relay network. This is the default.
nni	(Optional) Router functions as a switch connected to a switch (supports NNI connections).

[**no**] **frame-relay inverse-arp** *protocol dlci*

Use the **frame-relay inverse-arp** interface configuration command to enable the Inverse Address Resolution Protocol (Inverse ARP) on the router configured for Frame Relay. Use the **no** form of this command to disable this feature.

protocol	Supported protocols: **appletalk**, **decnet, ip**, **ipx**, **vines**, and **xns**.
dlci	A DLCI number used on the interface. Acceptable numbers are integers in the range 16 to 1007.

frame-relay ip tcp header-compression [**passive**]
no frame-relay ip tcp header-compression

To configure an interface to ensure that the associated PVC will always carry outgoing TCP/IP headers in compressed form, use the **frame-relay ip tcp header-compression** interface configuration command. To disable compression of TCP/IP packet headers on the interface, use the **no** form of this command.

passive	(Optional) Compresses the outgoing TCP/IP packet header only if an incoming packet had a compressed header.

frame-relay keepalive *number*
no frame-relay keepalive

To enable the Local Management Interface (LMI) mechanism for serial lines using Frame Relay encapsulation, use the **frame-relay keepalive** interface configuration command. To disable this capability, use the **no** form of this command.

number	An integer that defines the keepalive interval. The interval must be set and must be less than the interval set on the switch; see the **frame-relay lmi-t392dce** command description. The default is 10 seconds.

[**no**] **frame-relay lmi-n391dte** *keep-exchanges*

To set a full status polling interval, use the **frame-relay lmi-n391dte** interface configuration command. To restore the default interval value, assuming an LMI has been configured, use the **no** form of this command.

keep-exchanges	Number of keep exchanges to be done before requesting a full status message. Acceptable value is a positive integer in the range 1 through 255. The default is 6.

[**no**] **frame-relay lmi-n392dce** *threshold*

To set the DCE and NNI error threshold, use the **frame-relay lmi-n392dce** interface configuration command. To remove the current setting, use the **no** form of this command.

threshold	Error threshold value. Acceptable value is a positive integer in the range 1 through 10. The default is 2.

[**no**] **frame-relay lmi-n392dte** *threshold*

To set the error threshold on a DTE or NNI interface, use the **frame-relay lmi-n392dte** interface configuration command. To remove the current setting, use the **no** form of this command.

threshold	Error threshold value. Acceptable value is a positive integer in the range 1 through 10. The default is 2.

[**no**] **frame-relay lmi-n393dce** *events*

To set the DCE and NNI monitored events coun, use the **frame-relay lmi-n393dce** interface configuration commandt. To remove the current setting, use the **no** form of this command.

events	Monitored events count value. Acceptable value is a positive integer in the range 1 through 10. The default is 2.

[**no**] **frame-relay lmi-n393dte** *events*

To set the monitored event count on a DTE or NNI interface, use the **frame-relay lmi-n393dte** interface configuration command. To remove the current setting, use the **no** form of this command.

events	Monitored event count value. Acceptable value is a positive integer in the range 1 through 10. The default is 2.

[**no**] **frame-relay lmi-t392dce** *timer*

To set the polling verification timer on a DCE or NNI interface, use the **frame-relay lmi-t392dce** interface configuration command. To remove the current setting, use the **no** form of this command.

timer	Polling verification timer value. Acceptable value is a positive integer in the range 5 through 30. The default is 15 seconds.

[**no**] **frame-relay lmi-type** { **ansi** | **cisco** | **q933a**}

To select the Local Management Interface (LMI) type, use the **frame-relay lmi-type** interface configuration command. Use the **no** form of this command to remove a previously selected LMI type.

ansi	Annex D defined by ANSI standard T1.617.
cisco	LMI type defined jointly by Cisco and three other companies. This is the default.
q933a	ITU-T Q.933 Annex A.

frame-relay local-dlci *number*
no frame-relay local-dlci

To set the source DLCI for use when the LMI is not supported, use the **frame-relay local-dlci** interface configuration command . To remove the DLCI number, use the **no** form of this command.

number	Local (source) data link connection identifier (DLCI) number for the interface.

frame-relay map *protocol protocol-address dlci* [**broadcast**]
[**ietf** | **cisco**]
no frame-relay map *protocol protocol-address*

Use the **frame-relay map** interface configuration command to define the mapping between an address and the DLCI used to connect to the address. Use the **no frame-relay map** command to delete the map entry.

protocol	Supported protocol, bridging, or logical link control keywords: **appletalk**, **decnet**, **ip**, **ipx**, **llc2**, **rsrb**, **vines** and **xns**.
protocol-address	Destination protocol address.
dlci	DLCI number used to connect to the specified protocol address on the interface.
broadcast	(Optional) Broadcasts should be forwarded to this address when multicast is not enabled (see the **frame-relay multicast-dlci** command for more information about multicasts). This keyword also simplifies the configuration of OSPF (see the "Usage Guidelines" section for this command in the *Router Products CommandReference* publication).
ietf	(Optional) IETF form of Frame Relay encapsulation. Use when the router is connected to another vendor's equipment across a Frame Relay network.
cisco	(Optional) Cisco encapsulation method.

frame-relay map bridge *dlci* [**broadcast**]
no frame-relay map bridge *dlci*

Use the **frame-relay map bridge** interface configuration command to specify that broadcasts should be forwarded when bridging. Use the **no** form of this command to delete the map entry.

dlci	DLCI number to be used for bridging on the specified interface or subinterface.
broadcast	(Optional) Broadcasts should be forwarded to this address when multicast is not enabled.

frame-relay map clns *dlci* [**broadcast**]
no frame-relay map clns *dlci*

Use the **frame-relay map clns** interface configuration command to specify that broadcasts should be forwarded when routing using ISO CLNS. Use the **no** form of this command to delete the map entry.

dlci	DLCI number to which CLNS broadcasts should be forwarded on the specified interface.
broadcast	(Optional) Broadcasts should be forwarded when multicast is not enabled.

frame-relay map ip *ip-address dlci* [**broadcast**] [**cisco** | **ietf**]
[**nocompress**] **tcp header-compression** {**active** | **passive**}
no frame-relay map ip *ip-address dlci*

To assign header compression characteristics to an IP map that differ from the compression characteristics of the interface with which the IP map is associated, use the **frame-relay map ip tcp header-compression** interface configuration command. To remove the IP map, use the **no** form of this command. To disable TCP/IP header compression on the IP map, use the **nocompress** form of this command.

ip-address	IP address.
dlci	DLCI number.

broadcast (Optional) Forwards broadcasts to the specified IP address.

cisco (Optional) Uses Cisco's proprietary encapsulation. This is the default.

ietf (Optional) Uses RFC 1294 encapsulation. No TCP/IP header compression is done if IETF encapsulation is chosen for the IP map or the associated interface.

nocompress (Optional) Disables TCP/IP header compression for this map.

active Compresses the header of every outgoing TCP/IP packet.

passive Compresses the header of an outgoing TCP/IP packet only if an incoming TCP/IP packet had a compressed header.

frame-relay multicast-dlci *number*
no frame-relay multicast-dlci

Use the **frame-relay multicast-dlci** interface configuration command to define the DLCI to be used for multicasts. Use the **no** form of this command to remove the multicast group.

Note The **frame-relay multicast-dlci** command is provided mainly to allow testing of the Frame Relay encapsulation in a setting where two servers are connected back to back. This command is not required in a live Frame Relay network.

number Multicast DLCI. (Note that this is *not* the multicast group number, which is an entirely different value.)

[**no**] **frame-relay route** *in-dlci out-interface out-dlci*

Use the **frame-relay route** interface configuration command to specify the static route for PVC switching. Use the **no** form of this command to remove a static route.

in-dlci	DLCI on which the packet is received on the interface.
out-interface	Interface the router uses to transmit the packet.
out-dlci	DLCI the router uses to transmit the packet over the specified *out-interface*.

[**no**] **frame-relay short-status**

To instruct the network server to request the short status message from the switch (see Version 2.3 of the joint *Frame Relay Interface* specification), use the **frame-relay short-status** interface configuration command. Use the **no** form of this command to override the default

[**no**] **frame-relay switching**

Use the **frame-relay switching** global configuration command to enable PVC switching on a Frame Relay DCE or an NNI. Use the **no** form of this command to disable switching.

show frame-relay ip tcp header-compression

To display statistics and TCP/IP header compression information for the interface, use the **show frame-relay ip tcp header-compression** EXEC command.

show frame-relay lmi [*type number*]

Use the **show frame-relay lmi** EXEC command to display statistics about the Local Management Interface (LMI).

type	(Optional) Interface type; serial only.
number	(Optional) Interface number.

show frame-relay map

To display the current map entries and information about the connections, use the **show frame-relay map** EXEC command.

show frame-relay pvc [*type number* [*dlci*]]

To display statistics about PVCs for Frame Relay interfaces, use the **show frame-relay pvc** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.
dlci	(Optional) One of the specific DLCI numbers used on the interface. Statistics for the specified PVC display when a DLCI is also specified.

show frame-relay route

Use the **show frame-relay route** EXEC command to display all configured Frame Relay routes, along with their status.

show frame-relay traffic

Use the **show frame-relay traffic** EXEC command to display the router’s global Frame Relay statistics since the last reload.

show interfaces serial *number*

Use the **show interfaces serial** EXEC command to display information about a serial interface. When using the Frame Relay encapsulation, use the **show interfaces serial** command to display information about the multicast DLCI, the DLCI of the interface, and the LMI DLCI used for the Local Management Interface. The status information is taken from the LMI, when active.

number	Interface number.

ISDN Commands

This chapter describes the function and displays the syntax of each ISDN command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

interface bri *number*

interface bri *number***.***subinterface-number* [**multipoint |**
point-to-point]

To configure a BRI interface and enter interface configuration mode, use the **interface bri** global configuration command.

To configure a BRI subinterface, use the **interface bri** [**multipoint | point-to-point**] global configuration command.

number	Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the **show interfaces** command.
.*subinterface-number*	Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number this subinterface belongs to.
multipoint | **point-to-point**	(Optional) Specifies a multipoint or point-to-point subinterface. The default is **multipoint**.

[**no**] **isdn answer1** [*called-party-number*][**:***subaddress*]

[**no**] **isdn answer2** [*called-party-number*][**:***subaddress*]

To have the router verify a called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch, use the **isdn answer1** interface configuration command. To remove the verification request, use the **no** form of this command.

To have the router verify an additional called-party number or subaddress number in the incoming setup message for ISDN BRI calls, if the number is delivered by the switch, use the **isdn answer2** interface configuration command. To remove this second verification request, use the **no** form of this command.

called-party-number	(Optional) Telephone number of the called party. At least one of the *called-party-number* or *subaddress* must be specified.
:	Identifies the number that follows as a subaddress. Use the colon (:) when you configure both the called party number and the subaddress or when you configure only the subaddress.
subaddress	(Optional) Subaddress number, 20 or fewer characters long, used for ISDN multipoint connections. At least one of the *called-party-number* or *subaddress* must be specified. Use the colon (:) when you configure the subaddress only.

[**no**] **isdn caller** *number*

To configure ISDN caller ID screening, use the **isdn caller** interface configuration command. To disable this feature, use the **no** form of this command.

number Telephone number for which to screen. Specify an x to represent a single "don't-care" character. The maximum length of each number is 25 characters.

isdn calling-number *calling-number*
no isdn calling number

To configure an Australian basic-ts013 ISDN BRI interface to present a billing number of the device making the outgoing call, use the **isdn calling-number** interface configuration command. To remove a previously configured calling number, use the **no** form of this command.

calling-number Number of the device making the outgoing call; only one entry is allowed and it is limited to 16 digits.

isdn not-end-to-end *speed*

For incoming calls, to override the speed that the network reports it will use to deliver the call data, use the **isdn not-end-to-end** interface configuration command.

speed The line speed used for incoming calls that are not ISDN from end to end. Can be 56 or 64 kbps. The default line speed is 64 kbps.

[**no**] **isdn spid1** *spid-number* [*ldn*]

Use the **isdn spid1** interface configuration command to define at the router the service profile identifier (SPID) number that has been assigned by the ISDN service provider for the B1 channel. Use the **no isdn spid1** command to disable the specified SPID, thereby preventing access to the switch. If you include the LDN in the **no** form of this command, the access to the switch is permitted, but the other B-channel may not be able to receive incoming calls.

spid-number Number identifying the service to which you have subscribed. This value is assigned by the ISDN service provider and is usually a ten-digit telephone number with some extra digits.

ldn (Optional) Local directory number, as delivered by the service provider in the incoming Setup message. This is a seven-digit number assigned by the service provider.

isdn spid2 *spid-number* [*ldn*]
no isdn spid2 *spid-number* [*ldn*]

Use the **isdn spid2** interface configuration command to define at the router the SPID number that has been assigned by the ISDN service provider for the B2 channel. Use the **no isdn spid2** command to disable the specified SPID, thereby preventing access to the switch. If you include the LDN in the **no** form of this command, the access to the switch is permitted, but the other B-channel might not be able to receive incoming calls.

spid-number Number identifying the service to which you have subscribed. This value is assigned by the ISDN service provider and is usually a ten-digit telephone number with some extra digits.

ldn (Optional) Local directory number. This is a seven-digit number also assigned by the service provider.

isdn switch-type *switch-type*

To configure a central office switch on the ISDN interface, use the **isdn switch-type** global configuration command.

switch-type	Service provider switch type; see the "ISDN Service Provider Switch Types" table in the *Router Products Command Reference* publication for a list of supported switches. The default is **none**.

isdn tei [**first-call** \| **powerup**]
no isdn tei

To configure when ISDN Layer 2 terminal endpoint identifier (TEI) negotiation should occur, use the **isdn tei** global configuration command. Use the **no** form of this command to restore the default.

first-call	(Optional) ISDN TEI negotiation should occur when the first ISDN call is placed or received.
powerup	(Optional) ISDN TEI negotiation should occur when the router is powered on.

linecode b8zs

Use the **linecode b8zs** controller configuration command to select the B8ZS line-code type for the T1 line attached to an ISDN PRI.

pri-group [**timeslots** *range*]
no pri-group

To specify ISDN Primary Rate Interface (PRI) on a channelized T1 card on the Cisco 7000 series, use the **pri-group** controller configuration command. Use the **no pri-group** command to remove the ISDN PRI.

timeslots *range*	(Optional) Specifies a single range of values from 1 to 23.

show controllers bri *number*

To display information about the ISDN Basic Rate Interface (BRI), use the **show controllers bri** privileged EXEC command.

number Interface number. The value is 0 through 7 if the router has one BRI NIM or 0 through 15 if the router has two BRI NIMs.

show interfaces bri *number* [*first*] [*last*] [**accounting**]

Use the **show interfaces bri** privileged EXEC command to display information about the BRI D- and B-channels.

number Interface number. The value is 0 through 7 if the router has one BRI NIM or 0 through 15 if the router has two BRI NIMs. Specifying just the *number* will display the D-channel for that BRI interface.

first (Optional) Specifies the first of the B-channels; can be either 1 or 2. D-channel information is obtained by using the command without the optional arguments.

last (Optional) Specifies the last of the B-channels; can only be 2, indicating B-channels 1 and 2. D-channel information is obtained by using the command without the optional arguments.

accounting (Optional) Displays the number of packets of each protocol type that have been sent through the interface.

show isdn {**memory** | **timers** | **services**}

To display the information about memory, Layer 2 and Layer 3 timers and, on the Cisco 7000 series only, to display information about the status of PRI channels, use the **show isdn** EXEC command.

memory	Displays memory pool statistics.
timers	Displays the values of Layer 2 and Layer 3 timers.
services	Displays the status of PRI channels. (Cisco 7000 series only)

SMDS Commands

This chapter describes the function and displays the syntax of each SMDS command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **arp** *ip-address smds-address* **smds**

Use this variation of the **arp** global configuration command to enable ARP entries for static routing over the SMDS network. Use the **no** form of this command to disable this capability.

ip-address	IP address of the remote router.
smds-address	12-digit SMDS address in the dotted notation nnnn.nnnn.nnnn (48 bits long).
smds	Enables ARP for SMDS.

encapsulation smds

Use the **encapsulation smds** interface configuration command to enable SMDS service on the desired interface.

show arp

Use the **show arp** privileged EXEC command to display the entries in the ARP table for the router.

show smds addresses

Use the **show smds addresses** privileged EXEC command to display the individual addresses and the interface they are associated with.

show smds map

To display all SMDS addresses that are mapped to higher-level protocol addresses, use the **show smds map** privileged EXEC command.

show smds traffic

To display statistics about bad SMDS packets the router has received, use the **show smds traffic** privileged EXEC command.

[**no**] **smds address** *smds-address*

To specify the SMDS individual address for a particular interface, use the **smds address** interface configuration command. To remove the address from the configuration file, use the **no** form of this command.

smds-address	Individual address provided by the SMDS service provider. This address is protocol independent.

smds dxi

To enable the DXI 3.2 support, use the **smds dxi** interface configuration command. To disable the DXI 3.2 support, use the **no** form of this command.

[**no**] **smds enable-arp**

To enable dynamic Address Resolution Protocol (ARP), use the **smds enable-arp** interface configuration command. The multicast address for ARP must be set before this command is issued. Once ARP has been enabled, use the **no** form of this command to disable the interface.

[**no**] **smds multicast** *protocol smds-address*

To assign a multicast SMDS E.164 address to a higher-level protocol, use the **smds multicast** interface configuration command. To remove an assigned multicast address, use the **no smds multicast** command with the appropriate address.

protocol	Protocol type. See the "SMDS Multicast Supported Protocols" table in the *Router Products Command Reference* publication for a list of supported protocols and their keywords.
smds-address	SMDS address. Because SMDS does not incorporate broadcast addressing, a group address for a particular protocol must be defined to serve the broadcast function.

[**no**] **smds multicast arp** *smds-address* [*ip-address mask*]

To map the SMDS address to a multicast address, use the **smds multicast arp** interface configuration command. Use the **no** form of this command to disable this feature.

smds-address	SMDS address in E.164 format.
ip-address	(Optional) IP address.
mask	(Optional) Subnet mask for the IP address.

[**no**] **smds multicast bridge** *smds-address*

To enable spanning tree updates, use the **smds multicast bridge** interface configuration command. Use the **no** form of this command to disable this function.

smds-address	SMDS multicast address in E.164 format.

[**no**] **smds multicast ip** *smds-address* [*ip-address mask*]

To map an SMDS group address to a secondary IP address, use the **smds multicast ip** interface configuration command. Use the **no** form of this command to remove the address map.

smds-address	SMDS address in E.164 format.
ip-address	(Optional) IP address.
mask	(Optional) Subnet mask for the IP address.

[**no**] **smds static-map** *protocol protocol-address smds-address*
[**broadcast**]

To configure a static map between an individual SMDS address and a higher-level protocol address, use the **smds static-map** interface configuration command. Use the **no** form of this command with the appropriate arguments to remove the map.

protocol	Protocol. It can be one of the following values: **appletalk, clns**, **decnet**, **ip**, **ipx**, **vines**, or **xns**.
protocol-address	Address of the higher-level protocol.
smds-address	SMDS address, to complete the mapping.
broadcast	(Optional) Marks the specified protocol address as a candidate for broadcast packets. All broadcast requests will be sent to the unicast SMDS address.

X.25 and LAPB Commands

This chapter describes the function and displays the syntax of each X.25 and LAPB command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

bfe {**enter** | **leave**} *type number*

To allow the router to participate in emergency mode or to end participation in emergency mode when the interface is configured for **x25 bfe-emergency decision** and **x25 bfe-decision ask**, use the **bfe** EXEC command.

enter Causes the router to send a special address translation packet that includes an **enter emergency mode** command to the BFE if the emergency mode window is open. If the BFE is already in emergency mode, this command enables the sending of address translation information.

leave Disables the sending of address translation information from the router to the BFE when the BFE is in emergency mode.

type Interface type.

number Interface number.

clear x25-vc *type number* [*lcn*]

To clear switched virtual circuits (SVCs) and to reset permanent virtual circuits (PVCs), use the **clear x25-vc** privileged EXEC command. To clear all X.25 virtual circuits at once by restarting the packet layer service, use this command without an *lcn* argument.

type	Interface type.
number	Interface number.
lcn	(Optional) Virtual circuit.

[**no**] **cmns enable**

To enable Connection-Mode Network Service (CMNS) on a nonserial interface, use the **cmns enable** interface configuration command. Use the **no** form of this command to disable this capability.

encapsulation lapb [**dte** | **dce**] [**multi** | *protocol*]

To exchange datagrams over a serial interface using LAPB encapsulation, use the **encapsulation lapb** interface configuration command.

dte	(Optional) Specifies operation as a DTE. This is the default LAPB mode.
dce	(Optional) Specifies operation as a DCE.
multi	(Optional) Specifies use of multiple local-area network (LAN) protocols to be carried on the LAPB line.
protocol	(Optional) A single protocol to be carried on the LAPB line. A single protocol can be one of the following: **apollo**, **appletalk**, **clns** (ISO CLNS), **decnet**, **ip**, **ipx** (Novell IPX), **vines**, and **xns**. IP is the default protocol.

encapsulation x25 [**dte** | **dce**] [[**ddn** | **bfe**] | [**ietf**]]

To specify an interface’s operation as an X.25 device, use the **encapsulation x25** interface configuration command.

dte (Optional) Specifies operation as a DTE. This is the default X.25 mode.

dce (Optional) Specifies operation as a DCE.

ddn (Optional) Specifies DDN encapsulation on a router using DDN X.25 standard service.

bfe (Optional) Specifies BFE encapsulation on a router attached to a Blacker Front End device. Available for DTE operation only.

ietf (Optional) Specifies that the interface’s datagram encapsulation should default to use of the IETF standard method, as defined by RFC 1356.

lapb interface-outage *milliseconds*

To specify a period during which a link will remain connected, even if a brief hardware outage occurs, use the **lapb interface-outage** interface configuration command.

milliseconds Number of milliseconds a hardware outage can last without having the protocol disconnect the service. The default is 0 milliseconds, which disables this feature.

lapb k *window-size*

To specify the maximum permissible number of outstanding frames, called the window size, use the **lapb k** interface configuration command.

window-size Frame count. It can be a value from 1 to the modulo size minus 1. The default is 7 frames.

lapb modulo *modulus*

To specify the LAPB operating modulo as the basic (modulo 8) or extended (modulo 128) protocol modulo, use the **lapb modulo** interface configuration command.

modulus Either 8 or 128. The value 8 specifies LAPB’s basic mode; the value 128 specifies LAPB’s extended mode. The default is 8.

lapb n1 *bits*

To specify the maximum number of bits a frame can hold (the LAPB N1 parameter), use the **lapb n1** interface configuration command.

bits Number of bits from 1088 through 32840; it must be a multiple of eight. N1 defaults to the largest value available for the interface.

lapb n2 *tries*

To specify the maximum number of times a data frame can be transmitted (the LAPB N2 parameter), use the **lapb n2** interface configuration command.

tries Transmission count. It can be a value from 1 through 255. The default is 20 transmissions.

lapb protocol *protocol*

To configure the protocol carried on the LAPB line, use the **lapb protocol** interface configuration command.

protocol Protocol, entered by keyword. It can be one of the following: **appletalk**, **apollo**, **clns** (ISO CLNS), **decnet**, **ip**, **ipx** (Novell IPX), **vines**, and **xns**.

lapb t1 *milliseconds*

To set the retransmission timer period (the LAPB T1 parameter), use the **lapb t1** interface configuration command.

milliseconds	Time in milliseconds. It can be a value from 1 through 64000. The default is 3000 milliseconds.

lapb t4 *seconds*

To set the T4 idle timer, after which the router sends out a Poll packet to determine whether the link has suffered an unsignaled failure, use the **lapb t4** interface configuration command.

seconds	Number of seconds between reception of the last frame and the transmission of the outgoing Poll. The default value is 0 seconds, which disables the T4 timer feature.

show cmns [*type number*]

To display X.25 Level 3 parameters for LAN interfaces (such as Ethernet or Token Ring) and other information pertaining to CMNS traffic activity, use the **show cmns** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.

show interfaces serial *number*

To display information about a serial interface, use the **show interfaces serial** EXEC command.

number	Specifies the interface port number.

show llc2

To display active LLC2 connections, use the **show llc2** privileged EXEC command.

show x25 map

To display information about X.25 address maps, use the **show x25 map** EXEC command.

show x25 remote-red

To display the one-to-one mapping of the host IP addresses and the remote BFE device’s IP addresses, use the **show x25 remote-red** EXEC command.

show x25 route

To display the X.25 routing table, use the **show x25 route** EXEC command.

show x25 vc [*lcn*]

To display information about active switched virtual circuits (SVCs) and permanent virtual circuits (PVCs), use the **show x25 vc** EXEC command. To examine a particular virtual circuit, add an LCN argument to the **show x25 vc** command.

lcn	(Optional) Logical channel number (LCN).

[**no**] x25 accept-reverse

To configure the router to accept all reverse charge calls, use the **x25 accept-reverse** interface configuration command. To disable this facility, use the **no x25 accept-reverse** command.

x25 address *x.121-address*

To set the X.121 address of a particular network interface, use the **x25 address** interface configuration command.

x.121-address	Variable-length X.121 address. The address is assigned by the X.25 network service provider.

x25 bfe-decision {**no** | **yes** | **ask**}

To specify how a router configured for **x25 bfe-emergency decision** will participate in emergency mode, use the **x25 bfe-decision** interface configuration command.

no Prevents the router from participating in emergency mode and from sending address translation device. This is the default.

yes Allows the router to participate in emergency mode and to send address translation information enters emergency mode. The router obtains this information from the table created by the **x25 r**

ask Configures the router to prompt the console operator to enter the **bfe** EXEC command.

x25 bfe-emergency {**never** | **always** | **decision**}

To configure the circumstances under which the router participates in emergency mode, use the **x25 bfe-emergency** interface configuration command.

never Prevents the router from sending address translation information to the BFE. If it does not receive address translation information, the BFE cannot open a new connection for which it does not know the address. This is the default.

always Allows the router to pass address translations to the BFE when it enters emergency mode and an address translation table has been created.

decision Directs the router to wait until it receives a diagnostic packet from the BFE device indicating that the emergency mode window is open. The window is only open when a condition exists that allows the BFE is to enter emergency mode. When the diagnostic packet is received, the router's participation in emergency mode depends on how it is configured using the **x25 bfe-decision** command.

[**no**] **x25 default** *protocol*

To set a default protocol, use the **x25 default** interface configuration command. To remove the default protocol specified, use the **no x25 default** command.

protocol	Specifies the protocol to assume; may be **ip** or **pad**.

[**no**] **x25 facility** *facility-keyword value*

To force facilities on a per-call basis for calls originated by the router (switched calls are not affected), use the **x25 facility** interface configuration command. To disable a facility, use the **no x25 facility** command.

facility-keyword	User facility.
value	Facility value; see the "X.25 User Facilities" table in the *Router Products Command Reference* publication for supported facilities and their values.

x25 hic *circuit-number*

To set the highest incoming-only virtual circuit number, use the **x25 hic** interface configuration command.

circuit-number	Virtual circuit number from 1 through 4095, or 0 if there is no incoming-only virtual circuit range. The default is 0.

x25 hoc *circuit-number*

To set the highest outgoing-only virtual circuit number, use the **x25 hoc** interface configuration command.

circuit-number	Virtual circuit number from 1 through 4095, or 0 if there is no outgoing-only virtual circuit range. The default is 0.

x25 hold-queue *packets*
[**no**] **x25 hold-queue** [*packets*]

To set the maximum number of packets to hold until a virtual circuit is able to transmit, use the **x25 hold-queue** interface configuration command. To remove this command from the configuration file and restore the default value, use the **no** form of this command without an argument.

packets	Number of packets. A hold queue value of 0 allows an unlimited number of packets in the hold queue. The default is 10 packets.

x25 hold-vc-timer *minutes*
no x25 hold-vc-timer

To start the hold-vc-timer to prevent additional calls to a destination for a given period of time (thus preventing overruns on some X.25 switches caused by Call Request packets), use the **x25 hold-vc-timer** interface configuration command. To restore the default value for the timer, use the **no** form of this command.

minutes	Number of minutes to prevent calls from going to a previously failed destination. Incoming calls will still be accepted. The default is 0 minutes.

x25 htc *circuit-number*

To set the highest two-way virtual circuit number, use the **x25 htc** interface configuration command.

circuit-number	Virtual circuit number from 1 through 4095, or 0 if there is no two-way virtual circuit range. The default is 1024 for X.25 network service interfaces; 4095 for CMNS network service interfaces.

x25 idle *minutes*

To define the period of inactivity after which the router can clear a switched virtual circuit (SVC), use the **x25 idle** interface configuration command.

minutes	Idle period in minutes. The default is 0, which causes the router to keep the SVC open indefinitely.

[**no**] **x25 ip-precedence**

To enable the router to use IP precedence value when it opens a new virtual circuit, use the **x25 ip-precedence** interface configuration command. To cause the precedence value to be ignored when opening virtual circuits, use the **no** form of this command.

x25 ips *bytes*

To set the interface default maximum input packet size to match that of the network, use the **x25 ips** interface configuration command.

bytes	Byte count. It can be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. The default is 128 bytes.

x25 lic *circuit-number*

To set the lowest incoming-only virtual circuit number, use the **x25 lic** interface configuration command.

circuit-number	Virtual circuit number from 1 through 4095, or 0 if there is no incoming-only virtual circuit range. The default is 0.

[**no**] **x25 linkrestart**

To force X.25 Level 3 (packet-level) to restart when Level 2 (LAPB, the link level) resets, use the **x25 linkrestart** interface configuration command. To disable this function, use the **no** form of this command.

x25 loc *circuit-number*

To set the lowest outgoing-only virtual circuit number, use the **x25 loc** interface configuration command.

circuit-number Virtual circuit number from 1 through 4095, or 0 if there is no outgoing-only virtual circuit range. The default is 0.

x25 ltc *circuit-number*

To set the lowest two-way virtual circuit number, use the **x25 ltc** interface configuration command.

circuit-number Virtual circuit number from 1 through 4095, or 0 if there is no two-way virtual circuit range. The default is 1.

x25 map *protocol address* [*protocol2 address2* [...[*protocol9*
address9]]]
x.121-address [*option*]
no x25 map *protocol address x.121-address*

To set up the LAN protocols-to-remote host mapping, use the **x25 map** interface configuration command. To retract a mapping, use the **no x25 map** command with the appropriate network protocol(s) and X.121 address arguments.

protocol Protocol type, entered by keyword. As many as nine protocol and address pairs can be specified in one command line. See the "Protocols Supported by X.25" table in the *Router Products Command Reference* publication.

address	Protocol address.
x.121-address	X.121 address of the remote host.
option	(Optional) Provides additional functionality or allows X.25 facilities to be specified for originated calls. See the "X.25 Map Options" table in the *Router Products Command Reference* publication.

x25 map bridge *x.121-address* **broadcast** [*option*]

To configure Internet-to-X.121 address mapping for bridging over X.25, use the **x25 map bridge** interface configuration command.

x.121-address	The X.121 address.
broadcast	Required keyword for bridging over X.25.
option	(Optional) Services that can be added to this map. See "X.25 Map Options" table in the *Router Products Command Reference* publication.

[**no**] **x25 map cmns** *nsap mac-address*
[**no**] **x25 map cmns** *nsap* [*x.121-address*]

To map NSAP addresses to either MAC-layer addresses or X.121 addresses after enabling CMNS on a nonserial interface, use the **x25 map cmns** interface configuration command. To retract a mapping, use the **no** form of this command with the appropriate address arguments.

nsap	NSAP address. The NSAP can be either the actual DTE NSAP address or the prefix of the NSAP address. The NSAP prefix is sufficient for a best match to route a call.
mac-address	MAC-level address.
x.121-address	(Optional) X.121 address.

x25 map compressedtcp *address x.121-address* [*option*]
no x25 map compressedtcp *address x.121-address*

To map compressed TCP traffic to an X.121 address, use the **x25 map compressedtcp** interface configuration command. To delete a TCP header compression map for the link, use the **no** form of this command.

address IP address.

x.121-address X.121 address.

option (Optional) See the “X.25 Map Options” table in the *Router Products Command Reference* publication.

x25 modulo *modulus*

To set the window modulus, use the **x25 modulo** interface configuration command.

modulus Either 8 or 128. The value of the modulo parameter must agree with that of the device on the other end of the X.25 link. The default is 8.

x25 nvc *count*

To specify the maximum number of switched virtual circuits (SVCs) that a protocol can have open simultaneously to one host, use the **x25 nvc** interface configuration command.

count Circuit count from 1 to 8. A maximum of eight virtual circuits can be configured for each protocol/host pair l to increase throughput across networks. Protocols that do not tolerate out-of-order delivery, such as encapsulated TCP header compression, will only use one virtual circuit despite this value. The default is 1.

x25 ops *bytes*

To set the interface default maximum output packet size to match that of the network, use the **x25 ops** interface configuration command.

bytes	Byte count that is one of the following: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. The default is 128 bytes.

x25 pvc *circuit protocol address* [*protocol2 address2*[...[*protocol9 address9*]]] *x.121-address* [*option*]
no x25 pvc *circuit protocol address*

To establish an encapsulation permanent virtual circuit (PVC), use the *encapsulating* version of the **x25 pvc** interface configuration command. To delete the PVC, use the **no** form of this command with the appropriate channel number.

circuit	Virtual-circuit channel number which must be less than the virtual circuits assigned to the switched virtual circuits (SVCs).
protocol	Protocol type, entered by keyword. As many as nine protocol and address pairs can be specified in one command line. See the “Protocols Supported by X.25 PVCs” table in the *Router Products Command Reference* publication.
address	Protocol address of the host at the other end of the PVC.
x.121-address	X.121 address.
option	(Optional) Provides additional functionality or allows X.25 parameters to be specified for the PVC. Can be any of the options listed in the “X.25 PVC Options” table in the *Router Products Command Reference* publication.

x25 pvc *number1* **interface** *type number* **pvc** *number2* [*option*]

To configure a switched permanent virtual circuit (PVC) for a given interface, use the *switched* version of the **x25 pvc** interface configuration command.

number1 — PVC number that will be used on the local interface (as defined by the primary interface command).

interface — Required keyword to specify an interface.

type — Remote interface type.

number — Remote interface number.

pvc — Required keyword to specify a switched PVC.

number2 — PVC number that will be used on the remote interface.

option — (Optional) Adds certain features to the mapping specified. See “Switched PVC Options” table in the *Router Products Command Reference* publication.

x25 pvc *number1* **tunnel** *ip-address* **interface serial** *string* **pvc** *number2* [*option*]

To connect two permanent virtual circuits (PVCs) across a TCP/IP LAN, use the *tunnel* version of the **x25 pvc** interface configuration command.

number1 — PVC number of the connecting device.

tunnel — Indicates two PVCs will be connected across a TCP/IP LAN.

address — IP address of the router to which you are connecting.

interface serial — Indicates the interface is serial.

string — Serial interface specification that accepts either a number or a string in Cisco 7000 format (number/number) to denote the serial interface.

pvc	Indicates a PVC.
number2	Remote PVC number on the target interface.
option	(Optional) Adds certain features for the connection. See the "X.25 PVC Tunnel Options" table in the *Router Products Command Reference* publication.

x25 remote-red *host-ip-address* **remote-black** *blacker-ip-address*

To set up the table that lists the Blacker Front End (BFE) nodes (host or gateways) to which the router will send packets, use the **x25 remote-red** interface configuration command.

host-ip-address	IP address of the host or a router that the packets are being sent to.
remote-black	Delimits the addresses for the table being built.
blacker-ip-address	IP address of the remote BFE device in front of the host to which the packet is being sent.

[**no**] **x25 route** [**#** *position*] *x.121-address* [**cud** *pattern*] **interface** *type number*

x25 route [**#** *position*] *x.121-address* [**cud** *pattern*] **ip** *address* [*address2 ... address6*]
no x25 route [**#** *position*] *x.121-address* [**cud** *pattern*] **ip** *address*

[**no**] **x25 route** [**#** *position*] *x.121-address* [**cud** *pattern*] **alias** *type number*

[**no**] **x25 route** [**#** *position*] *x.121-address* [**substitute-source** *rewrite-pattern*] [**substitute-dest** *rewrite-pattern*] [**cud** *pattern*] **interface** *type number*

To create an entry in the X.25 routing table, use the **x25 route** global configuration command. To remove an entry from the table, enter the **no** form of this command with the appropriate arguments and keywords.

Note For typographical reasons, the last command is shown on three lines. When using the optional keywords in this variation of the **x25 route** command, the **substitute-source** keyword must precede the **substitute-dest** keyword, and both must precede the **cud** keyword. The entire command must be on one line.

# *position*	(Optional) A pound sign (#) followed by a number to designate a positional parameter at which to insert the new entry. If no *position* parameter is given, the entry is appended to the end of the routing table.
x.121-address	Called X.121 address pattern. This argument can be either an actual X.121 destination address or a regular expression such as 1111*, representing a group of X.121 addresses.
cud *pattern*	(Optional) Call User Data pattern, which is specified as a printable ASCII string. The Call User Data field may be present in a call packet and is commonly 4 bytes long.
interface *type number*	Keyword and destination interface type and unit or port number.
ip *address*	Keyword and IP address of the network interface or DTE for connections routed through a LAN. Optionally, up to five alternate IP addresses can be listed and each in turn will be tried in the event that the first destination fails.

alias *type number* Keyword and interface type and unit or port number of the interface alias. Encapsulation calls are normally accepted when the destination address is that of the interface (or the zero-length X.121 address). Aliases allow the specified interface to accept calls with other destination addresses.

substitute-source *rewrite-pattern* (Optional) See the "Pattern Rewrite Elements," "Pattern Matching," and "Character Matching" tables in the *Router Products Command Reference* publication.

substitute-dest *rewrite-pattern* (Optional) Specifies the called X.121 address to replace in locally routed X.25 calls. (For backwards compatibility, the **substitute** keyword will be accepted as **substitute-dest** and written to nonvolatile memory in the new format.) The backslash (\) character is treated specially in the argument *rewrite-pattern*; it indicates that the digit immediately following it selects a portion of the original called address to be inserted in the new called address. The characters \0 are replaced with the entire original address. The characters \1 through \9 are replaced with the strings that matched the first through ninth parenthesized parts of *X.121-pattern.* See the "Pattern Rewrite Elements" table in the *Router Products Command Reference* publication.

x25 routing [**use-tcp-if-defs**]
no x25 routing

To enable X.25 switching or tunneling, use the **x25 routing** global configuration command. To disable the forwarding of X.25 calls, use the **no** form of this command.

use-tcp-if-defs (Optional) May be used to modify the acceptance of calls received over TCP.

x25 rpoa *name number*
no x25 rpoa *name*

To specify a sequence of packet network carriers, use the **x25 rpoa** global configuration command. To remove the specified name, use the **no** form of this command.

name	Recognized Private Operating Agency (RPOA), which must be unique with respect to all other RPOA names. It is used in the **x25 facility** and **x25 map** interface configuration commands.
number	A sequence of 1 or more numbers used to describe an RPOA; up to 10 numbers are accepted.

[**no**] **x25 suppress-called-address**

To omit the destination address in outgoing calls, use the **x25 suppress-called-address** interface configuration command. To reset this command to the default state, use the **no** form of this command.

[**no**] **x25 suppress-calling-address**

To omit the source address in outgoing calls, use the **x25 suppress-calling-address** interface configuration command. To reset this command to the default state, use the **no** form of this command.

x25 t10 *seconds*

To set the value of the Restart Indication retransmission timer (T10) on DCE devices, use the **x25 t10** interface configuration command.

seconds	Time in seconds. The default is 60 seconds.

x25 t11 *seconds*

To set the value of the Incoming Call timer (T11) on DCE devices, use the **x25 t11** interface configuration command.

seconds	Time in seconds. The default is 180 seconds.

x25 t12 *seconds*

To set the value of the Reset Indication retransmission timer (T12) on DCE devices, use the **x25 t12** interface configuration command.

seconds	Time in seconds. The default is 60 seconds.

x25 t13 *seconds*

To set the value of the Clear Indication retransmission timer (T13) on DCE devices, use the **x25 t13** interface configuration command.

seconds	Time in seconds. The default is 60 seconds.

x25 t20 *seconds*

To set the value of the Restart Request retransmission timer (T20) on DTE devices, use the **x25 t20** interface configuration command.

seconds	Time in seconds. The default is 180 seconds.

x25 t21 *seconds*

To set the value of the Call Request timer (T21) on DTE devices, use the **x25 t21** interface configuration command.

seconds	Time in seconds. The default is 200 seconds.

x25 t22 *seconds*

To set the value of the Reset Request retransmission timer (T22) on DTE devices, use the **x25 t22** interface configuration command.

seconds	Time in seconds. The default is 180 seconds.

x25 t23 *seconds*

To set the value of the Clear Request retransmission timer (T23) on DTE devices, use the **x25 t23** interface configuration command.

seconds	Time in second. The default is 180 seconds.

x25 th *delay-count*

To set the data packet acknowledgment threshold, use the **x25 th** interface configuration command.

delay-count	Value between zero and the input window size. A value of 1 sends one Receiver Ready acknowledgment per packet. The default is 0 (which disables the acknowledgment threshold).

[**no**] **x25 use-source-address**

To override the X.121 addresses of outgoing calls forwarded over a specific interface, use the **x25 use-source-address** interface configuration command. To prevent updating the source addresses of outgoing calls, use the **no** form of this command.

x25 win *packets*

To change the default incoming window size to match that of the network, use the **x25 win** interface configuration command.

packets	Packet count that can range from 1 to one less than the window modulus. The default is 2 packets.

x25 wout *packets*

To change the default outgoing window size to match that of the network, use the **x25 wout** interface configuration command.

packets	Packet count that can range from 1 to the window modulus. The default is 2 packets.

Apollo Domain Commands

This chapter describes the function and displays the syntax of each Apollo Domain command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

apollo access-group *access-list-name*
no apollo access-group

To apply an access list to an interface, use the **apollo access-group** interface configuration command. To remove the access list, use the **no** form of this command.

access-list-name	Name of an access list to apply to the interface.

apollo access-list *access-list-name* {**deny** | **permit**}
[*firstnet*-]*lastnet.host* [*wildcard-mask*]
no apollo access-list *access-list-name*

To define an Apollo Domain access list, use the **access-list** global configuration command. To remove an access list, use the **no** form of this command.

access-list-name	Name of the access list.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
firstnet	(Optional) Number that specifies the lower limit of a selected Apollo network range.
lastnet.host	Number that specifies the upper limit of a selected Apollo network range. This is a 32-bit Apollo address consisting of a network number and a host number separated by a period. To specify all networks, use a value of –1.

wildcard-mask (Optional) A wildcard mask that uses the one bits to ignore the host part of the network address. Host bits corresponding to wildcard mask bits set to zero are used in comparisons.

apollo maximum-paths *paths*
no apollo maximum-paths

To set the maximum number of paths the router uses when sending packets, use the **apollo maximum-paths** global configuration command. To restore the default value, use the **no** form of this command.

paths Maximum number of equal-cost paths from which the router chooses. The argument *paths* can be a value from 1 to 512. The default is 1.

[**no**] **apollo network** *number*

To enable Apollo Domain routing on a particular interface, use the **apollo network** interface configuration command. To disable Apollo Domain routing on an interface, use the **no** form of this command. By default, Apollo routing is disabled.

number Network number. This is an eight-digit hexadecimal number consisting of the network address followed by the host address.

[**no**] **apollo route** *destination-network network.host*

To add a static route to the Apollo Domain routing table, use the **apollo route** global configuration command. To remove a route from the routing table, use the **no** form of this command.

destination-network Network to which you want to establish a static route. This is a 12-bit hexadecimal number. You can omit leading zeros.

network.host Network address of the router to which to forward packets destined for *destination-network*. The argument *network* is a 12-bit hexadecimal number. You can omit leading zeros. The argument *host* is the host number of the target router. This is a 20-bit hexadecimal value.

[**no**] **apollo routing** *host*

To enable Apollo routing, use the **apollo routing** global configuration command. To disable Apollo routing, use the **no** form of this command. By default, Apollo routing is disabled.

host Host number of the router. This is a five-digit hexadecimal host address that is unique across the Apollo internet.

apollo update-time *interval*
no apollo update-time

To set the interval between Apollo Domain routing updates, use the **apollo update-time** interface configuration command. To restore the default value, use the **no** form of this command.

interval Interval, in seconds, at which Apollo Domain routing updates are sent. The minimum interval is 10 seconds, and the maximum is 2493644 seconds. The default is 30 seconds.

show apollo arp

To list the entries in the Apollo Domain ARP table, use the **show apollo arp** EXEC command.

show apollo interface [*type number*]

To display the status of the Apollo Domain interfaces configured in the router and the parameters configured on each interface, use the **show apollo interface** EXEC command.

type	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), loopback, null, serial, or tunnel.
number	(Optional) Interface number.

show apollo route [*network*]

To display the contents of the Apollo Domain routing table, use the **show apollo route** EXEC command.

network	(Optional) Number of the network that the route is to. This is a 12-bit hexadecimal number.

show apollo traffic

To display information about the number and type of Apollo Domain packets transmitted and received by the router, use the **show apollo traffic** EXEC command.

AppleTalk Commands

This chapter describes the function and displays the syntax of each AppleTalk command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

access-list *access-list-number* {**deny** | **permit**} **additional-zones**

To define the default action to take for access checks that apply to zones, use the **access-list additional-zones** global configuration command.

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

access-list *access-list-number* {**deny** | **permit**} **cable-range** *cable-range*
no access-list *access-list-number* [{**deny** | **permit**} **cable-range** *cable-range*]

To define an AppleTalk access list for a cable range (for extended networks only), use the **access-list cable-range** global configuration command. To remove an access list, use the **no** form of this command.

access-list-number	Number of the access list. This is a decimal number from 600 to 699.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

cable-range — Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number.

access-list *access-list-number* {**deny** | **permit**} **includes**
cable-range
no access-list *access-list-number* [{**deny** | **permit**} **includes**
cable-range]

To define an AppleTalk access list that overlaps any part of a range of network numbers or cable ranges (for both extended and nonextended networks), use the **access-list includes** global configuration command. To remove an access list, use the **no** form of this command.

access-list-number — Number of the access list. This is a decimal number from 600 to 699.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

cable-range — Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number. To specify a network number, set the starting and ending network numbers to the same value.

access-list *access-list-number* {**deny** | **permit**} **network** *network*
no access-list *access-list-number* [{**deny** | **permit**} **network** *network*]

To define an AppleTalk access list for a single network number (that is, for a nonextended network), use the **access-list network** global configuration command. To remove an access list, use the **no** form of this command.

access-list-number — Number of the access list. This is a decimal number from 600 to 699.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

network — AppleTalk network number.

access-list *access-list-number* {**deny** | **permit**} **other-access**

To define the default action to take for access checks that apply to networks or cable ranges, use the **access-list other-access** global configuration command.

access-list-number — Number of the access list. This is a decimal number from 600 to 699.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

access-list *access-list-number* {**deny** | **permit**} **within** *cable-range*
no access-list *access-list-number* [{**deny** | **permit**} **within** *cable-range*]

To define an AppleTalk access list for an extended or a nonextended network whose network number or cable range is included entirely within the specified cable range, use the **access-list within** global configuration command. To remove this access list, use the **no** form of this command.

access-list-number — Number of the access list. This is a decimal number from 600 to 699.

deny Denies access if the conditions are matched.

permit Permits access if the conditions are matched.

cable-range Cable range or network number. The argument specifies the start and end of the cable range, separated by a hyphen. These arguments are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number. To specify a network number, set the starting and ending network numbers to the same value.

access-list *access-list-number* {**deny** | **permit**} **zone** *zone-name*
no access-list *access-list-number* [{**deny** | **permit**} **zone** *zone-name*]

To define an AppleTalk access list that applies to a zone, use the **access-list zone** global configuration command. To remove an access list, use the **no** form of this command.

access-list number Number of the access list. This is a decimal number from 600 to 699.

deny Denies access if the conditions are matched.

permit Permits access if the conditions are matched.

zone-name Name of the zone. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

appletalk access-group *access-list-number*
no appletalk access-group [*access-list-number*]

To assign an access list to an interface, use the **appletalk access-group** interface configuration command. To remove the access list use the **no** form of this command.

access-list-number	Number of the access list. This is a decimal number from 600 to 699.

appletalk address *network***.***node*
no appletalk address [*network***.***node*]

To enable nonextended AppleTalk routing on an interface, use the **appletalk address** interface configuration command. To disable nonextended AppleTalk routing, use the **no** form of this command.

*network***.***node*	AppleTalk network address assigned to the interface. The argument *network* is the 16-bit network number in the range 0 to 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

[**no**] **appletalk alternate-addressing**

To display network numbers in a two-octet format, use the **appletalk alternate-addressing** global configuration command. To return to displaying network numbers in the format *network.node*, use the **no** form of this command.

[**no**] **appletalk arp** [**probe** | **request**] **interval** *interval*

To specify the time interval between the retransmission of ARP packets, use the **appletalk arp interval** global configuration command. To restore both default intervals, use the **no** form of this command.

probe (Optional) Indicates that the interval specified is to be used with AARP requests that are trying to determined the address of the local router when the router is being configured. If you omit probe and request, probe is the default.

request (Optional) Indicates that the interval specified is to be used when AARP is attempting to determine the hardware address of another node so that AARP can deliver a packet.

interval Interval, in milliseconds, between AppleTalk ARP transmissions. When used with the **probe** keyword, the default interval is 200 milliseconds. When used with the **request** keyword, the default interval is 1000 milliseconds.

[**no**] **appletalk arp** [**probe** | **request**] **retransmit-count** *number*

To specify the number of AARP probe or request transmissions, use the **appletalk arp retransmit-count** global configuration command. To restore both default values, use the **no** form of this command.

probe (Optional) Indicates that the number specified is to be used with AARP requests that are trying to determine the address of the local router when the router is being configured. If you omit probe and request, probe is the default.

request (Optional) Indicates that the number specified is to be used when AARP is attempting to determine the hardware address of another node so that AARP can deliver a packet.

number — Number of AARP retransmissions that will occur. The minimum number is 1. When used with the **probe** keyword, the default value is 10 retransmissions. When used with the **request** keyword, the default value is 5 retransmissions. Specifying 0 selects the default value.

appletalk arp-timeout *interval*
no appletalk arp-timeout [*interval*]

To specify the interval at which entries are aged out of the ARP table, use the **appletalk arp-timeout** interface configuration command. To return to the default timeout, use the **no** form of this command.

interval — Time, in minutes, after which an entry is removed from the AppleTalk ARP table. The default is 240 minutes, or 4 hours.

[**no**] **appletalk aurp tickle-time** [*seconds*]

To set the AURP last-heard-from timer value, use the **appletalk aurp tickle-time** interface configuration command. To return to the default last-heard-from timer value, use the **no** form of this command.

seconds — Time-out value, in seconds. This value can be a number in the range 30 to infinity. The default is 90 seconds.

[**no**] **appletalk aurp update-interval** [*seconds*]

To set the minimum interval between AURP routing updates, use the **appletalk aurp update-interval** global configuration command. To return to the default interval, use the **no** form of this command.

seconds — AURP routing update interval, in seconds. This interval must be a multiple of 10. The default is 30 seconds.

[**no**] **appletalk cable-range** *cable-range* [*network***.***node*]

To enable an extended AppleTalk network, use the **appletalk cable-range** interface configuration command to enable an extended AppleTalk network. To disable an extended AppleTalk network, use the **no** form of this command.

cable-range Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These arguments are decimal number from 0 to 65279. The starting network number must be less than or equal to the ending network number.

*network***.***node* (Optional) Suggested AppleTalk address for the interface. The argument *network* is the 16-bit network number, and the argument *node* is the 8-bit node number. Both numbers are decimal. The suggested network number must fall within the specified range of network numbers.

[**no**] **appletalk checksum**

To enable the generation and verification of checksums for all AppleTalk packets (except routed packets), use the **appletalk checksum** global configuration command. To disable checksum generation and verification, use the **no** form of this command.

[**no**] **appletalk client-mode**

To allow users to access an AppleTalk zone when dialing into an asychronous line via the router's auxiliary port, use the **appletalk client-mode** interface configuration command. To disable this function, use the **no** form of this command.

[**no**] **appletalk discovery**

To place an interface into discovery mode, use the **appletalk discovery** interface configuration command. To disable discovery mode, use the **no** form of this command.

appletalk distribute-list *access-list-number* **in**
no appletalk distribute-list [*access-list-number* **in**]

To filter routing updates received from other routers over a specified interface, use the **appletalk distribute-list in** interface configuration command. To remove the routing table update filter, use the **no** form of this command.

access-list-number	Number of the access list. This is a decimal number from 600 to 699.

appletalk distribute-list *access-list-number* **out**
no appletalk distribute-list [*access-list-number* **out**]

To filter routing updates transmitted to other routers, use the **appletalk distribute-list out** interface configuration command. To remove the routing table update filter, use the **no** form of this command.

access-list-number	Number of the access list. This is a decimal number from 600 to 699.

appletalk domain-group *domain-number*
no appletalk domain-group [*domain-number*]

To assign a predefined domain number to an interface, use the **appletalk domain-group** interface configuration command. To remove an interface from a domain, use the **no** form of this command.

domain-number	Number of an AppleTalk domain. It can be a decimal integer from 1 through 1000000.

[**no**] **appletalk domain** *domain-number* **hop-reduction**

To reduce the hop-count value in packets traveling between segments of a domains, use the **appletalk domain hop-reduction** global configuration command. To disable the reduction of hop-count values, use the **no** form of this command.

domain-number	Number of an AppleTalk domain. It can be a decimal integer from 1 through 1000000.

[**no**] **appletalk domain** *domain-number* **name** *domain-name*

To create a domain and assign it a name and number, use the **appletalk domain name** global configuration command. To remove a domain, use the **no** form of this command.

domain-number	Number of an AppleTalk domain. It can be a decimal integer from 1 through 1000000.
domain-name	Name of an AppleTalk domain. The name must be unique across the AppleTalk internetwork. It can be up to 32 characters long and can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

appletalk domain *domain-number* **remap-range** {**in** | **out**} *start-range-end-range*
no appletalk domain *domain-number* **remap-range** {**in** | **out**} [*start-range-end-range*]

To remap ranges of AppleTalk network numbers or cable ranges between two segments of a domain, use the **appletalk domain remap-range** global configuration command. To disable remapping, use the **no** form of this command.

domain-number	Number of an AppleTalk domain. It can be a decimal integer from 1 through 1000000.
in	Specifies that the remapping is performed on inbound packets, that is, on packets arriving at the domain router. All network numbers or cable ranges coming from the domain are remapped into the specified range.

out Specifies that the remapping is performed on outbound packets, that is, on packets exiting from the domain router. All network numbers or cable ranges going to the domain are remapped into the specified range.

start-range First AppleTalk network number or beginning of cable range to remap. The number must be immediately followed by a hyphen.

end-range Last AppleTalk network number or end of cable range to remap. The number must be immediately preceded by a hyphen.

[**no**] **appletalk eigrp-splithorizon**

To configure split horizon, use the **appletalk eigrp-splithorizon** interface configuration command. To disable split horizon, use the **no** form of this command.

[**no**] **appletalk eigrp-timers** *hello-interval hold-tim***e**

To configure the AppleTalk Enhanced IGRP hello packet interval and the route hold time, use the **appletalk eigrp-timers** interface configuration command. To return to the default values for these timers, use the **no** form of this command.

hello-interval Interval between hello packets, in seconds. The default interval is 5 seconds. It can be a maximum of 30 seconds.

hold-time Hold time, in seconds. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The hold time can be in the range of 15 to 90 seconds. The default is 45 seconds.

[**no**] **appletalk event-logging**

To log significant network events, use the **appletalk event-logging** global configuration command. To disable this function, use the **no** form of this command.

[**no**] **appletalk free-trade-zone**

To establish a free-trade zone, use the **appletalk free-trade-zone** interface configuration command. To disable a free-trade zone, use the **no** form of this command.

appletalk getzonelist-filter *access-list-number*
no appletalk getzonelist-filter [*access-list-number*]

To filter GetZoneList (GZL) replies, use the **appletalk getzonelist-filter** interface configuration command. To remove a filter, use the **no** form of this command.

access-list-number	Number of the access list. This is a decimal number from 600 to 699.

[**no**] **appletalk glean-packets**

To derive AARP table entries from incoming packets, use the **appletalk glean-packets** interface configuration command. To disable this function, use the **no** form of this command.

[**no**] **appletalk ignore-verify-errors**

To allow a router to start functioning even if the network is misconfigured, use the **appletalk ignore-verify-errors** global configuration command. To disable this function, use the **no** form of this command.

appletalk iptalk *network*.*node zone*
no appletalk iptalk [*network*.*node zone*]

To enable IPTalk encapsulation on an interface that already has a configured IP address, use the **appletalk iptalk** interface configuration command. To disable IPTalk encapsulation, use the **no** form of this command.

network.*node* AppleTalk network address assigned to the interface. The argument *network* is the 16-bit network number, and the argument *node* is the 8-bit node number. Both numbers are decimal.

zone Name of the zone for the connected AppleTalk network.

appletalk iptalk-baseport *port-number*
no appletalk iptalk-baseport [*port-number*]

To specify the UDP port number when configuring IPTalk, use the **appletalk iptalk-baseport** global configuration command. To return to the default UDP port number, use the **no** form of this command.

port-number First UDP port number in the range of UDP ports used in mapping AppleTalk well-known DDP socket numbers to UDP ports. The default is 768.

appletalk lookup-type *service-type*
no appletalk lookup-type [*service-type*]

To specify which NBP service types are retained in the name cache, use the **appletalk lookup-type** global configuration command. To disable the caching of services, use the **no** form of this command.

service-type	AppleTalk service types. The name of a service type can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal numbers. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of possible types, see AppleTalk service types table in the *Router Products Command Reference* publication. The default is to retain ciscoRouter entries in name cache.

appletalk macip dynamic *ip-address* [*ip-address*]
    zone *server-zone*
no appletalk macip [**dynamic** *ip-address* [*ip-address*]
    zone *server-zone*]

To allocate IP addresses to dynamic MacIP clients, use the **appletalk macip dynamic** global configuration command. To delete a MacIP dynamic address assignment, use the **no** form of this command.

ip-address	IP address, in four-part dotted decimal notation. To specify a range, enter two IP addresses, which represent the first and last addresses in the range.

zone *server-zone* Zone in which the MacIP server resides. The argument *server-zone* can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to the Apple Computer, Inc. specification *Inside AppleTalk.*

appletalk macip server *ip-address* **zone** *server-zone*
no appletalk macip [**server** *ip-address* **zone** *server-zone*]

To establish a MacIP server for a zone, use the **appletalk macip server** global configuration command. To shut down a MACIP server, use the **no** form of this command.

ip-address IP address, in four-part dotted decimal notation. It is suggested that this address match the address of an existing IP interface.

zone *server-zone* Zone in which the MacIP server resides. The argument *server-zone* can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to the Apple Computer, Inc. specification *Inside AppleTalk.*

appletalk macip static *ip-address* {*ip-address* | **zone** *server-zone*}
no appletalk macip [**static** *ip-address* [*ip-address*] **zone** *server-zone*]

To allocate an IP address to be used by a MacIP client that has reserved a static IP address, use the **appletalk macip static** global configuration command. To delete a MacIP static address assignment, use the **no** form of this command.

ip-address	IP address, in four-part dotted decimal format. To specify a range, enter two IP addresses, which represent the first and last addresses in the range.
zone *server-zone*	Zone in which the MacIP server resides. The argument *server-zone* can include special characters from the Apple Macintosh character set. To include a special character, specify a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20. For a list of Macintosh characters, refer to Apple Computer, Inc. specification *Inside AppleTalk.*

appletalk name-lookup-interval *seconds*
no appletalk name-lookup-interval [*seconds*]

To set the interval between service pollings by the router on its AppleTalk interfaces, use the **appletalk name-lookup-interval** global configuration command. To purge the name cache and return to the default polling interval, use the **no** form of this command.

seconds	Interval, in seconds, between NBP lookup pollings. This can be any positive integer; there is no upper limit. It is recommended that you use an interval between 300 seconds (5 minutes) and 1200 seconds (20 minutes). The smaller the interval, the more packets are generated to handle the names. Specifying an interval of 0 purges all entries from the name cache and disables the caching of service type information that is controlled by the **appletalk lookup-type** command, including the caching of information about our routers. The default is 0 seconds.

[**no**] **appletalk permit-partial-zones**

To permit access to the other networks in a zone when access to one of those networks is denied, use the **appletalk permit-partial-zones** global configuration command. To return to the default behavior, which is to deny access to all networks in a zone if access to one of those networks is denied, use the **no** form of this command.

[**no**] **appletalk pre-fdditalk**

To enable the recognition of pre-FDDITalk packets, use the **appletalk pre-fdditalk** global configuration command. To disable this function, use the **no** form of this command.

[**no**] **appletalk protocol** {**aurp** | **eigrp** | **rtmp**}

To specify the routing protocol to use on an interface, use the **appletalk protocol** interface configuration command. To disable a routing protocol, use the **no** form of this command.

aurp	Specifies that the routing protocol to use is AURP. You can enable AURP only on tunnel interfaces.
eigrp	Specifies that the routing protocol to use is Enhanced IGRP.
rtmp	Specifies that the routing protocol to use is RTMP. RTMP is enabled by default.

appletalk proxy-nbp *network-number zone-name*
no appletalk proxy-nbp [*network-number zone-name*]

To assign a proxy network number for each zone in which there is a router that supports only nonextended AppleTalk, use the **appletalk proxy-nbp** global configuration command. To delete the proxy, use the **no** form of this command.

network-number	Network number of the proxy. It is a 16-bit decimal number and must be unique on the network. This is the network number that will be advertised by the router as if it were a real network number.
zone-name	Name of the zone that contains the routers that support only nonextended AppleTalk. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

[**no**] **appletalk require-route-zones**

To prevent the advertisement of routes (network numbers or cable ranges) that have no assigned zone, use the **appletalk require-route-zones** global configuration command. To disable this option and allow the router to advertise to its neighbors routes that have no network-zone association, use the **no** form of this command.

[**no**] **appletalk route-cache**

To enable fast switching on all supported interfaces, use the **appletalk route-cache** interface configuration command. To disable fast switching, use the **no** form of this command.

[**no**] **appletalk route-redistribution**

To redistribute RTMP routes into AppleTalk Enhanced IGRP and vice versa, use the **appletalk route-redistribution** global configuration command. To keep Enhanced IGRP and RTMP routes separate, use the **no** form of this command.

[**no**] **appletalk routing** [**eigrp** *router-number*]

To enable AppleTalk routing, use the **appletalk routing** global configuration command. To disable AppleTalk routing, use the **no** form of this command. If you omit the keyword and argument, this command enables AppleTalk routing without enabling Enhanced IGRP. In this case, the routing protocol used is RTMP.

eigrp *router-number* — (Optional) Specifies the Enhanced IGRP routing protocol. The argument *router-number* can be a decimal integer from 1 to 65535. It must be unique in your AppleTalk Enhanced IGRP internetwork.

[**no**] **appletalk send-rtmps**

To allow a router to send routing updates to its neighbors, use the **appletalk send-rtmps** interface configuration command. To block updates from being sent, use the **no** form of this command. By default, the router sends routing updates.

appletalk static cable-range *cable-range* **to** *network***.***node*
  zone *zone-name*
no appletalk static cable-range *cable-range* **to** *network***.***node*
  [**zone** *zone-name*]

To define a static route on an extended network, use the **appletalk static cable-range** global configuration command. To remove a static route, use the **no** form of this command.

cable-range
Cable range value. The argument specifies the start and end of the cable range, separated by a hyphen. These values are decimal numbers from 1 to 65279. The starting network number must be less than or equal to the ending network number.

*network***.***node*
AppleTalk network address of the remote router. The argument *network* is the 16-bit network number in the range 0 to 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

zone *zone-name*
Name of the zone on the remote network. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

[**no**] **appletalk static network** *network-number* **to** *network***.***node*
[**zone** *zone-name*]

To define a static route on a nonextended network, use the **appletalk static network** global configuration command. To remove a static route, use the **no** form of this command.

network-number	AppleTalk network number assigned to the interface. It is a 16-bit decimal number and must be unique on the network. This is the network number that will be advertised by the router as if it were a real network number.
*network***.***node*	AppleTalk network address of the remote router. The argument *network* is the 16-bit network number in the range 0 to 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.
zone *zone-name*	Name of the zone on the remote network. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

[**no**] **appletalk strict-rtmp-checking**

To perform maximum checking of routing updates to ensure their validity, use the **appletalk strict-rtmp-checking** global configuration command. To disable the maximum checking, use the **no** form of this command.

appletalk timers *update-interval valid-interval invalid-interval*
no appletalk timers [*update-interval valid-interval invalid-interval*]

To change the routing update timers, use the **appletalk timers** global configuration command. To return to the default routing update timers, use the **no** form of this command.

update-interval Time, in seconds, between routing updates sent to other routers on the network. The default is 10 seconds.

valid-interval Time, in seconds, that the router will consider a route valid without having heard a routing update for that route. The default is 20 seconds (two times the update interval).

invalid-interval Time, in seconds, that the route is retained after the last update. The default is 60 seconds (three times the valid interval).

[**no**] **appletalk virtual-net** *network-number zone-name*

To add AppleTalk users logging in on an asynchronous line and using PPP encapsulation to an internal network, use the **appletalk virtual-net global configuration** command. To remove an internal network, use the **no** form of this command.

network-number AppleTalk network address assigned to the interface. This is a 16-bit decimal network number in the range 0 to 65279. The network address must be unique across your AppleTalk internetwork.

zone-name Name of a new or existing zone to which the AppleTalk user will belong.

appletalk zip-query-interval *interval*
no zip-query-interval [*interval*]

To specify the interval at which the router sends ZIP queries, use the **appletalk zip-query-interval** global configuration command. To return to the default interval, use the **no** form of this command.

interval Interval, in seconds, at which the router sends ZIP queries. It can be any positive integer. The default is 10 seconds.

appletalk zipreply-filter *access-list-number*
no appletalk zipreply-filter [*access-list-number*]

To configure a ZIP reply filter, use the **appletalk zipreply-filter** interface configuration command. To remove a filter, use the **no** form of this command.

access-list-number Number of the access list. This is a decimal number from 600 to 699.

appletalk zone *zone-name*
no appletalk zone [*zone-name*]

To set the zone name for the connected AppleTalk network, use the **appletalk zone** interface configuration command. To delete a zone, use the **no** form of this command.

zone-name Name of the zone. The name can include special characters from the Apple Macintosh character set. To include a special character, type a colon followed by two hexadecimal characters. For zone names with a leading space character, enter the first character as the special sequence :20.

clear appletalk arp [*network***.***node*]

To delete all entries or a specified entry from the AARP table, use the **clear appletalk arp** EXEC command. If no network node is specified, this command deletes all entries from the table.

*network***.***node*	(Optional) Specific AppleTalk network address to be deleted from the router's AARP table. The argument *network* is the 16-bit network number in the range 0 to 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

clear appletalk neighbor [*neighbor-address*]

To delete all entries or a specified entry from the neighbor table, use the **clear appletalk neighbor** EXEC command. If no neighbor address is specified, this command deletes all entries from the table.

neighbor-address	(Optional) Network address of the specific neighboring router to be deleted from the neighbor table. The address is in the format *network.node*. The argument *network* is the 16-bit network number in the range 1 to 65279. The argument *node* is the 8-bit node number in the range 0 to 254. Both numbers are decimal.

clear appletalk route [*network*]

To delete all entries or a specified entry from the routing table, use the **clear appletalk route** EXEC command. If no network is specified, this command deletes all entries from the table

network	(Optional) Number of the specific network the route is to.

clear appletalk traffic

To reset AppleTalk traffic counters, use the **clear appletalk traffic** EXEC command.

ping appletalk *network***.***node*

To check host reachability and network connectivity, use the **ping appletalk** user EXEC command.

appletalk	Specifies the AppleTalk protocol.
*network***.***node*	AppleTalk address of the system to ping.

ping [**appletalk**] [*network***.***node*]

To check host reachability and network connectivity, use the **ping appletalk** privileged EXEC command.

appletalk	(Optional) Specifies the AppleTalk protocol.
network.node	(Optional) AppleTalk address of the system to ping.

show appletalk access-lists

To display the AppleTalk access lists currently defined, use the **show appletalk access-lists** user EXEC command.

show appletalk adjacent-routes

To display routes to networks that are directly connected or that are one hop away, use the **show appletalk adjacent-routes** privileged EXEC command.

show appletalk arp

To display the entries in the AARP cache, use the **show appletalk arp** privileged EXEC command.

show appletalk aurp events

To display the pending events in the AURP update-events queue, use the **show appletalk aurp events** privileged EXEC command.

show appletalk aurp topology

To display entries in the AURP private path database, which consists of all paths learned from exterior routers, use the **show appletalk aurp topology** privileged EXEC command.

show appletalk cache

To display the routes in the AppleTalk fast-switching table on an extended AppleTalk network, use the **show appletalk cache** EXEC command.

show appletalk domain [*domain-number*]

To display all domain-related information, use the **show appletalk domain** EXEC command.

domain-number	(Optional) Number of an AppleTalk domain about which to display information. It can be a decimal integer from 1 through 1000000.

show appletalk eigrp neighbors [*interface*]

To display the neighbors discovered by Enhanced IGRP, use the **show appletalk eigrp neighbors** EXEC command.

interface	(Optional) Displays information about the specified neighbor router.

show appletalk eigrp topology [*network-number* | **active** | **zero-successors**]

To display the AppleTalk Enhanced IGRP topology table, use the **show appletalk eigrp topology** EXEC command.

network-number	(Optional) Number of the AppleTalk network whose topology table entry you want to display.
active	(Optional) Displays the entries for all active routes.
zero-successors	(Optional) Displays the entries for destinations for which no successors exist. These entries are destinations that the router currently does not know how to reach via Enhanced IGRP. This option is useful for debugging network problems.

show appletalk globals

To display information and settings about the router's AppleTalk internetwork and other parameters, use the **show appletalk globals** EXEC command.

show appletalk interface [**brief**] [*type number*]

To display the status of the AppleTalk interfaces configured in the router and the parameters configured on each interface, use the **show appletalk interface** privileged EXEC command.

brief	(Optional) Displays a brief summary of the status of the AppleTalk interfaces.
type	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), FDDI, High Speed Serial Interface, Virtual Interface, ISDN Basic Rate Interface, ATM interface, loopback, null, or serial.

number	(Optional) Interface number.

show appletalk macip-clients

To display status information about all known MacIP clients, use the **show appletalk macip-clients** EXEC command.

show appletalk macip-servers

To display status information about a router’s servers, use the **show appletalk macip-servers** EXEC command.

show appletalk macip-traffic

To display statistics about MacIP traffic through the router, use the **show appletalk macip-traffic** EXEC command.

show appletalk name-cache

To display a list of NBP services offered by nearby routers and other devices that support NBP, use the **show appletalk name-cache** EXEC command.

show appletalk nbp

To display the contents of the NBP name registration table, use the **show appletalk nbp** EXEC command.

show appletalk neighbors [*neighbor-address*]

To display information about AppleTalk routers that are directly connected to any of the networks to which this router is directly connected, use the **show appletalk neighbors** EXEC command. If no neighbor address is specified, this command displays information about all AppleTalk routers.

neighbor-address	(Optional) Displays information about the specified neighbor router.

show appletalk remap [**domain** *domain-number* [{**in** | **out**}
[{**to** | **from**} *domain-network*]]]

To display domain remapping information, use the **show appletalk remap** EXEC command.

domain *domain-number*	(Optional) Number of an AppleTalk domain about which to display remapping information. It can be a decimal integer from 1 through 1000000.
in	(Optional) Displays remapping information about inbound packets, that is, on packets entering the local segment of the domain.
out	(Optional) Displays remapping information about outbound packets, that is on packets exiting from the local segment of the domain.
to	(Optional) Displays information about the network number or cable range to which an address has been remapped.
from	(Optional) Displays information about the original network number or cable range.
domain-network	(Optional) Number of an AppleTalk network.

show appletalk route [*network* | *interface*]

To display the entries in the AppleTalk routing table, use the **show appletalk route** EXEC command. If no network or unit type is specified, this command displays all entries in the routing table.

network	(Optional) Displays the routing table entry for the specified network.
interface	(Optional) Displays the routing table entries for networks that can be reached via the specified interface type and number.

show appletalk sockets [*socket-number*]

To display information about process-level operation in the sockets of an AppleTalk interface, use the **show appletalk sockets** EXEC command. If no socket number is specified, this command displays information about all sockets.

socket-number	(Optional) Displays information about the specified socket number.

show appletalk static

To display information the statically defined routes, use the **show appletalk static** EXEC command.

show appletalk traffic

To display statistics about AppleTalk traffic, including MacIP traffic, use the **show appletalk traffic** EXEC command.

show appletalk zone [*zone-name*]

To display the entries in the zone information table, use the **show appletalk zone** EXEC command. If no zone name is specified, the command displays all entries in the zone information table.

zone-name	(Optional) Displays the entry for the specified zone.

Banyan VINES Commands

This chapter describes the function and displays the syntax of each Banyan VINES command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

clear vines cache [**interface** *interface* | **neighbor** *address* |
server *network*]

To delete entries from the VINES fast-switching cache, use the **clear vines cache** EXEC command. If you do not specify any keywords or arguments, all entries in the fast-switch cache are deleted.

interface *interface*	(Optional) Deletes from the fast-switching cache table any entry that has one or more paths that go through the specified interface.
neighbor *address*	(Optional) Deletes from the fast-switching cache table any entry that has one or more paths via the specified neighbor router.
server *network*	(Optional) Deletes from the fast-switching cache table any entry whose network number part of the destination address matches the specified network address.The argument *network* can be either a 4-byte hexadecimal number or a 4-byte decimal number (if you have issued a **vines decimal** command).

clear vines ipc *number*

To delete VINES IPC connection blocks from the router, use the **clear vines ipc** EXEC command.

number	Hexadecimal number of the IPC connection to delete.

clear vines neighbor {*network* | *****}

To delete entries from the neighbor table, use the **clear vines neighbor** EXEC command.

network	Network number of the neighbor whose entry should be deleted from the neighbor table. The argument *network* can be either a 4-byte hexadecimal number or a 4-byte decimal number (if you have issued a **vines decimal** command).
*****	Deletes all entries from the neighbor path table except the entry for the local router.

clear vines route {*network* | *****}

To delete network addresses from the routing table, use the **clear vines route** EXEC command.

network	Network number of the entry to delete from the routing table. The argument *network* can be either a 4-byte hexadecimal number, a 4-byte decimal number (if you have issued a **vines decimal** command), or a host name (if you have issued a **vines host** command).
*****	Deletes all entries from the routing table.

clear vines traffic

To clear all VINES-related statistics that are displayed by the **show vines traffic** command, use the **clear vines traffic** EXEC command.

ping [**vines**] [*address*]

To determine basic network connectivity, use the **ping** EXEC command.

vines (Optional) Specifies the VINES protocol. If you omit this keyword, the router prompts for it.

address (Optional) Address of system to ping. If you omit the address, the router prompts for it.

show vines access [*access-list-number*]

To display the VINES access lists currently defined, use the **show vines access** EXEC command. If no access list number is specified, all access lists are displayed.

access-list-number (Optional) Number of the access list to display.

show vines cache [*address* | **interface** *type number* | **neighbor** *address* | **server** *network*]

To display the contents of the VINES fast-switching cache, use the **show vines cache** EXEC command. If no keywords or arguments are specified, all entries in the fast-switching cache are displayed.

address (Optional) Displays the entry in the fast-switching cache for the specified station.

interface *type number* (Optional) Displays all neighbors in the fast-switching cache that are accessible via the specified interface type and number.

neighbor *address* — (Optional) Displays all routes in the VINES fast-switching cache that have the specified neighbor as their first hop. The argument *address* is a 6-byte hexadecimal number in the format *network:host*, where *network* is 4 bytes and *host* is 2 bytes, a 4-byte decimal number in the same format (if you have issued a **vines decimal** command), or a host name (if you have issued a **vines host** command).

server *network* — (Optional) Displays all entries in the VINES fast-switching cache that are in the specified logical network. The argument *network* can be either a 4-byte hexadecimal number or a 4-byte decimal number (if you have issued a **vines decimal** command).

show vines host [*name*]

To display the entries in the VINES host name table, use the **show vines host** EXEC command. If no name is specified, all entries in the host name table are displayed.

name — (Optional) Displays the entry in the VINES name table that has the specified name.

show vines interface [*type number*]

To display status of the VINES interfaces configured in the router and the parameters configured on each interface, use the **show vines interface** EXEC command. If no interface is specified, values for all interfaces are displayed.

type — (Optional) Interface type.

number — (Optional) Interface number.

show vines ipc

To display information about any currently active IPC connections, use the **show vines ipc** EXEC command.

show vines neighbor [*address* | **interface** *type number* | **server** *number*]

To display the entries in the VINES neighbor table, use the **show vines neighbor** EXEC command. If no keywords or arguments are specified, all entries in the neighbor table are displayed.

address	(Optional) Displays the entry for the specified neighbor.
interface *type number*	(Optional) Displays all neighbor paths in the neighbor table that use the specified interface.
server *number*	(Optional) Displays all entries in the neighbor table that have the specified network number.

show vines route [*number* | **neighbor** *address*]

To display the contents of the VINES routing table, use the **show vines route** EXEC command. If no keywords or arguments are specified, all entries in the routing table are displayed.

number	(Optional) Displays the routing table entry for the specified network.
neighbor *address*	(Optional) Displays all routes in the VINES routing table that have the specified neighbor as their first hop.

show vines service [**fs** | **nsm** | **ss** | **vs**]

To display information about the router’s current time, use the show **vines service** EXEC command.

fs	(Optional) Displays file service information.
nsm	(Optional) Displays network and system management service information.
ss	(Optional) Displays server service information.
vs	(Optional) Displays security service information.

show vines traffic [*type number*]

To display the statistics maintained about VINES protocol traffic, use the **show vines traffic** EXEC command. If no interface is specified, values for all interfaces are displayed.

type number	(Optional) Displays values for a specific interface.

trace [**vines** | **oldvines**] [*address*]

To determine the path that a packet takes when traversing a VINES network, use the **trace** EXEC command.

vines	(Optional) Specifies the VINES protocol. If you omit this keyword, the router prompts for it.
oldvines	(Optional) Specifies the VINES protocol. This trace is compatible with our **trace** function prior to IOS Release 10.2.

address	(Optional) Address of a node. This is a 6-byte hexadecimal number in the format *network:host*, where *network* is 4 bytes and *host* is 2 bytes.

[**no**] **vines access-group** *access-list-number*

To apply an access list to an interface, use the **vines access-group** interface configuration command. To remove the access list, use the **no** form of this command.

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 1 to 100. For extended access lists, *access-list-number* is a decimal number from 101 to 200.

vines access-list *access-list-number* {**deny** | **permit**} *protocol*
source-address source-mask [*source-port*] *destination-address*
destination-mask [*destination-port*]
no vines access-list *access-list-number*

To specify a standard VINES access list, use this version of the **vines access-list** global configuration command. To remove the access list, use the **no** form of this command.

access-list-number	Number of the access list. This is a decimal number from 1 to 100.
deny	Denies access if the conditions are matched.
permit	Allows access if the conditions are matched.

protocol

VINES protocol ID number or name. It can be a value from 1 to 255 or one of the following protocol keywords:

- **arp**—Address Resolution Protocol
- **icp**—Internet Control Protocol
- **ip**—VINES Internet Protocol
- **ipc**—Interprocess Communications
- **rtp**—Routing Update Protocol
- **spp**—Sequence Packets Protocol

source-address

Address of the network from which the packet is being sent. This is a 6-byte hexadecimal number in the format *network:host*, where *network* is 4 bytes and *host* is 2 bytes.

source-mask

Mask to be applied to *source-address*. This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bit in the address that should be ignored.

source-port

(Optional) Number of the local port from which the packet is being sent. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 through 0xFFFF. Well-known local port numbers have values from 0x0001 through 0x01FF. Transient local port numbers have values from 0x0200 through 0xFFFE. Refer to the IPC port number table in the *Router Products Command Reference* publication for a list of some IPC port numbers.

destination-address Address of the network to which the packet is being sent. This is a 6-byte hexadecimal number in the format *network:host*, where *network* is 4 bytes and *host* is 2 bytes.

destination-mask Mask to be applied to *destination-address*. This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bits in the address that should be ignored.

destination-port (Optional) Number of the local port to which the packet is being sent. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 through 0xFFFF. Well-known local port numbers have values from 0x0001 through 0x01FF. Transient local port numbers have values from 0x0200 through 0xFFFE. Refer to the IPC port number table in the *Router Products Command Reference* publication for a list of some IPC port numbers.

vines access-list *access-list-number* {**deny** | **permit**} *protocol*
source-address source-mask [*source-port source-port-mask*]
destination-address destination-mask [*destination-port*
destination-port-mask]
no vines access-list *access-list-number*

To create an extended VINES access list, use this version of the **vines access-list** global configuration command. To remove an extended access list, use the **no** form of this command.

access-list-number — Number of the access list. This is a decimal number from 101 to 200.

deny — Denies access if the conditions are matched.

permit — Allows access if the conditions are matched.

protocol — VINES protocol ID number or name. The number can be a value from 1 to 255 or one of the following protocol keywords:

- **arp**—Address Resolution Protocol
- **icp**—Internet Control Protocol
- **ip**—VINES Internet Protocol
- **ipc**—Interprocess Communications
- **rtp**—Routing Update Protocol
- **spp**—Sequence Packets Protocol 276

source-address — Address of the network from which the packet is being sent. This is a 6-byte hexadecimal number in the format *network:host*, where *network* is 4 bytes and *host* is 2 bytes.

source-mask — Mask to be applied to *source-address*. This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bits in the address that should be ignored.

source-port Number of the local port from which the packet is being sent. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 through 0xFFFF. Well-known local port numbers have values from 0x0001 through 0x01FF. Transient local port numbers have values from 0x0200 through 0xFFFE. Refer to the IPC port number table in the *Router Products Command Reference* publication for a list of some IPC port numbers.

source-port-mask (Optional) Mask to be applied to *source-port*. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 through 0xFFFF. These bits correspond to the bits in the port that should be ignored.

destination-address VINES address of the network to which the packet is being sent. This is a 6-byte hexadecimal number in the format *network:host*, where *network* is 4 bytes and *host* is 2 bytes.

destination-mask Mask to be applied to *destination-address*. This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bits in the address that should be ignored.

destination-port
Number of the local port to which the packet is being sent. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 through 0xFFFF. Well-known local port numbers have values from 0x0001 through 0x01FF. Transient local port numbers have values from 0x0200 through 0xFFFE. Refer to the IPC port number table in the *Router Products Command Reference* publication for a list of some IPC port numbers.

destination-port-mask
(Optional) Mask to be applied to *destination-port*. This argument is required when the protocol specified is IPC or SPP, and is not accepted when any other protocol is specified. It can be a number from 0x0000 through 0xFFFF. These bits correspond to the bits in the port that should be ignored.

vines access-list *access-list-number* {**deny** | **permit**} *source-address source-mask*
no vines access-list *access-list-number*

To create a simple VINES access list, use this version of the **vines access-list** global configuration command. To remove a simple access list, use the **no** form of this command.

access-list-number	Access list number. It is a number from 201 to 300.
deny	Denies access if the conditions are matched.
permit	Allows access if the conditions are matched.
source-address	Address of the network from which the packet is being sent. This is a 6-byte hexadecimal number in the format *network:host*, where *network* is 4 bytes and *host* is 2 bytes.
source-mask	Mask to be applied to *source-address*. This is a 6-byte hexadecimal value. Place ones in the bit positions you want to mask. These bits correspond to the bits in the address that should be ignored.

[**no**] **vines arp-enable** [**dynamic**]

To enable the processing of ARP packets, use the **vines arp-enable** interface configuration command. To disable the processing of ARP packets, use the **no** form of this command. By default, the interface always responds to ARP and SARP requests.

dynamic	(Optional) Respond to ARP and SARP requests on this interface only if there are no other VINES servers present.

[**no**] **vines decimal**

To display VINES addresses in decimal notation, use the **vines decimal** global configuration command. To return to displaying the addresses in hexadecimal, use the **no** form of this command. By default, addresses are displayed in hexadecimal.

vines encapsulation [**arpa** | **snap** | **vines-tr**]
no vines encapsulation

To set the MAC-level encapsulation used for VINES broadcast packets, use the **vines encapsulation** interface configuration command. To disable encapsulation, use the **no** form of this command.

arpa	(Optional) ARPA encapsulation. This is the default encapsulation for Ethernet interfaces.
snap	(Optional) SNAP encapsulation. This encapsulation uses an IEEE 802.2 SNAP header. This is the default encapsulation for all media except Ethernet and Token Ring.
vines-tr	(Optional) Our VINES Token Ring encapsulation. This is the default encapsulation for Token Ring interfaces.

vines host *name address*
no vines host *name*

To associate a host name with a VINES address, use the **vines host** global configuration command. To delete the association, use the **no** form of this command. The default is to display hosts by address.

name	VINES host name. It can be any length and sequence of characters separated by white space.
address	Number of a VINES network. You enter it in the current VINES radix, in the format *network*:*host*, where *network* is 4 bytes and *host* is 2 bytes.

vines input-network-filter *access-list-number*
no vines input-network-filter

To filter the information contained in routing messages received from other stations, use the **vines input-network-filter** interface configuration command. To disable this filtering, use the **no** form of this command.

access-list-number	Number of the access list. It is a decimal number from 201 to 300.

vines input-router-filter *access-list-number*
no vines input-router-filter

To filter received routing messages based upon the address of the sending station, use the **vines input-router-filter** interface configuration command. To disable this filtering, use the **no** form of this command.

access-list-number	Number of the access list. It is a decimal number from 201 to 300.

vines metric [*whole* [*fractional*]]
no vines metric

To enable VINES routing on an interface, use the **vines metric** interface configuration command. To disable VINES routing, use the **no** form of this command.

whole	(Optional) Integer cost value associated with the interface. It is optional for all interface types. If you omit *metric*, the router automatically chooses a reasonable value. Refer to the metric values table in the *Router Products Command Reference* publication. If metric is zero, then a fractional portion must be supplied.

fractional — (Optional) Fractional cost value associated with the interface expressed in 10,000ths. It is optional for all interface types, but may only be present if a whole number portion is specified. This number will be rounded to the nearest 1/16. If you omit *metric*, the router automatically chooses a reasonable value. These values are listed in VINES IPC port number table in the *Router Products Command Reference* publication.

vines neighbor *address mac-address encapsulation* [*whole* [*fractional*]]
no vines neighbor *address mac-address*

To specify a static path to a neighbor station, use the **vines neighbor** interface configuration command. To remove a static path from the neighbor table, use the **no** form of this command.

address — VINES IP address of the station to which to add or remove a static path.

mac-address — MAC-level address used to reach the neighbor station.

encapsulation — Encapsulation type to use on the media. It can be one of the following values:

- **arpa**—Use ARPA encapsulation. This is recommended for Ethernet interfaces.
- **snap**—Use an IEEE 802.2 SNAP header. This is recommended for FDDI interfaces.
- **vines-tr**—Use our VINES Token Ring encapsulation. This is recommended for Token Ring interfaces.

whole — (Optional) Delay metric to use on the neighbor. If you omit this argument, the metric used is that specified with the **vines metric** command for the selected interface.

fractional (Optional) Fractional metric value associated with this neighbor. This number will be rounded to the nearest 1/16. If you omit both whole and fractional numbers, then the interface metric will be used.

vines output-network-filter *access-list-number*
no vines output-network-filter

To filter the information contained in routing updates transmitted to other stations, use the **vines output-network-filter** interface configuration command. To disable this filtering, use the **no** form of this command.

access-list-number Number of the access list. It is a decimal number from 201 to 300.

[**no**] **vines propagate** [**dynamic**]

To modify how routers forward a broadcast packet, use the **vines propagate** interface configuration command. To return to the default dynamic forwarding scheme, use the **no** form of this command. If you omit the keyword, broadcast messages are always propagated on the interface.

dynamic (Optional) Propagates broadcasts on this interface only if there are no servers on any local network.

vines redirect [*seconds*]
no vines redirect

To determine how frequently a router sends an RTP redirect message on an interface, use the **vines redirect** interface configuration command. To restore the default, use the **no** form of this command.

seconds (Optional) Interval, in seconds, that the router waits after sending a redirect message on an interface before it sends another redirect message on that same interface. If you specify a value of 0, the router never sends redirect messages on that interface. The default is 1 second.

[**no**] **vines route** *number address* [*whole* [*fractional*]]

To specify a static route to a server, use the **vines route** global configuration command. To remove a static route from the routing table, use the **no** form of this command. By default, no static routes are specified.

number Number of the server to which to add or remove the static route.

address VINES IP address of the neighbor station to use to reach the server.

whole (Optional) Metric value assigned to this route.

fractional (Optional) Fractional cost value associated with this route.

[**no**] **vines route-cache**

To enable fast switching, use the **vines route-cache** interface configuration command. To disable fast switching, use the **no** form of this command.

vines routing [*address* | **recompute**]
no vines routing

To enable VINES routing, use the **vines routing** global configuration command. To disable VINES routing, use the **no** form of this command.

address	(Optional) Network address of the router. You should specify an address on a router that does not have any Ethernet or FDDI interfaces. You also can specify an address in the unlikely event that two routers map themselves to the same address.
recompute	(Optional) Dynamically redetermine the router's network address.

[**no**] **vines serverless** [**dynamic** | **broadcast**]

To configure a Banyan VINES network that does not have a server, use the **vines serverless** interface configuration command. To turn off this functionality, use the **no** form of this command. If all keywords are omitted, broadcasts are always forwarded toward one server.

dynamic	(Optional) Forward broadcasts toward one server only if there are no servers present on this interface. This is the default.
broadcast	(Optional) Flood broadcasts out all router interfaces in order to reach all servers.

[**no**] **vines split-horizon**

To use split horizon when sending routing updates, use the **vines split-horizon** interface configuration command. To disable split horizon, use the **no** form of this command.

[**no**] **vines srtp-enabled**

To enable Sequenced Routing Update Protocol (SRTP), use the **vines srtp-enabled** global configuration command. To disable SRTP, use the **no** form of this command.

vines time access-group *access-list-number*
no vines time access-group

To control the servers from which the router will accept VINES network time, use the **vines time access-group** global configuration command. To accept VINES network time messages from any server, use the **no** form of this command.

access-list-number	Number of the access list. It is a decimal number from 201 to 300.

vines time destination *address*
no vines time destination

To control the servers to which the router sends VINES network time, use the **vines time destination** global configuration command. To send VINES network time messages to all servers, use the **no** form of this command.

address	Destination VINES address for the network time messages.

[**no**] **vines time participate**

To enable the router's participation in the synchronization of time across a VINES network, use the **vines time participate** global configuration command. To disable the router's participation in time synchronization, use the **no** form of this command.

[**no**] **vines time set-system**

To set the router's internal time based upon the received VINES network time, use the **vines time set-system** global configuration command. To uncouple the router's time from VINES network time, use the **no** form of this command.

[**no**] **vines time use-system**

To set VINES network time based upon the router’s internal time, use the **vines time use-system** global configuration command. To uncouple VINES network time from the router’s time, use the **no** form of this command.

[**no**] **vines update deltas**

To modify the manner in which routing updates are sent, use the **vines update deltas** interface configuration command. To return to the default method, use the **no** form of this command.

[**no**] **vines update interval** [*seconds*]

To modify the frequency at which routing updates are sent, use the **vines update interval** interface configuration command. To return to the default frequency, use the **no** form of this command.

seconds	Interval, in seconds, between the sending of periodic VINES routing updates. This can be a number in the range 0 to 2^{32} and will be rounded up to the nearest 5 seconds. The default value is 90 seconds. If you omit *seconds* or specify a value of 0, the default value of 90 seconds is used.

DECnet Commands

This chapter describes the function and displays the syntax of each DECnet command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

access-list *access-list-number* {**permit** | **deny**} *source source-mask*
no access-list

To create a standard access list, use the **access-list** global configuration command. Use the **no** form of this command to delete the entire access list.

access-list-number	Integer you choose between 300 and 399 that uniquely identifies the access list.
permit	Permits access when there is an address match.
deny	Denies access when there is an address match.
source	Source address. DECnet addresses are written in the form *area.node*. For example, 50.4 is node 4 in area 50. All addresses are in decimal.
source-mask	Mask to be applied to the address of the source node. Bits are set wherever the corresponding bits in the address should be ignored. All masks are in decimal.

access-list *access-list-number* {**permit** | **deny**} *source source-mask*
[*destination*] [*destination-mask*]
no access-list

To create an extended access list, use the **access-list** global configuration command. Use the **no** form of this command to delete the entire access list.

access-list-number — Integer you choose between 300 and 399 that uniquely identifies the access list.

permit — Permits access when there is an address match.

deny — Denies access when there is an address match.

source — Source address. DECnet addresses are written in the form *area.node*. For example, 50.4 is node 4 in area 50. All addresses are in decimal.

source-mask — Mask to be applied to the address of the source node. All masks are in decimal.

destination — (Optional) Destination node's DECnet address in decimal format. DECnet addresses are written in the form *area.node*. For example, 50.4 is node 4 in area 50.

destination-mask — (Optional) Destination mask. DECnet addresses are written in the form *area.node*. For example, 50.4 is node 4 in area 50. All masks are in decimal.

access-list *access-list-number* {**permit** | **deny**} *source source-mask*
[*destination destination-mask* **eq** | **neq** [*source-object* |
destination-object | *identification* | **any**]]
no access-list

The optional argument *source-object* consists of the following string:

src [[**eq** | **neq** | **gt** | **lt**] *object-number*] [**exp** *regular expression*]
[**uic** [*group, user*]]

The optional argument *destination-object* consists of the following string:

dst [[**eq** | **neq** | **gt** | **lt**] *object-number*] [**exp** *regular expression*]
[**uic** [*group, user*]]

The optional argument *identification* consists of the following string:

[**id** *regular expression*] [**password** *regular expression*] [**account** *regular expression*]

To create an access list that filters *connect initiate* packets, use the **access-list** global configuration command. Use the **no** form of this command to disable the access list.

access-list-number	Integer you choose between 300 and 399 that uniquely identifies the access list.
permit	Permits access when there is an address match.
deny	Denies access when there is an address match.
source	Source address. DECnet addresses are written in the form *area.node*. For example, 50.4 is node 4 in area 50. All addresses are in decimal.
source-mask	Mask to be applied to the address of the source node. All masks are in decimal.
destination	(Optional) Destination node's DECnet address in decimal format. DECnet addresses are written in the form *area.node*. For example, 50.4 is node 4 in area 50. All addresses are in decimal.

destination-mask

(Optional) Destination mask. DECnet addresses are written in the form *area.node*. For example, 50.4 is node 4 in area 50. All masks are in decimal.

eq | **neq**

Use either of these keywords:

eq—item matches the packet if *all* the specified parts of *source-object*, *destination-object*, and *identification* match data in the packet.

neq—item matches the packet if *any* of the specified parts do *not* match the corresponding entry in the packet.

source-object

(Optional) Contains the keyword **src** and one of the following optional keywords:

eq | **neq** | **lt** | **gt**—equal to, not equal to, less than, or greater than. These keywords must be followed by the argument *object-number*, a numeric DECnet object number.

exp—stands for expression; followed by a regular expression that matches a string.

uic—stands for user identification code; followed by a numeric user ID (UID) expression.The argument [*group*, *user*] is a numeric UID expression. In this case, the bracket symbols are literal; they must be entered. The group and user parts can be specified in decimal, in octal by prefixing the number with a 0, or in hex by prefixing the number with 0x. The uic expression is displayed in show displays as an octal number.

destination-object

(Optional) Contains the mandatory keyword **dst** and one of the following optional keywords:

eq | **neq** | **lt** | **gt**—equal to, not equal to, less than, or greater than. These keywords must be followed by the argument *object-number*, a numeric DECnet object number.

exp—stands for expression; followed by a regular expression that matches a string.

uic—stands for user identification code; followed by a numeric user ID (UID) expression. In this case, the bracket symbols are literal; they must be entered. The group and user parts can either be specified in decimal, in octal by prefixing the number with a 0, or in hex by prefixing the number with 0x. The uic expression is displayed in show displays as an octal number.

identification

(Optional) Uses any of the following three keywords:

id—regular expression; refers to user ID.

password—regular expression; the password to the account.

account—regular expression; the account string.

any

Item matches if *any* of the specified parts *do* match the corresponding entries for *source-object*, *destination-object*, or *identification*.

clear decnet counters

To clear DECnet counters that are shown in the output of the **show decnet traffic** EXEC command, use the **clear decnet counters** EXEC command.

decnet access-group *access-list number*

To create a DECnet access group, use the **decnet access-group** interface configuration command.

access-list-number	Either a standard or extended DECnet access list. A standard DECnet access list applies to destination addresses. The value (or values in the case of extended lists) can be in the range 300 through 399.

decnet advertise *decnet-area hops cost*
no decnet advertise [*decnet-area*]

To configure border routers to propagate Phase IV areas through an OSI backbone, use the **decnet advertise** global configuration command. To disable this feature, use the **no** form of this command.

decnet-area	Phase IV area that you want propagated.
hops	Hop count to be associated with the route being advertised. Default is 0.
cost	Cost to be associated with the route being advertised. Default is 0.
decnet-area	Phase IV area that you want propagated.

decnet [*network-number*] **area-max-cost** *value*

To set the maximum cost specification value for *interarea* routing, use the **decnet area-max-cost** global configuration command.

network-number	(Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). The default is network 0.
value	Maximum cost for a route to a distant area that the router may consider usable; the router treats as unreachable any route with a cost greater than the value you specify. A valid range for cost is from 1 through 1022. This parameter is only valid for area routers. The default is 1022.

decnet [*network-number*] **area-max-hops** *value*

To set the maximum hop count value for *interarea* routing, use the **decnet area-max-hops** global configuration command.

network-number	(Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.
value	Maximum number of hops for a usable route to a distant area. The router treats as unreachable any route with a count greater than the value you specify. A valid range for the hop count is from 1 through 30. The default is 30 hops.

decnet congestion-threshold *number*
no decnet congestion-threshold

Use the **decnet congestion-threshold** interface configuration command to set the congestion-experienced bit if the output queue has more than the specified number of packets in it. A *number* value of zero or the **no** form of this command prevents this bit from being set. Use the **no** form of this command to remove the parameter setting and set it to 0.

number	Number of packets that are allowed in the output queue before the system will set the congestion experience bit. This value is an integer between 0 and 0x7fff. The value zero prevents this bit from being set. Only relatively small integers are reasonable. The default is 1 packet.

[**no**] **decnet conversion** *nsap-prefix*

To allow Phase IV routers (running Software Release 9.1 or later) to run in a Phase V network and vice versa, enable conversion with the **decnet conversion** global configuration command. To disable conversion, use the **no** form of this command.

nsap-prefix	Value used for the IDP field when constructing NSAPs from a Phase IV address**.**

decnet cost *cost-value*
no decnet cost

To set a cost value for an interface, use the **decnet cost** interface configuration command. Use the **no** form of this command to disable DECnet routing for an interface.

cost-value	Integer from 1 through 63. There is no default cost for an interface, although a suggested cost for FDDI is 1, for Ethernet is 4, and for serial links is greater than 10.

decnet encapsulation {**pre-dec** | **dec**}

To provide DECnet encapsulation over Token Ring, use the **decnet encapsulation** interface configuration command.

pre-dec Configures routers for operation on the same Token Ring with routers running software versions prior to Release 9.1. In this mode, Cisco routers cannot communicate with non-Cisco equipment. Referred to as Cisco-style encapsulation.

dec Provides encapsulation that is compatible with other Digital equipment. All Cisco routers must be running Software Release 9.1 or later. The default is **dec**.

decnet hello-timer *seconds*
no decnet hello-timer

To change the interval for sending broadcast hello messages, use the **decnet hello-timer** interface configuration command. To restore the default value, use the **no** form of this command.

seconds Interval at which the router sends hello messages. It can be a decimal number in the range 1 through 8191 seconds. The default is 15 seconds.

decnet host *name decnet-address*
no decnet host *name*

Use the **decnet host** global configuration command to associate a name-to-DECnet address mapping, which will show up in the output of various commands. To disable name mapping, use the **no** form of this command.

name A name you choose that uniquely identifies this DECnet address.

decnet-address Source address. DECnet addresses are written in the form *area.node*. For example, 50.4 is node 4 in area 50. All addresses are in decimal.

decnet in-routing-filter *access-list-number*
no decnet in-routing-filter

To provide access control to hello messages or routing information received on an interface, use the **decnet in-routing-filter** interface configuration command. Use the **no** form of this command to remove access control.

access-list-number	Standard DECnet access list. This list applies to destination addresses. The value can be in the range 300 through 399.

decnet *first-network* **map** *virtual-address second-network real-address*

To establish an address translation for selected nodes, use the **decnet map** global configuration command.

first-network	DECnet network numbers in the range 0 through 3.
virtual-address	Numeric DECnet address (10.5, for example).
second-network	DECnet network number you map to; DECnet numbers range from 0 through 3.
real-address	Numeric DECnet address (10.5, for example).

decnet [*network-number*] **max-address** *value*

To configure the router with a maximum number of node addresses, use the **decnet max-address** global configuration command.

network-number	(Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.
value	A number less than or equal to 1023 that represents the maximum node address possible on the network. In general, all routers on the network should use the same value for this argument. The default is 1023.

decnet [*network-number*] **max-area** *area-number*

To set the largest number of areas that the router can handle in its routing table, use the **decnet max-area** global configuration command.

network-number	(Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.
area-number	Area number from 1 through 63. Like the **decnet max-address** global configuration command value, this argument controls the sizes of internal routing tables and of messages sent to other nodes. All routers on the network should use the same maximum address value. The default is 63.

decnet [*network-number*] **max-cost** *cost*

To set the maximum cost specification for *intra-area* routing, use the **decnet max-cost** global configuration command.

network-number	(Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.
cost	Cost from 1 through 1022. The default is 1022.

decnet [*network-number*] **max-hops** *hop-count*

To set the maximum hop count specification value for *intra-area* routing, use the **decnet max-hops** global configuration command.

network-number (Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.

hop-count Hop count from 1 through 30. The router ignores routes that have a hop count greater than the corresponding value of this parameter. The default is 30 hops.

decnet [*network-number*] **max-paths** *value*

To define the maximum number of equal-cost paths to a destination that the router will keep in its routing table, use the **decnet max-paths** global configuration command.

network-number (Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.

value Decimal number equal to the maximum number of equal-cost paths the router will save. The valid range is from 1 through 31. The default is 1.

decnet [*network-number*] **max-visits** *value*

To set the limit on the number of times a packet can pass through a router, use the **decnet max-visits** global configuration command.

network-number	(Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.
value	Number of times a packet can pass through a router. It can be a decimal number in the range 1 through 63. If a packet exceeds *value*, the router discards the packet. Digital recommends that the value of the **max-visits** parameter be at least twice that of the **max-hops** parameter, to allow packets to still reach their destinations when routes are changing. The default is 63 times.

[**no**] **decnet multicast-map** *multicast-address-type functional-address*

Use the **decnet multicast-map** interface configuration command to specify a mapping between DECnet multicast addresses and Token Ring functional addresses, other than the default mapping. The **no** form of this command deletes the specified information.

multicast-address-type	Type of multicast address that is used. The following are valid values: • **iv-all-routers** All Phase-IV routers • **iv-all-endnodes** All Phase-IV endnodes • **iv-prime-all-routers** All Phase IV Prime routers

functional-address Functional MAC address that this multicast ID will map to. In the form of “c000.xxxx.yyyy.” See the table “Default Mapping of DECnet Multicast Address Types and Token Ring Functional Addresses” of the *Router Products Command Reference* publication for the default mapping.

decnet [*network-number*] **node-type** {**area** | **routing-iv**}

To specify the node type, use the **decnet node-type** global configuration command.

network-number (Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.

area Router participates in the DECnet routing protocol with other area routers, as described in the Digital documentation, and routes packets from and to routers in other areas. This is sometimes referred to as Level 2, or interarea, routing. An area router does not just handle interarea routing; it also acts as an intra-area or Level 1 router in its own area.

routing-iv Router acts as an intra-area (standard DECnet Phase IV, Level 1 router) and ignores Level 2 routing packets. In this mode, it routes packets destined for other areas to a designated interarea router, exchanging packets with other end-nodes and routers in the same area.

decnet out-routing-filter *access-list-number*
no decnet out-routing-filter

To provide access control to routing information being sent out on an interface, use the **decnet out-routing-filter** interface configuration command. Use the **no** form of this command to remove access control.

access-list-number	Standard DECnet access list applying to destination addresses. The value can be in the range 300 through 399.

decnet path-split-mode {**normal** \| **interim**}

To specify how the router will split the routable packets between equal-cost paths, use the **decnet path-split-mode** global configuration command with the appropriate keyword.

normal	Normal mode, where equal-cost paths are selected on a round-robin basis. This is the default.
interim	Traffic for any particular (higher-layer) session is always routed over the same path. This mode supports older implementations of DECnet (VMS Versions 4.5 and earlier) that do not support out-of-order packet caching. Other sessions may take another path, thus using equal-cost paths that a router may have for a particular destination.

[**no**] **decnet route propagate static**

Use this form of the **decnet propagate static** global configuration command to enable static route propagation. The **no** form of this command disables propagation.

decnet route *decnet-address next-hop-type number* [*snpa-address*]
[*hops* [*cost*]]
no decnet route *decnet-address next-hop-type number*

Use this form of the decnet route global configuration command to create an interface static route. The **no** form of this command removes this route.

decnet-address	DECnet address. This value is entered into a static routing table and used to match a destination DECnet address. Use a node address value of 0 to specify an area static route.
next-hop-type	Interface type.
number	Interface unit number.
snpa-address	(Optional) Optional for serial links; required for multiaccess networks.
hops	(Optional) Hop count to be associated with the route being advertised. Default is 0.
cost	(Optional) Cost to be associated with the route being advertised. Default is 0.

decnet route *decnet-address next-hop-address* [*hops* [*cost*]]
no decnet route *decnet-address next-hop-address*

Use this form of the **decnet route** global configuration command to enter a specific static route. DECnet addresses that match are forwarded to the *next-hop-address*. The **no** form of this command removes this route.

decnet-address	DECnet address. This value is entered into a static routing table and used to match a destination DECnet address. Use a node address value of 0 to specify an area static route.

next-hop-address This value is used to establish the next hop of the route for forwarding packets.

hops (Optional) Hop count to be associated with the route being advertised. Default is 0.

cost (Optional) Cost to be associated with the route being advertised. Default is 0.

decnet route default next-hop-address [*hops* [*cost*]]
no decnet route default *next-hop-address*

Use this form of the **decnet route default** global configuration command to enter a specific default route. The **no** form of this command removes this route.

next-hop-address This value is used to establish the next hop of the route for forwarding packets.

hops (Optional) Hop count to be associated with the route being advertised. Default is 0.

cost (Optional) Cost to be associated with the route being advertised. Default is 0.

next-hop-address This value is used to establish the next hop of the route for forwarding packets.

[**no**] **decnet route-cache**

To enable fast-switching, use the **decnet route-cache** interface configuration command. To disable fast switching, use the **no** form of this command.

decnet router-priority *value*

To elect a designated router to which packets will be sent when no destination is specified, use the **decnet router-priority** interface configuration command.

value	Priority of the router. This can be a number in the range 0 through 127. The larger the number the higher the priority. The default priority is 64.

decnet [*network-number*] **routing** [**iv-prime**] *decnet-address*
no decnet routing

To enable DECnet routing, use the **decnet routing** global configuration command. To disable DECnet routing, use the **no** form of this command.

network-number	(Optional) Network number in the range 0 through 3. Specified when using Address Translation Gateway (ATG). If not specified, the default is network 0.
iv-prime	(Optional) Enables DECnet Phase IV Prime routing.
decnet-address	Address in DECnet format X.Y, where X is the area number and Y is the node number.

decnet routing-timer *seconds*
no decnet routing-timer

To specify how often the router sends routing updates that list the hosts that the router can reach, use the **decnet routing-timer** interface configuration command. Use the **no** form of this command to disable the routing update timer.

seconds	Time, in seconds, from 1 through 65535. The default is 40 seconds.

lat host-delay *number*
no host-delay

To set the delayed acknowledgment for incoming LAT slave connections, use the **lat host-delay** global configuration command. To restore the default, use the **no** form of this command.

number	The delay in milliseconds.

[**no**] **lat service** *service-name* **autocommand** *command*

To associate a command with a service, use the **lat service autocommand** global configuration command. To remove the specified autocommand, use the **no** form of this command.

service-name	Name of the service.
command	Command to be associated with the service.

ping

Use the DECnet **ping** privileged EXEC command to send DECnet echo packets to test the reachability of a remote host over a DECnet network.

ping decnet {*host* | *address*}

Use the **ping decnet** user EXEC command to send DECnet echo packets to test the reachability of a remote host over a DECnet network.

host	DECnet host of system to ping.
address	DECnet address of system to ping.

show decnet

Use the **show decnet** privileged EXEC command to display the global DECnet parameters.

show decnet interface [*type number*]

Use the **show decnet interface** EXEC command to display the global DECnet status and configuration for all interfaces, or the status and configuration for a specified interface.

type	(Optional) Interface type.
number	(Optional) Interface unit number.

show decnet map

Use the **show decnet map** EXEC command to display the address mapping information used by the DECnet Address Translation Gateway.

show decnet neighbors

Use the **show decnet neighbors** privileged EXEC command to display all Phase IV and Phase IV Prime adjacencies and the MAC address associated with each neighbor.

show decnet route [*decnet-address*]

Use the **show decnet route** EXEC command to display the DECnet routing table.

decnet-address	(Optional) DECnet address and, when specified, the first hop route to that address is displayed.

show decnet traffic

The **show decnet traffic** EXEC command shows the DECnet traffic statistics, including datagrams sent, received, and forwarded.

IP Commands

This chapter describes the function and displays the syntax of IP commands. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **access-class** *access-list-number* {**in** | **out**}

To restrict incoming and outgoing connections between a particular virtual terminal line (into a Cisco device) and the addresses in an access list, use the **access-class** line configuration command. To remove access restrictions, use the **no** form of this command.

access-list-number	Number of an access list. This is a decimal number from 1 through 99.
in	Restricts incoming connections between a particular Cisco device and the addresses in the access list.
out	Restricts outgoing connections between a particular Cisco device and the addresses in the access list.

access-list *access-list-number* {**deny** | **permit**} *source*
[*source-wildcard*]
no access-list *access-list-number*

To define a standard IP access list, use the standard version of the **access-list** global configuration command. To remove a standard access lists, use the **no** form of this command.

access-list-number — Number of an access list. This is a decimal number from 1 through 99.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

source — Number of the network or host from which the packet is being sent. There are two alternative ways to specify the source:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

source-wildcard — (Optional) Wildcard bits to be applied to the *source*. There are two alternative ways to specify the source wildcard:

- Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.

access-list *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*]
no access-list *access-list-number*

access-list *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*]

For ICMP, you can also use the syntax shown above.

access-list *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*]

For IGMP, you can also use the syntax shown above.

access-list *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*]

For TCP, you can also use the the syntax shown above.

access-list *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos*]

For UDP, you can also use the syntax shown above.

To define an extended IP access list, use the extended version of the **access-list** global configuration command. To remove the access lists, use the **no** form of this command.

access-list-number Number of an access list. This is a decimal number from 100 through 199.

deny Denies access if the conditions are matched.

permit

Permits access if the conditions are matched.

protocol

Name or number of an IP protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 through 255 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword **ip**. Some protocols allow further qualifiers described below.

source

Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

source-wildcard

Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard:

- Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore.
- Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.

destination

Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination:

- Use a 32-bit quantity in four-part dotted-decimal format.
- Use the keyword **any** as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

destination-wildcard

Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard:

- Use a 32-bit quantity in four-part dotted-decimal format. Place ones in the bit positions you want to ignore.
- Use the keyword **any** as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255.
- Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

precedence *precedence*

(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by name as listed in the “Precedence Names” table in the *Router Products Command Reference* publication.

tos

(Optional) Packets can be filtered by type of service level, as specified by a number from 0 to 15 or by name as listed in the “Type of Service Names” table in the *Router Products Command Reference* publication.

icmp-type — (Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.

icmp-code — (Optional) ICMP packets which are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.

icmp-message — (Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the “ICMP Message Type Names” table in the *Router Products Command Reference* publication.

igmp-type — (Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the “IGMP Message Names” table in the *Router Products Command Reference* publication.

operator — (Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range).

If the operator is positioned after the *source* and *source-wildcard*, it must match the source port.

If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port.

The **range** operator requires two port numbers. All other operators require one port number.

port

(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names are listed in the “TCP Port Names” table in the *Router Products Command Reference* publication. TCP port names can only be used when filtering TCP.

UDP port names are listed in the section “UDP Port Names” table in the *Router Products Command Reference* publication. UDP port names can only be used when filtering UDP.

established

(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

[**no**] **arp** *ip-address hardware-address type* [**alias**]

To add a permanent entry in the ARP cache, use the **arp** global configuration command. To remove an entry from the ARP cache, use the **no** form of this command.

ip-address	IP address in four-part dotted-decimal format corresponding to the local data link address.
hardware-address	Local data link address (a 48-bit address).
type	Encapsulation description. For Ethernet interfaces, this is typically the **arpa** keyword. For FDDI and Token Ring interfaces, this is always **snap**.
alias	(Optional) Indicates that the router should respond to ARP requests as if it were the owner of the specified address.

[**no**] **arp** {**arpa** | **probe** | **snap**}

To control the interface-specific handling of IP address resolution into 48-bit Ethernet, FDDI, and Token Ring hardware addresses, use the **arp** interface configuration command. To disable an encapsulation type, use the **no** form of this command.

arpa	Standard Ethernet-style ARP (RFC 826); the default.
probe	HP Probe protocol for IEEE-802.3 networks.
snap	ARP packets conforming to RFC 1042.

[**no**] **arp timeout** *seconds*

To configure how long an entry remains in the ARP cache, use the **arp timeout** interface configuration command. To restore the default value, use the **no** form of this command.

seconds	Time, in seconds, that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache.

clear arp-cache

To delete all dynamic entries from the ARP cache, to clear the fast-switching cache, and to clear the IP route cache, use the **clear arp-cache** EXEC command.

clear host {*name* | *****}

To delete entries from the host-name-and-address cache, use the **clear host** EXEC command.

name	Particular host entry to remove.
*****	Removes all entries.

clear ip accounting [**checkpoint**]

To clear the active or checkpointed database when IP accounting is enabled, use the **clear ip accounting** EXEC command.

checkpoint	(Optional) Clears the checkpointed database.

clear ip nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ip nhrp** EXEC command.

clear ip route {*network* [*mask*] | *****}

To delete entries from the IP routing table, use the **clear ip route** EXEC command.

network	Network or subnet address to remove.
mask	(Optional) Subnet mask to remove.
*****	Removes all routing table entries.

clear ip sse

To have the route processor recompute the SSE program for IP on the Cisco 7000 series, use the **clear ip sse** EXEC command.

clear sse

To reinitialize the route processor on the Cisco 7000 series, use the **clear sse** EXEC command.

[**no**] **dnsix-dmdp retries** *count*

To set the retransmit count used by the DNSIX Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** global configuration command. To restore the default number of retries, use the **no** form of this command.

count	Number of times DMDP will retransmit a message. It can be a decimal integer from 0 through 200. The default is 4 retries, or until acknowledged.

[**no**] **dnsix-nat authorized-redirection** *ip-address*

To specify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** global configuration command. To delete an address, use the **no** form of this command.

ip-address IP address of the host from which redirection requests are permitted.

[**no**] **dnsix-nat primary** *ip-address*

To specify the IP address of the host to which DNSIX audit messages are sent, use the **dnsix-nat primary** global configuration command. To delete an entry, use the **no** form of this command.

ip-address IP address for the primary collection center.

[**no**] **dnsix-nat secondary** *ip-address*

To specify an alternate IP address for the host to which DNSIX audit messages are sent, use the **dnsix-nat secondary** global configuration command. To delete an entry, use the **no** form of this command.

ip-address IP address for the secondary collection center.

[**no**] **dnsix-nat source** *ip-address*

To start the audit-writing module and to define audit trail source address, use the **dnsix-nat source** global configuration command. To disable the DNSIX audit trail writing module, use the **no** form of this command.

ip-address Source IP address for DNSIX audit messages.

[**no**] **dnsix-nat transmit-count** *count*

To have the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** global configuration command. To revert to the default audit message count, use the **no** form of this command.

count	Number of audit messages to buffer before transmitting to the server. Integer from 1 through 200. The default is 1.

[**no**] **ip access-group** *access-list-number* {**in** \| **out**}

To control access to an interface, use the **ip access-group** interface configuration command. To remove the specified access group, use the **no** form of this command. If a keyword is not specified, **out** is the default.

access-list-number	Number of an access lists. This is a decimal number from 1 through 199.
in	Filters on inbound packets.
out	Filters on outbound packets.

[**no**] **ip accounting** [**access-violations**]

To enable IP accounting on an interface, use the **ip accounting** interface configuration command. To disable IP accounting, use the **no** form of this command.

access-violations	(Optional) Enables IP accounting with the ability to identify IP traffic that fails IP access lists.

[**no**] **ip accounting-list** *ip-address mask*

To define filters to control the hosts for which IP accounting information is kept, use the **ip accounting-list** global configuration command. To remove a filter definition, use the **no** form of this command.

ip-address IP address in dotted-decimal format.

mask IP mask.

[**no**] **ip accounting-threshold** *threshold*

To set the maximum number of accounting entries to be created, use the **ip accounting-threshold** global configuration command. To restore the default number of entries, use the **no** form of this command.

threshold Maximum number of entries (source and destination address pairs) that the router accumulates. The default is 512 entries.

ip accounting-transits *count*
no ip accounting-transits

To control the number of transit records that are stored in the IP accounting database, use the **ip accounting-transits** global configuration command. To return to the default number of records, use the **no** form of this command.

count Number of transit records to store in the IP accounting database. The default is 0.

[**no**] **ip address** *ip-address mask*

To set an IP address for an interface, use the **ip address** interface configuration command. To remove an IP address, use the **no** form of this command.

ip-address IP address.

mask Mask for the associated IP subnet.

[**no**] **ip address** *ip-address mask* **secondary**

To set multiple IP addresses for an interface, use the **ip address secondary** interface configuration command. To remove an address, use the **no** form of this command.

ip-address	IP address.
mask	Mask for the associated IP subnet.

[**no**] **ip broadcast-address** [*ip-address*]

To define a broadcast address for an interface, use the **ip broadcast-address** interface configuration command. To restored the default IP broadcast address, use the **no** form of this command.

ip-address	(Optional) IP broadcast address for a network. The default address is 255.255.255.255 (all ones).

ip cache-invalidate-delay [*minimum maximum quiet threshold*]
no ip cache-invalidate-delay

To control the invalidation rate of the IP route cache, use the **ip cache-invalidate-delay** global configuration command. To allow the IP route cache to be immediately invalidated, use the **no** form of this command.

minimum	(Optional) Minimum time, in seconds, between invalidation request and actual invalidation. The default is 2 seconds.
maximum	(Optional) Maximum time, in seconds, between invalidation request and actual invalidation. The default is 5 seconds.
quiet	(Optional) Length of quiet period, in seconds, before invalidation.
threshold	(Optional) Maximum number of invalidation requests considered to be quiet.

[**no**] **ip classless**

At times the router might receive packets destined for a subnet of a network that has no network default route. To have the router forward such packets to the best supernet route possible, use the **ip classless** global configuration command. To disable this feature, use the **no** form of this command.

[**no**] **ip default-gateway** *ip-address*

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** global configuration command. To disable this function, use the **no** form of this command.

ip-address	IP address of the router.

[**no**] **ip directed-broadcast** [*access-list-number*]

To enable the translation of directed broadcast to physical broadcasts, use the **ip directed-broadcast** interface configuration command. To disable this function, use the **no** form of this command.

access-list-number	(Optional) Number of the access list. If specified, a broadcast must pass the access list to be forwarded. If not specified, all broadcasts are forwarded.

[**no**] **ip domain-list** *name*

To define a list of default domain names to complete unqualified host names, use the **ip domain-list** global configuration command. To delete a name from a list, use the **no** form of this command.

name	Domain name. Do not include the initial period that separates an unqualified name from the domain name.

[**no**] **ip domain-lookup**

To enable the IP Domain Name System-based host name-to-address translation, use the **ip domain-lookup** global configuration command. To disable the Domain Name System, use the **no** form of this command.

[**no**] **ip domain-lookup nsap**

To allow Domain Name System (DNS) queries for CLNS addresses, use the **ip domain-lookup nsap** global configuration command. To disable this feature, use the **no** form of this command.

ip domain-name *name*
no ip domain-name

To define a default domain name that the router uses to complete unqualified host names (names without a dotted-decimal domain name), use the **ip domain-name** global configuration command. To disable use of the Domain Name System, use the **no** form of this command.

name	Default domain name used to complete unqualified host names.Do not include the initial period that separates an unqualified name from the domain name.

[**no**] **ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}

To specify which protocols and ports the router forwards when forwarding broadcast packets, use the **ip forward-protocol** global configuration command. To remove a protocol or port, use the **no** form of this command.

udp	Forward User Datagram Protocol (UDP) datagrams. See the "Default" section in the *Router Products Command Reference* publication for a list of port numbers forwarded by default.
port	(Optional) Destination port that controls which UDP services are forwarded.
nd	Forward Network Disk (ND) datagrams. This protocol is used by older diskless SUN workstations.
sdns	Secure Data Network Service.

[**no**] **ip forward-protocol any-local-broadcast**

To forward any broadcasts including local subnet broadcasts, use the **ip forward-protocol any-local-broadcast** global configuration command. To disable this type of forwarding, use the **no** form of this command.

[**no**] **ip forward-protocol spanning-tree**

To permit IP broadcasts to be flooded throughout the internetwork in a controlled fashion, use the **ip forward-protocol spanning-tree** global configuration command. To disable the flooding of IP broadcasts, use the **no** form of this command.

[**no**] **ip forward-protocol turbo-flood**

To speed up flooding of User Datagram Protocol (UDP) datagrams using the spanning-tree algorithm, use the **ip forward-protocol turbo-flood** global configuration command. To disable this feature, use the **no** form of this command.

[**no**] **ip gdp gdp**

To configure the router discovery feature using the Cisco Gateway Discovery Protocol (GDP) routing protocol, use the **ip gdp gdp** interface configuration command. To disable this feature, use the **no** form of this command.

[**no**] **ip gdp igrp**

To configure the router discovery feature using the Cisco Interior Gateway Routing Protocol (IGRP), use the **ip gdp igrp** interface configuration command. To disable this feature, use the **no** form of this command.

[**no**] **ip gdp irdp**

To configure the router discovery feature using the ICMP Router Discovery Protocol (IRDP), use the **ip gdp irdp** interface configuration command. To disable this feature, use the **no** form of this command.

[**no**] **ip gdp rip**

To configure the router discovery feature using the Routing Information Protocol (RIP), use the **ip gdp rip** interface configuration command. To disable this feature, use the **no** form of this command.

[**no**] **ip helper-address** *address*

To have the router forward User Datagram Protocol (UDP) broadcasts, including BOOTP, received on an interface, use the **ip helper-address** interface configuration command. To disable the forwarding of broadcast packets to specific addresses, use the **no** form of this command.

address	Destination broadcast or host address to be used when forwarding UDP broadcasts. You can have more than one helper address per interface.

ip host *name* [*tcp-port-number*] *address1* [*address2*[...[*address8*]]]
no ip host *name address*

To define a static host name-to-address mapping in the host cache, use the **ip host** global configuration command. To remove the name-to-address mapping, use the **no** form of this command.

name	Name of the host. The first character can be either a letter or a number, but if you use a number, the operations you can perform are limited.
tcp-port-number	(Optional) TCP port number to connect to when using the defined host name in conjunction with an EXEC connect or telnet command. The default is Telnet (port 23).
address	Associated IP address. You can bind up to eight addresses to a host name.

[**no**] **ip hp-host** *hostname ip-address*

To enter into the host table the host name of an HP host to be used for HP Probe Proxy service, use the **ip hp-host** global configuration command. To remove a host name, use the **no** form of this command.

hostname	Name of the host.
ip-address	IP address of the host.

[**no**] **ip mask-reply**

To have the router to respond to Internet Control Message Protocol (ICMP) mask requests by sending ICMP Mask Reply messages, use the **ip mask-reply** interface configuration command. To disable this function, use the **no** form of this command.

[**no**] **ip mobile arp** [**timers** *keepalive hold-time*] [**access-group** *access-list-number*]

To enable local-area mobility, use the **ip mobile arp** interface configuration command. To disable local-area mobility, use the **no** form of this command.

timers	(Optional) Indicates that you are setting local-area mobility timers.
keepalive	(Optional) Frequency, in seconds, at which the router sends unicast ARP messages to a relocated host to verify that the host is present and has not moved. The default keepalive time is 300 seconds (5 minutes).
hold-time	(Optional) Hold time, in seconds. This is the length of time the router considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default hold time is 900 seconds (15 minutes).
access-group	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
access-list-number	(Optional) Number of a standard IP access list. It is a decimal number from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.

ip mtu *bytes*
no ip mtu

To set the maximum transmission unit (MTU) size of IP packets sent on an interface, use the **ip mtu** interface configuration command. To restore the default MTU size, use the **no** form of this command.

bytes	MTU in bytes. The minimum is 128 bytes; the maximum depends on the interface medium.

[**no**] **ip name-server** *server-address1* [*server-address2*
[...[*server-address6*]]]

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** global configuration command. To remove the addresses specified, use the **no** form of this command.

server-address1[... [*server-address6*]]	IP addresses of up to six name servers.

ip netmask-format {**bitcount** | **decimal** | **hexadecimal**}
no ip netmask-format [**bitcount** | **decimal** | **hexadecimal**]

To specify the format in which netmasks are displayed in **show** command output, use the **ip netmask-format** line configuration command. To restore the default display format, use the **no** form of this command.

bitcount	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates that the netmask is 24 bits.
decimal	Network masks are displayed in dotted decimal notation (for example, 255.255.255.0). The default is dotted decimal notation.
hexadecimal	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0XFFFFFF00).

ip nhrp authentication *string*
no ip nhrp authentication [*string*]

To configure the authentication string for an interface using Next Hop Resolution Protocol (NHRP), use the **ip nhrp authentication** interface configuration command. To remove the authentication string, use the **no** form of this command.

string	Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to 8 characters long.

ip nhrp holdtime *seconds-positive* [*seconds-negative*]
no ip nhrp holdtime [*seconds-positive* [*seconds-negative*]]

To change the number of seconds that NHRP nonbroadcast, multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the **ip nhrp holdtime** interface configuration command. To restore the default value, use the **no** form of this command.

seconds-positive	Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses. The default is 7200 seconds (2 hours).
seconds-negative	(Optional) Time in seconds that NBMA addresses are advertised as valid in negative authoritative NHRP responses. The default is 7200 seconds (2 hours).

ip nhrp interest *access-list-number*
no ip nhrp interest [*access-list-number*]

To control which IP packets can trigger sending a Next Hop Resolution Protocol (NHRP) Request, use the **ip nhrp interest** interface configuration command. To restore the default value, use the **no** form of this command.

access-list-number	Standard or extended IP access list number in the range 1 through 199.

ip nhrp map *ip-address nbma-address*
no ip nhrp map *ip-address nbma-address*

To statically configure the IP-to-NBMA address mapping of IP destinations connected to a nonbroadcast, multiaccess (NBMA) network, use the **ip nhrp map** interface configuration command. To remove the static entry from NHRP cache, use the **no** form of this command.

ip-address	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
nbma-address	Nonbroadcast, multiaccess (NBMA) address which is directly reachable through the NBMA network. The address format varies depending on the medium you are using. For example, ATM has an NSAP address, Ethernet has a MAC address, and SMDS has an E.164 address. This address is mapped to the IP address.

[**no**] **ip nhrp map multicast** *nbma-address*

To configure NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast** interface configuration command. To remove the destinations, use the **no** form of this command.

nbma-address	Nonbroadcast, multiaccess (NBMA) address which is directly reachable through the NBMA network. The address format varies depending on the medium you are using.

ip nhrp network-id *number*
no ip nhrp network-id [*number*]

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id** interface configuration command. To disable NHRP on the interface, use the **no** form of this command.

number	Globally unique, 32-bit network identifier for a nonbroadcast, multiaccess (NBMA) network. The range is 1 to 4294967295.

[**no**] **ip nhrp nhs** *nhs-address* [*net-address* [*netmask*]]

To specify the address of one or more NHRP Next Hop Servers, use the **ip nhrp nhs** interface configuration command. To remove the address, use the **no** form of this command.

nhs-address	Address of the Next Hop Server being specified.
net-address	(Optional) IP address of a network served by the Next Hop Server.
netmask	(Optional) IP network mask to be associated with the *net* IP address. The *net* IP address is logically ANDed with the mask.

[**no**] **ip nhrp record**

To re-enable the use of forward record and reverse record options in NHRP Request and Reply packets, use the **ip nhrp record** interface configuration command. To suppress the use of such options, use the **no** form of this command.

ip nhrp responder *type number*
no ip nhrp responder [*type*] [*number*]

To designate which interface's primary IP address the Next Hop Server will use in NHRP Reply packets when the NHRP requestor uses the Responder Address option, use the **ip nhrp responder** interface configuration command. To remove the designation, use the **no** form of this command.

type	Interface type whose primary IP address is used when a Next Hop Server complies with a Responder Address option (for example, **serial**, **tunnel**).
number	Interface number whose primary IP address is used when a Next Hop Server complies with a Responder Address option.

[**no**] **ip probe proxy**

To enable the HP Probe Proxy support, which allows a router to respond to HP Probe Proxy Name requests, use the **ip probe proxy** interface configuration command. To disable HP Prove Proxy, use the **no** form of this command.

[**no**] **ip proxy-arp**

To enable proxy ARP on an interface, use the **ip proxy-arp** interface configuration command. To disable proxy ARP on the interface, use the **no** form of this command.

[**no**] **ip redirects**

To enable the sending of redirect messages if the router is forced to resend a packet through the same interface on which it was received, use the **ip redirects** interface configuration command. To disable the sending of redirect messages, use the **no** form of this command.

[**no**] **ip route-cache** [**cbus**]
[**no**] **ip route-cache same-interface**
[**no**] **ip route-cache sse**

To control the use of a high-speed switching cache for IP routing as well as the use of autonomous switching, use the **ip route-cache** interface configuration command. To disable fast switching and autonomous switching, use the **no** form of this command.

cbus	(Optional) Enables both autonomous switching and fast switching. By default, autonomous switching is disabled. By default, fast switching may be enabled or disabled, depending on the interface and medium.
same-interface	Enables fast switching packets back out the interface on which they arrived. By default, fast switching may be enabled or disabled, depending on the interface and medium.
sse	Enables SSE fast switching on the SSP board on the Cisco 7000 series. By default, SSE switching is disabled.

[**no**] **ip routing**

To enable IP routing on the router, use the **ip routing** global configuration command. To disable IP routing on the router, use the **no** form of this command.

[**no**] **ip security add**

To add a basic security option to all outgoing packets, use the **ip security add** interface configuration command. To disable the adding of a basic security option to all outgoing packets, use the **no** form of this command.

[**no**] **ip security aeso** *source compartment-bits*

To attach Auxiliary Extended Security Options (AESOs) to an interface, use the **ip security aeso** command. To disable AESO on an interface, use the **no** form of this command.

source	Extended Security Option (ESO) source. This can be an integer from 0 through 255.
compartment-bits	Compartment bits in hexadecimal.

[**no**] **ip security dedicated** *level authority* [*authority...*]

To set the level of classification and authority on the interface, use the **ip security dedicated** interface configuration command. To reset the interface to the default classification and authorities, use the **no** form of this command.

level	Degree of sensitivity of information. The level keywords are listed in the IPSO level keywords table in the *Router Products Command Reference* publication.
authority	Organization that defines the set of security levels that will be used in a network. The authority keywords are listed in IPSO authority keywords table in the *Router Products Command Reference* publication.

[**no**] **ip security eso-info** *source compartment-size default-bit*

To configure system-wide defaults for extended IP Security Option (IPSO) information, use the **ip security eso-info** global configuration command. To return to the default settings, use the **no** form of this command.

source	Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 through 255.
compartment-size	Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 through 16.
default-bit	Default bit value for any unsent compartment bits.

[**no**] **ip security eso-max** *source compartment-bits*

To specify the maximum sensitivity level for an interface, use the **ip security eso-max** interface configuration command. To return to the default, use the **no** form of this command.

source	Extended Security Option (ESO) source. An integer from 1 through 255.
compartment-bits	Compartment bits in hexadecimal.

[**no**] **ip security eso-min** *source compartment-bits*

To configure the minimum sensitivity for an interface, use the **ip security eso-min** interface configuration command. To return to the default, use the **no** form of this command.

source	Extended Security Option (ESO) source. An integer from 1 through 255.
compartment-bits	Compartment bits in hexadecimal.

[**no**] **ip security extended-allowed**

To accept packets on an interface that has an extended security option present, use the **ip security extended-allowed** interface configuration command. To restore the default, use the **no** form of this command.

[**no**] **ip security first**

To prioritize the presence of security options on a packet, use the **ip security first** interface configuration command. To disable this function, use the **no** form of this command.

[**no**] **ip security ignore-authorities**

To have the router ignore the authorities field of all incoming packets, use the **ip security ignore-authorities** interface configuration command. To disable this function, use the **no** form of this command.

[**no**] **ip security implicit-labelling** [*level authority* [*authority*...]]

To force the router to accept packets on the interface, even if they do not include a security option, use the **ip security implicit-labelling** interface configuration command. To disable this function, use the **no** form of this command.

level	(Optional) Degree of sensitivity of information. If your interface has multilevel security set, you must specify this argument. The level keywords are listed in the IPSO level keywords table in the *Router Products Command Reference* publication.
authority	(Optional) Organization that defines the set of security levels that will be used in a network. If your interface has multilevel security set, you must specify this argument. You can specify more than one. The authority keywords are listed in IPSO authority keywords table in the *Router Products Command Reference* publication.

ip security multilevel *level1* [*authority1*...] **to** *level2 authority2*
[*authority2*...]
no ip security multilevel

To set the range of classifications and authorities on an interface, use the **ip security multilevel** interface configuration command. To disable this function, use the **no** form of this command.

level1 — Degree of sensitivity of information. The classification level of incoming packets must be equal to or greater than this value for processing to occur. The level keywords are listed in the IPSO level keywords table in the *Router Products Command Reference* publication.

authority1 — (Optional) Organization that defines the set of security levels that will be used in a network. The authority bits must be a superset of this value. The authority keywords are listed in IPSO authority keywords table in the *Router Products Command Reference* publication.

to — Separates the range of classifications and authorities.

level2 — Degree of sensitivity of information. The classification level of incoming packets must be equal to or less than this value for processing to occur. The level keywords are listed in the IPSO level keywords table in the *Router Products Command Reference* publication.

authority2 — Organization that defines the set of security levels that will be used in a network. The authority bits must be a proper subset of this value. The authority keywords are listed in IPSO authority keywords table in the *Router Products Command Reference* publication.

[**no**] **ip security reserved-allowed**

To treat as valid any packets that have Reserved1 through Reserved4 security levels, use the **ip security reserved-allowed** interface configuration command. To disable this feature, use the **no** form of this command.

[**no**] **ip security strip**

To remove any basic security option on outgoing packets on an interface, use the **ip security strip** interface configuration command. To disable this function, use the **no** form of this command.

[**no**] **ip source-route**

To allow the router to handle IP datagrams with source routing header options, use the **ip source-route** global configuration command. To have the router discard any IP datagram containing a source-route option, use the **no** form of this command.

[**no**] **ip subnet-zero**

To enable the use of subnet zero for interface addresses and routing updates, use the **ip subnet-zero** global configuration command. To restore the default, use the **no** form of this command.

[**no**] **ip tcp compression-connections** *number*

To specify the total number of header compression connections that can exist on an interface, use the **ip tcp compression-connections** interface configuration command. To restore the default, use the **no** form of this command.

number	Number of connections the cache supports. It can be a number from 3 through 256.

[**no**] **ip tcp header-compression** [**passive**]

To enable TCP header compression, use the **ip tcp header-compression** interface configuration command. To disable compression, use the **no** form of this command.

passive	(Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, the router compresses all traffic.

ip tcp path-mtu-discovery
no ip tcp path-mtu-discovery

To enable Path MTU Discovery for all new TCP connections from the router, use the **ip tcp path-mtu-discovery** interface configuration command. To disable the feature, use the **no** form of this command.

[**no**] **ip tcp synwait-time** *seconds*

To set a period of time the router waits while attempting to establish a TCP connection before it times out, use the **ip tcp synwait-time** global configuration command. To restore the default time, use the **no** form of this command.

seconds	Time in seconds the router waits while attempting to establish a TCP connection. It can be an integer from 5 to 300 seconds. The default is 30 seconds.

[**no**] **ip unnumbered** *interface-name*

To enable IP processing on a serial interface without assigning an explicit IP address to the interface, use the **ip unnumbered** interface configuration command. To disable the IP processing on the interface, use the **no** form of this command.

interface-name	Name of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.

[**no**] **ip unreachables**

To enable the generation of ICMP Unreachable messages, use the **ip unreachables** interface configuration command. To disable this function, use the **no** form of this command.

ping [*protocol*] {*host* | *address*}

To check host reachability and network connectivity, use the **ping** (IP packet internet groper function) EXEC command.

protocol	(Optional) Protocol keyword. The default is IP.
host	Host name of system to ping.
address	IP address of system to ping.

show access-lists

To display the contents of all current access lists, use the **show access-lists** privileged EXEC command.

show arp

To display the entries in the ARP table for the router, use the show **arp** privileged EXEC command.

show dnsix

To display state information and the current configuration of the DNSIX audit writing module, use the **show dnsix** privileged EXEC command.

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses, use the **show hosts** EXEC command.

show ip access-list [*access-list-number*]

To display the contents of all current IP access lists, use the **show ip access-list** EXEC command.

access-list-number (Optional) Number of the IP access list to display. This is a decimal number from 1 to 199.

show ip accounting [**checkpoint**] [**output-packets** | **access-violations**]

To display the active accounting or checkpointed database, use the **show ip accounting** privileged EXEC command.

checkpoint (Optional) Displays the checkpointed database.

output-packets (Optional) Indicates that information pertaining to packets that passed access control and were successfully routed should be displayed. If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** is the default.

access-violations (Optional) Indicates that information pertaining to packets that failed access lists and were not routed should be displayed. If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** is the default.

show ip aliases

To display the router's IP addresses mapped to TCP ports (aliases) and SLIP addresses, which are treated similarly to aliases, use the **show ip aliases** EXEC command.

show ip arp

To display the Address Resolution Protocol (ARP) cache, where SLIP addresses appear as permanent ARP table entries, use the show **ip arp** EXEC command.

show ip cache [*prefix mask*] [*type number*]

To display the routing table cache used to fast switch IP traffic, use the **show ip cache** EXEC command.

prefix	(Optional) Display only the entries in the cache that match the prefix and mask combination.
mask	(Optional) Display only the entries in the cache that match the prefix and mask combination.
type	(Optional) Display only the entries in the cache that match the interface type and number combination.
number	(Optional) Display only the entries in the cache that match the interface type and number combination.

show ip interface [*type number*]

To display the usability status of interfaces, use the **show ip interface** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.

show ip masks *address*

To display the masks used for network addresses and the number of subnets using each mask, use the **show ip masks** EXEC command.

address	Network address for which a mask is required.

show ip nhrp [**dynamic** | **static**] [*type number*]

To display the Next Hop Resolution Protocol (NHRP) cache, use the **show ip nhrp** EXEC command.

dynamic	(Optional) Displays only the dynamic (learned) IP-to-NBMA address cache entries.
static	(Optional) Displays only the static IP-to-NBMA address entries in the cache (configured through the **ip nhrp map** command).
type	(Optional) Interface type about which to display the NHRP cache (for example, **atm**, **tunnel**).
number	(Optional) Interface number about which to display the NHRP cache.

show ip nhrp traffic

To display Next Hop Resolution Protocol (NHRP) traffic statistics, use the **show ip nhrp traffic** EXEC command.

show ip redirects

To display the address of a default gateway (router) and the address of hosts for which a redirect has been received, use the **show ip redirects** EXEC command.

show ip route [*address* [*mask*] | *protocol*]

To display the entries in the routing table, use the **show ip route** EXEC command.

address	(Optional) Address about which routing information should be displayed.
mask	(Optional) Argument for a subnet mask.
protocol	(Optional) Argument for a particular routing protocol, or **static** or **connected**.

show ip route summary

To display summary information about entries in the routing table, use the **show ip route summary** EXEC command.

show ip tcp header-compression

To display statistics about TCP header compression, use the **show ip tcp header-compression** EXEC command.

show ip traffic

To display statistics about IP traffic, use the **show ip traffic** EXEC command.

show sse summary

To display a summary of Silicon Switch Processor (SSP) statistics, use the **show sse summary** EXEC command.

show standby

To display standby protocol information, use the **show standby** EXEC command.

[**no**] **standby** [*group-number*] **authentication** *string*

To configure an authentication string for the Hot Standby Router Protocol, use the **standby authentication** interface configuration command. To delete an authentication string, use the **no** form of this command.

group-number	(Optional) Group number on the interface to which this authentication string applies. The default number is 0.
string	Authentication string. It can be up to eight characters in length. The default string is **cisco**.

[**no**] **standby** [*group-number*] **ip** [*ip-address*]

To activate the Hot Standby Router Protocol, use the **standby ip** interface configuration command. To disable the Hot Standby Router Protocol, use the **no** form of this command.

group-number	(Optional) Group number on the interface for which the Hot Standby Router Protocol is being activated. The default number is 0.
ip-address	(Optional) IP address of the Hot Standby Router interface.

[**no**] **standby** [*group-number*] **preempt**

To indicate that, when the local router has a Hot Standby priority higher than the current active router, the local router should attempt to assume control as the active router, use the **standby preempt** interface configuration command. To have the local router assume control as the active router only if it receives information indicating that there is no router currently in the active state (acting as the designated router), use the **no** form of this command.

group-number	(Optional) Group number on the interface for which the Hot Standby preemptive feature is being activated. The default number is 0.

[**no**] **standby** [*group-number*] **priority** *priority-number*

To prioritize a potential Hot Standby router, use the **standby priority** interface configuration command. To restore the priority to the default, use the **no** form of this command.

group-number	(Optional) Group number on the interface to which the priority number applies. The default number is 0.
priority-number	Priority value. It is an integer from 0 through 255. The default is 100.

[**no**] **standby** [*group-number*] **timers** *hellotime holdtime*

To configure the time between hellos and the time before other routers declare the active Hot Standby or standby router to be down, use the **standby timers** interface configuration command. To restore the timers to their default values, use the **no** form of this command.

group-number	(Optional) Group number on the interface to which the timers apply. The default is 0.
hellotime	Hello interval in seconds. This is an integer from 1 through 255. The default is 1 second.
holdtime	Time in seconds before the active or standby router is declared to be down. This is an integer from 1 through 255. The default is 3 seconds.

[**no**] **standby** [*group-number*] **track** *type number* [*interface-priority*]

To configure an interface so that the router's Hot Standby priority changes based on the availability of other interfaces, use the **standby track** interface configuration command. To remove the tracking, use the **no** form of this command.

group-number	(Optional) Group number on the interface to which the tracking applies. The default number is 0.
type	Interface type (combined with interface number) that will be tracked.
number	Interface number (combined with interface type) that will be tracked.
interface-priority	(Optional) Amount by which the Hot Standby priority for the router is decremented (or incremented) when the interface goes down (or comes back up). The default value is 10.

term ip netmask-format {**bitcount** | **decimal** | **hexadecimal**}
term no ip netmask-format [**bitcount** | **decimal** | **hexadecimal**]

To specify the format in which netmasks are displayed in **show** command output, use the **term ip netmask-format** EXEC command. To restore the default display format, use the **no** form of this command.

bitcount Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.55/24 indicates that the netmask is 24 bits.

decimal Netmasks are displayed in dotted decimal notation (for example, 255.255.255.0).

hexadecimal Netmasks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0XFFFFFF00).

trace ip *destination*

To discover the routes the router's packets follow when traveling to their destination, use the **trace** user EXEC command.

destination (Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

trace [*destination*]

To discover the routes the router's packets follow when traveling to their destination, use the **trace** privileged EXEC command.

destination (Optional) Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

transmit-interface *interface-name*
no transmit-interface

To assign a transmit interface to a receive-only interface, use the **transmit-interface** interface configuration command. To return to normal duplex Ethernet interfaces, use the **no** form of this command.

interface-name	Transmit interface to be linked with the (current) receive-only interface

tunnel mode {**aurp** | **cayman** | **dvmrp** | **eon** | **gre ip** [**multipoint**] | **nos**}
no tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** interface configuration command. To set to the default, use the **no** form of this command.

aurp	AppleTalk Update Routing Protocol (AURP).
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible CLNS tunnel.
gre ip	Generic route encapsulation (GRE) protocol over IP.
multipoint	(Optional) Enables a GRE tunnel to be used in a multipoint fashion. Can be used with the **gre ip** keyword only, and requires the use of the **tunnel key** command.
nos	KA9Q/NOS compatible IP over IP.

IP Routing Protocols Commands

This chapter describes the function and displays the syntax of each IP routing command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **aggregate-address** *address mask* [**as-set**] [**summary-only**] [**suppress-map** *map-name*]

To create an aggregate entry in a BGP routing table, use the **aggregate-address** router configuration command. To disable this feature, use the **no** form of this command.

address	Aggregate address.
mask	Aggregate mask.
as-set	(Optional) Generate AS set path information.
summary-only	(Optional) Filter more specific routes from updates.
suppress-map *map-name*	(Optional) Name of route-map to suppress.

[**no**] **area** *area-id* **authentication**
no area *area-id*

To enable authentication for an OSPF area, use the **area authentication** router configuration command. To remove an area's authentication specification or a specified area from the router's configuration, use the **no** form of this command.

area-id	Identifier of the area for which authentication is to be enabled. The identifier can be specified as either a decimal value or an IP address.

[**no**] **area** *area-id* **default-cost** *cost*

To specify a cost for the default summary route sent into a stub area, use the **area default-cost** router configuration command. To remove the assigned default route cost, use the **no** form of this command.

area-id Identifier for the stub area. The identifier can be specified as either a decimal value or as an IP address.

cost Cost for the default summary route used for a stub area. The acceptable value is a 24-bit number. The default cost is 1.

[**no**] **area** *area-id* **range** *address mask*

To consolidate and summarize routes at an area boundary, use the **area range** router configuration command. To disable this function, use the **no** form of this command.

area-id Identifier of the area about which routes are to be summarized. It can be specified as either a decimal value or as an IP address.

address IP address.

mask IP mask.

[**no**] **area** *area-id* **stub**

To define an area as a stub area, use the **area stub** router configuration command. To disable this function, use the **no** form of this command.

area-id Identifier for the stub area. The identifier can be either a decimal value or an IP address.

[**no**] **area** *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*]
[**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]
[**dead-interval** *seconds*] [**authentication-key** *password*]

To define an OSPF virtual link, use the **area virtual-link** router configuration command with the optional parameters. To remove a virtual link, use the **no** form of this command.

area-id — Area ID assigned to the transit area for the virtual link. This can be either a decimal value or a valid IP address. There is no default.

router-id — Router ID associated with the virtual link neighbor. The router ID appears in the **show ip ospf** display. It is internally derived by each router from the router's interface IP addresses. This value must be entered in the format of an IP address. There is no default.

hello-interval — (Optional) Number of seconds between the hello packets that the router sends on an interface.

seconds — (Optional) Unsigned integer value to be advertised in the router's hello packets. The value must be the same for all routers attached to a common network. The default is 10 seconds.

retransmit-interval — (Optional) Number of seconds between link state advertisement retransmissions for adjacencies belonging to the interface.

seconds — (Optional) Expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds.

transmit-delay — (Optional) Estimated number of seconds it takes to transmit a link state update packet on the interface.

seconds (Optional) Integer value that must be greater than zero. Link state advertisements in the update packet have their age incremented by this amount before transmission. The default value is 1 second.

dead-interval (Optional) Number of seconds that a router’s hello packets are not seen before its neighbors declare the router down.

seconds (Optional) Unsigned integer value. The default is four times the hello interval. As with the hello interval, this value must be the same for all routers attached to a common network.

authentication-key (Optional) Specific password to be used by neighboring routers.

password (Optional) Any continuous string of characters, up to 8 bytes long, that you can enter from the keyboard. This string acts as a key that will allow the authentication procedure to generate or verify the authentication field in the OSPF header. This key is inserted directly into the OSPF header when originating routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to route OSPF traffic. There is no default value.

area-password [*password*]
no area-password [*password*]

To configure the IS-IS area authentication password, use the **area-password** router configuration command. To disable the password, use the **no** form of this command.

password Password you assign.

[**no**] **auto-summary**

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the **auto-summary** router configuration command. To disable this feature, use the **no** form of this command.

[**no**] **autonomous-system** *local-as*

To specify the local autonomous system that the router resides in for EGP, use the **autonomous-system** global configuration command. To remove the autonomous system number, use the **no** form of this command.

local-as	Local autonomous system number to which the router belongs.

[**no**] **bgp common-as** *autonomous-system* [*autonomous-system* ...]

To specify which autonomous systems belong to a common administration, use the **bgp common-as** router configuration command. To remove an autonomous system from the common administration, use the **no** form of this command.

autonomous-system	Autonomous system numbers that belong to a common administration.

[**no**] **bgp confederation identifier** *autonomous-system*

To specify a BGP confederation identifier, use the **bgp confederation identifier** router configuration command. To remove the confederation identifier, use the **no** form of this command.

autonomous-system	Autonomous system number that internally includes multiple autonomous systems.

[**no**] **bgp confederation peers** *autonomous-system* [*autonomous-system* ...]

To configure the autonomous systems that belong to the confederation, use the **bgp confederation peers** router configuration command. To remove an autonomous system from the confederation, use the **no** form of this command.

autonomous-system	Autonomous system number.

[**no**] **bgp default local-preference** *value*

To change the default local preference value, use the **bgp default local-preference** command. To return to the default setting, use the **no** form of this command.

value	Local preference value. Higher is more preferred. Integer from 0 through 4294967295.

[**no**] **bgp fast-external-fallover**

To immediately reset the BGP sessions of any directly adjacent external peers if the link used to reach them goes down, use the **bgp fast-external-fallover** router configuration command. To disable this feature, use the **no** form of this command.

clear ip bgp {***** | *address*}

To reset a BGP connection, use the **clear ip bgp** EXEC command at the system prompt.

*****	Resets all current BGP sessions.
address	Resets only the identified BGP neighbor.

clear ip eigrp neighbors [*ip-address* | *interface*]

To delete entries from the neighbor table, use the **clear ip eigrp neighbors** EXEC command.

ip-address (Optional) Address of the neighbor.

interface (Optional) Interface type and number. Specifying this argument removes from the neighbor table all entries learned via this interface.

clear ip igmp group [*group-name* | *group-address* | *type number*]

To delete entries from the IGMP cache, use the **clear ip igmp group** privileged EXEC command.

group-name (Optional) Name of the multicast group, as defined in the DNS hosts table or with the **ip host** command.

group-address (Optional) Address of the multicast group. This is a multicast IP address in four-part dotted notation.

type (Optional) Interface type.

number (Optional) Interface number.

clear ip mroute * | {*group-name* | *group-address*} [*source-address*]

To delete entries from the IP multicast routing table, use the **clear ip mroute** EXEC command.

***** Deletes all entries from the IP multicast routing table.

group-name Name of the multicast group, as defined in the DNS hosts table or with the **ip host** command.

group-address Address of the multicast group. This is a multicast IP address in four-part dotted notation.

source-address	(Optional) Address of a router that is a member of the multicast group. If you specify *source-address*, you must specify either *group-name* or *group-address*.

clear ip route {*network* [*mask*] | *****}

To delete entries from the IP routing table, use the **clear ip route** EXEC command.

network	Network or subnet address to remove.
mask	(Optional) Subnet mask to remove.
*****	Removes all routing table entries.

[**no**] **default-information allowed** {**in** | **out**} [**route-map** *map-tag*]

To control the candidate default routing information between IGRP or Enhanced IGRP processes, use the **default-information allowed** router configuration command. To suppress IGRP or Enhanced IGRP candidate information in incoming updates, use the **no default-information allowed in** command. To suppress IGRP or Enhanced IGRP candidate information in outbound updates, use the **no default-information allowed out** command.

in	Allows IGRP or Enhanced IGRP exterior or default routes to be received by an IGRP or Enhanced IGRP process.
out	Allows IGRP or Enhanced IGRP exterior routes to be advertised in updates.
route-map *map-tag*	(Optional) Indicates that the route map should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. The argument *map-tag* is the identifier of a configured route map. If you specify **route-map** without specifying *map-tag*, no routes are imported. If you omit **route-map**, all routes are redistributed.

[**no**] **default-information originate**

To allow the redistribution of network 0.0.0.0 into BGP, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

[**no**] **default-information originate**

To explicitly configure EGP to generate a default route, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

[**no**] **default-information originate** [**route-map** *map-name*]

To generate a default route into an IS-IS routing domain, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

originate	Originates the default route regardless of whether it resides in the routing table.
route-map *map-name*	(Optional) Routing process will generate the default route if the route-map is satisfied.

[**no**] **default-information originate** [**always**] [**metric** *metric-value*]
[**metric-type** *type-value*] {**level-1** | **level-1-2** | **level-2**}
[**route-map** *map-name*]

To generate a default route into an OSPF routing domain, use the **default-information originate** router configuration command. To disable this feature, use the **no** form of this command.

originate

For OSPF, causes the router to generate a default external route into an OSPF domain if the router already has a default route and you want to propagate to other routers. For IS-IS, originates the default route whether or not it resides in the routing table.

always

(Optional) For OSPF, the default route always will be advertised whether or not the router has a default route.

metric *metric-value*

(Optional) Metric used for generating the default route. If a value is not specified for this option, and no value is specified using the **default-metric** router configuration command, the default metric value is 10. The value used is specific to the protocol.

metric-type *type-value*

(Optional) For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values:

1—Type 1 external route

2—Type 2 external route

If a **metric-type** is not specified, the router adopts a Type 2 external route.

For IS-IS, it can be one of two values:

internal—IS-IS metric which is < 63.

external—IS-IS metric which is > 64 < 128. The default is **internal**.

level-1	For IS-IS only, Level 1 routes are redistributed into other IP routing protocols independently. It specifies if IS-IS advertises network 0.0.0.0 into the Level 1 area.
level-1-2	For IS-IS only, both Level 1 and Level 2 routes are redistributed into other IP routing protocols. It specifies if IS-IS advertises network 0.0.0.0 into both levels in a single command.
level-2	For IS-IS only, Level 2 routes are redistributed into other IP routing protocols independently. It specifies if IS-IS advertises network 0.0.0.0 into the Level 2 subdomain.
route-map *map-name*	(Optional) Routing process will generate the default route if the route-map is satisfied.

[**no**] **default-metric** *number*

To set default metric values for the BGP, EGP, OSPF, and RIP routing protocols, use this form of the **default-metric** router configuration command. To return to the default state, use the **no** form of this command.

number	Default metric value appropriate for the specified routing protocol

[**no**] **default-metric** *bandwidth delay reliability loading mtu*

To set metrics for IGRP or Enhanced IGRP, use this form of the **default-metric** router configuration command. To remove the metric value and return to the default state, use the **no** form of this command.

bandwidth	Minimum bandwidth of the route in kilobits per second. It can be 0 or any positive integer.
delay	Route delay in tens of microseconds. It can be 0 or any positive number that is a multiple of 39.1 nanoseconds.
reliability	Likelihood of successful packet transmission expressed as a number between 0 and 255. The value 255 means 100 percent reliability, and the value 0 means no reliability.
loading	Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).
mtu	Minimum maximum transmission unit (MTU) size of the route in bytes. It can be 0 or any positive integer.

[**no**] **distance** *weight* [*address mask* [*access-list-number*]] [**ip**]

To define an administrative distance, use the **distance** router configuration command. To remove a distance definition, use the **no** form of this command.

weight — Administrative distance. This can be an integer from 10 to 255. (The values 0 through 9 are reserved for internal use.) Used alone, the argument *weight* specifies a default administrative distance that the router uses when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table.

address — (Optional) IP address in four-part dotted notation.

mask — (Optional) IP address mask in four-part dotted-decimal format. A bit set to 1 in the *mask* argument instructs the router to ignore the corresponding bit in the address value.

access-list-number — (Optional) Number of a standard IP access list to be applied to incoming routing updates.

ip — (Optional) IP-derived routes for IS-IS. It can be applied independently for IP routes and ISO CLNS routes.

distance bgp *external-distance internal-distance local-distance*
no distance bgp

To allow the use of external, internal, and local administrative distances that could be a better route to a node, use the **distance bgp** router configuration command. To return to the default values, use the **no** form of this command.

external-distance Administrative distance for BGP external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.

internal-distance Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. A distance of 255 is the maximum possible distance, and any route with that distance will not be installed in the routing table.

local-distance Administrative distance for BGP local routes. Local routes are those networks listed with a **network** router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. A distance of 255 is the maximum possible distance, and any route with that distance will not be installed in the routing table.

distance eigrp *internal-distance external-distance*
no distance eigrp

To allow the use of two administrative distances—internal and external—that could be a better route to a node, use the **distance eigrp** router configuration command. To reset these values to their defaults, use the **no** form of this command.

internal-distance	Administrative distance for IP Enhanced IGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. It can be a value from 1 to 255.
external-distance	Administrative distance for IP Enhanced IGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. It can be a value from 1 to 255.

[**no**] **distribute-list** *access-list-number* **in** [*interface-name*]

To filter networks received in updates, use the **distribute-list in** router configuration command. To change or cancel the filter, use the **no** form of this command.

access-list-number	Standard IP access list number. The list explicitly specifies which networks are to be received and which are to be suppressed.
in	Applies the access list to incoming routing updates.
interface-name	(Optional) Interface on which the access list should be applied to incoming updates. If no interface is specified, the access list will be applied to all incoming updates.

[**no**] **distribute-list** *access-list-number* **out** [*interface-name* | *routing-process* | *autonomous-system-number*]

To suppress networks from being advertised in updates, use the **distribute-list out** router configuration command. To cancel this function, use the **no** form of this command.

access-list-number	Standard IP access list number. The list explicitly specifies which networks are to be sent and which are to be suppressed in routing updates.
out	Applies the access list to outgoing routing updates.
interface-name	(Optional) Name of a particular interface.
routing-process	(Optional) Name of a particular routing process, or the keyword **static** or **connected**.
autonomous-system-number	(Optional) Autonomous system number.

[**no**] **domain-password** [*password*]

To configure the IS-IS routing domain authentication password, use the **domain-password** router configuration command. To disable a password, use the **no** form of this command.

password	Password you assign.

[**no**] **ip address** *address mask* [**secondary**]

To specify the IP address on an interface, use the **ip address** interface configuration command. To remove an address, use the **no** form of this command.

address	IP address.
mask	IP address mask.
secondary	(Optional) Address to be added as a secondary address.

[**no**] **ip as-path access-list** *access-list-number* {**permit** | **deny**} *as-regular-expression*

To define a BGP-related access list, use the **ip as-path access-list** global configuration command. To disable use of the access list, use the **no** form of this command.

access-list-number — Integer from 1 to 199 that indicates the regular expression access list number.

permit — Permits access for matching conditions.

deny — Denies access to matching conditions.

as-regular-expression — Autonomous system in the access list using a regular expression. See the “Regular Expressions” appendix of the *Router Products Command Reference* publication for information about forming regular expressions.

ip community-list *community-list-number* {**permit** | **deny**} *community-number*
no ip community-list *community-list-number*

To create a community list for BGP and control access to it, use the **ip community-list** global configuration command. To delete the community list, use the **no** form of this command.

community-list-number — Integer 1 through 99 that identifies one or more permit or deny groups of communities.

permit — Permits access for a matching condition.

deny — Denies access for a matching condition.

community-number Community number configured by a **set community** command. Valid value is one of the following:

- 1 through 4294967200. You can specify a single number or multiple numbers separated by a space.
- **internet**—The Internet community.
- **no-export—**Do not advertise this route to an EBGP peer.
- **no-advertise**—Do not advertise this route to any peer (internal or external).

[**no**] **ip default-network** *network-number*

To select a network as a candidate route for computing the gateway of last resort, use the **ip default-network** global configuration command. To remove a route, use the **no** form of this command.

network-number Number of the network.

[**no**] **ip dvmrp accept-filter** *access-list-number* [*distance*]

To configure an acceptance filter for incoming DVMRP reports, use the **ip dvmrp accept-filter** interface configuration command. To disable this feature, use the **no** form of this command.

access-list-number Number of a standard IP access list. This can be a number from 0 to 99. A value of 0 means that all sources are accepted with the configured distance.

distance (Optional) Administrative distance to the destination.

ip dvmrp default-information {**originate** | **only**}
no ip dvmrp default-information {**originate** | **only**}

To advertise network 0.0.0.0 to DVMRP neighbors on an interface, use the **ip dvmrp default-information** interface configuration command. To prevent the advertisement, use the **no** form of this command.

originate	Other routes more specific than 0.0.0.0 can also be advertised.
only	No DVMRP routes other than 0.0.0.0 are advertised.

[**no**] **ip dvmrp metric** *metric* [*access-list-number*] [*protocol process-id*]

To configure the metric associated with a set of destinations for DVMRP reports, use the **ip dvmrp metric** interface configuration command. To disable this function, use the **no** form of this command.

metric	Metric associated with a set of destinations for DVMRP reports. It can be a value from 0 to 32. A value of 0 means that the route is not advertised. A value of 32 is equivalent to infinity (unreachable).
access-list-number	(Optional) Number of an access list. If you specify this argument, only the destinations that match the access list are reported with the configured metric. Any destinations not advertised because of split horizon do not use the configured metric.

protocol (Optional) Name of unicast routing protocol. It can be **bgp**, **egp**, **eigrp**, **igrp**, **isis**, **ospf**, or **rip**. (Note that these are the protocol names you can specify with a **router** *protocol* command.)

If you specify these arguments, only routes learned by the specified routing protocol are advertised in DVMRP report messages.

If you omit these arguments, only directly connected networks are advertised when DVMRP neighbors are discovered.

process-id (Optional) Process ID number of the unicast routing protocol.

ip gdp [**priority** *number* | **reporttime** *seconds* | **holdtime** *seconds*]
no ip gdp

To enable GDP routing on an interface, use the **ip gdp** interface configuration command. To disable GDP routing, use the **no** form of this command.

priority *number* (Optional) Alters the GDP priority; default is a priority of 100. A larger number indicates a higher priority. The default is 100.

reporttime *seconds* (Optional) Alters the GDP reporting interval; the default is 5 seconds for broadcast media such as Ethernets, and never for nonbroadcast media such as X.25. The default is 5 for broadcast media; 0 for nonbroadcast media.

holdtime *seconds* (Optional) Alters the GDP default hold time of 15 seconds. The default is 15 seconds.

[**no**] **ip hello-interval eigrp** *autonomous-system-number seconds*

To configure the hello interval for the IP Enhanced IGRP routing process designated by an autonomous system number, use the **ip hello-interval eigrp** interface configuration command. To restore the default value, use the **no** form of this command.

autonomous-system-number	Autonomous system number.
seconds	Hello interval, in seconds.

[**no**] **ip hold-time eigrp** *autonomous-system-number seconds*

To configure the hold time for the IP Enhanced IGRP routing process designated by the autonomous system number, use the **ip hold-time eigrp** interface configuration command. To restore the default value, use the **no** form of this command.

autonomous-system-number	Autonomous system number.
seconds	Hold time, in seconds.

[**no**] **ip igmp access-group** *access-list-number*

To control the multicast groups that hosts on the subnet serviced on an interface can join, use the **ip igmp access-group** interface configuration command. To disable groups on an interface, use the **no** form of this command.

access-list-number	Number of a standard IP access list. This can be a number from 1 to 99.

[**no**] **ip igmp join-group** *group-address*

To have the router join a multicast group, use the **ip igmp join-group** interface configuration command. To cancel membership in a multicast group, use the **no** form of this command.

group-address	Address of the multicast group. This is a multicast IP address in four-part dotted notation.

ip igmp query-interval *seconds*
no ip igmp query-interval

To configure the frequency at which the router sends IGMP host-query messages, use the **ip igmp query-interval** interface configuration command. To return to the default frequency, use the **no** form of this command.

seconds	Frequency, in seconds, at which to transmit IGMP host-query messages. The can be a number from 0 to 65535. The default is 60 seconds.

ip irdp [**multicast** | **holdtime** *seconds* | **maxadvertinterval** *seconds* | **minadvertinterval** *seconds* | **preference** *number* | **address** *addres*s [*number*]]
no ip irdp

To enable ICMP Router Discovery Protocol (IRDP) processing on an interface, use the **ip irdp** interface configuration command. To disable IRDP routing, use the **no** form of this command.

multicast	(Optional) Use the multicast address (224.0.0.1) instead of IP broadcasts.
holdtime *seconds*	(Optional) Length of time in seconds advertisements are held valid. The default is three times the **maxadvertinterval** value. Must be greater than **maxadvertinterval** and cannot be greater than 9000 seconds.

maxadvertinterval *seconds*
(Optional) Maximum interval in seconds between advertisements. The default is 600 seconds.

minadvertinterval *seconds*
(Optional) Minimum interval in seconds between advertisements. The default is 0.75 times the **maxadvertinterval**. If you change the **maxadvertinterval** value, this value defaults to three-quarters of the new value.

preference *number*
(Optional) Router's preference value. The allowed range is -2^{31} to 2^{31}. The default is 0. A higher value increases the router's preference level. You can modify a particular router so that it will be the preferred router to which others home. The default is 0.

address *address* [*number*]
(Optional) IP address (*address*) to proxy-advertise, and optionally, its preference value (*number*).

[**no**] **ip multicast-routing**

To enable IP multicast routing on the router, use the **ip multicast-routing** global configuration command. To disable IP multicast routing, use the **no** form of this command.

ip multicast-threshold *ttl*
no ip multicast-threshold [*ttl*]

To configure the time-to-live (TTL) threshold of packets being forwarded out an interface, use the **ip multicast-threshold** interface configuration command. To return to the default TTL threshold, use the **no** form of this command.

ttl
Time-to-live value, in hops. It can be a value from 0 to 255. The default value is 0, which means that all multicast packets are forwarded out the interface.

ip ospf authentication-key *password*
no ip ospf authentication-key

To assign a password to be used by neighboring routers that are using OSPF’s simple password authentication, use the **ip ospf authentication-key** interface configuration command. To remove a previously assigned OSPF password, use the **no** form of this command.

password Any continuous string of characters, up to 8 bytes long, that can be entered from the keyboard.

ip ospf cost *cost*
no ip cost

To explicitly specify the cost of sending a packet on an interface, use the **ip ospf cost** interface configuration command. To reset the path cost to the default value, use the **no** form of this command.

cost Unsigned integer value expressed as the link state metric. It can be a value in the range 1 to 65535.

ip ospf dead-interval *seconds*
no ip ospf dead-interval

To set how long a router’s Hello packets must not have been seen before its neighbors declare the router down, use the **ip ospf dead-interval** interface configuration command. To return to the default time, use the **no** form of this command.

seconds Unsigned integer that specifies the interval in seconds; the value must be the same for all nodes on the network. The default is four times the interval set by the **ip ospf hello-interval** command.

ip ospf hello-interval *seconds*
no ip ospf hello-interval

To specify the interval between Hello packets that the router sends on the interface, use the **ip ospf hello-interval** interface configuration command. To return to the default time, use the **no** form of this command.

seconds	Unsigned integer that specifies the interval in seconds. The value must be the same for all nodes on a specific network. The default is 10 seconds.

[**no**] **ip ospf-name-lookup**

To configure OSPF to look up Domain Name System (DNS) names for use in all OSPF **show** EXEC command displays, use the **ip ospf-name-lookup** global configuration command. To disable this feature, use the **no** form of this command.

ip ospf network {**broadcast** | **non-broadcast** | **point-to-multipoint**}
no ip ospf network

To configure the OSPF network type to a type other than the default for a given media, use the **ip ospf network** interface configuration command. To return to the default value, use the **no** form of this command.

broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to nonbroadcast.
point-to-multipoint	Sets the network type to point-to-multipoint.

ip ospf priority *number*
no ip ospf priority

To configure the OSPF network type to a type other than the default for a given media, use the **ip ospf network** interface configuration command. To return to the default value, use the **no** form of this command.

number 8-bit unsigned integer that specifies the priority. The range is from 0 to 255. The default is 1.

ip ospf retransmit-interval *seconds*
no ip ospf retransmit-interval

To specify the number of seconds between link state advertisement retransmissions for adjacencies belonging to the interface, use the **ip ospf retransmit-interval** interface configuration command. The **no** form of this command resets the link state advertisement retransmission interval to the default value.

seconds Time in seconds between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is 1 to 65535 seconds. The default is 5 seconds.

ip ospf transmit-delay *seconds*
no ip ospf transmit-delay

To set the estimated time it takes to transmit a link state update packet on the interface, use the **ip ospf transmit-delay** interface configuration command. To return to the default value, use the **no** form of this command.

seconds Time in seconds that it takes to transmit a link state update. It can be an integer in the range is 1 to 65535 seconds. The default is 1 second.

[**no**] **ip pim** {**dense-mode** | **sparse-mode**}

To enable IP multicast routing on an interface, use the **ip pim** interface configuration command. To disable the PIM multicast routing protocol on the interface, use the **no** form of this command.

dense-mode	Enables dense mode of operation.
sparse-mode	Enables sparse mode of operation.

ip pim query-interval *seconds*
no ip pim query-interval [*seconds*]

To configure the frequency of PIM router-query messages, use the **ip pim query-interval** interface configuration command. To return to the default interval, use the **no** form of this command.

seconds	Interval, in seconds, at which periodic PIM router-query messages are sent. It can be a number from 1 to 65535. The default is 30 seconds.

[**no**] **ip pim rp-address** *ip-address* [*access-list-number*]

To configure the address of a PIM rendezvous point (RP), use the **ip pim rp-address** global configuration command. To remove an RP address, use the **no** form of this command.

ip-address	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted notation.
access-list-number	(Optional) Number of an access list that defines which RPs are members of the group. This is a standard IP access list. The number can be from 1 to 100.

ip route *network* [*mask*] {*address* | *interface*} [*distance*]
no ip route

To establish static routes, use the **ip route** global configuration command. To remove static routes, use the **no** form of this command.

network	IP address of the target network or subnet.
mask	(Optional) Network mask that lets you mask network and subnetwork bits.
address	IP address of the next hop that can be used to reach that network.
interface	Network interface to use.
distance	(Optional) An administrative distance.

[**no**] **ip router isis** [*tag*]

To configure an IS-IS routing process for IP on an interface, use the **ip router isis** interface configuration command. To disable IS-IS for IP, use the **no** form of this command.

tag	(Optional) Defines a meaningful name for a routing process. If not specified, a null tag is assumed. It must be unique among all IP router processes for a given router. Use the same text for the argument *tag* as specified in the **router isis** global configuration command.

[**no**] **ip split-horizon**

To enable the split-horizon mechanism, use the **ip split-horizon** interface configuration command. To disable the split-horizon mechanism, use the **no** form of this command.

[**no**] **ip split-horizon eigrp** *autonomous-system-number*

To enable IP Enhanced IGRP split horizon, use the **ip split-horizon eigrp** interface configuration command. To disable split horizon, use the **no** form of this command.

autonomous-system-number	Autonomous system number.

[**no**] **ip summary-address eigrp** *autonomous-system-number address mask*

To configure a summary aggregate address for a specified interface, use the **ip summary-address eigrp** interface configuration command. To disable a configuration, use the **no** form of this command.

autonomous-system-number	Autonomous system number.
address	IP summary aggregate address to apply to an interface.
mask	Subnet mask.

[**no**] **is-type** {**level-1** | **level-1-2** | **level-2-only**}

To configure the IS-IS level at which the router operates, use the **is-type** router configuration command. To reset the default value, use the **no** form of this command.

level-1	Router acts as a station router.
level-1-2	Router acts as both a station router and an area router. This is the default.
level-2-only	Router acts as an area router only.

isis circuit-type {**level-1** | **level-1-2** | **level-2-only**}
no isis circuit-type

To configure the type of adjacency, use the **isis circuit-type** interface configuration command. To reset the circuit type to Level l and Level 2, use the **no** form of this command.

level-1	A Level 1 adjacency may be established if there is at least one area address in common between this system and its neighbors.
level-1-2	A Level 1 and 2 adjacency is established if the neighbor is also configured as **level-1-2** and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.
level-2-only	A Level 2 adjacency is established if and only if the neighbor is configured exclusively to be a Level 2 router.

[**no**] **isis csnp-interval** *seconds* {**level-1** | **level-2**}

To configure the IS-IS complete sequence number PDUs (CSNP) interval, use the **isis csnp-interval** interface configuration command. To restore the default value, use the **no** form of this command.

seconds	Interval of time between transmission of CSNPs on multiaccess networks. This interval only applies for the designated router. The default is 10 seconds.
level-1	Configures the interval of time between transmission of CSNPs for Level 1 independently.
level-2	Configures the interval of time between transmission of CSNPs for Level 2 independently.

isis hello-interval *seconds* {**level-1** | **level-2**}
no isis hello-interval {**level-1** | **level-2**}

To specify the length of time between Hello packets that the router sends, use the **isis hello-interval** interface configuration command. To restore the default value, use the **no** form of this command.

seconds	Unsigned integer value. A value three times the hello interval *seconds* is advertised as the *holdtime* in the hello packets transmitted. It must be the same for all routers attached to a common network. With smaller hello intervals, topological changes are detected faster, but there is more routing traffic. The default is 10 seconds.
level-1	Configures the hello interval for Level 1 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.
level-2	Configures the hello interval for Level 2 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.

isis metric *default-metric* [*delay-metric* [*expense-metric* [*error-metric*]]]
{**level-1** | **level-2**}
no isis metric {**level-1** | **level-2**}

To configure the metric for an interface, use the **isis metric** interface configuration command. To restore the default metric value, use the **no** form of this command.

default-metric	Metric used for the redistributed route. The default metric is used as a value for the IS-IS metric. This is the value assigned when there is no QOS routing performed. Only this metric is supported by Cisco routers. You can configure this metric for Level 1 and/or Level 2 routing. The range is from 0 to 63. The default value is 10.
delay-metric	Not supported.
expense-metric	Not supported.
error-metric	Not supported.
level-1	Router acts as a station router (Level 1) only.
level-2	Router acts as an area router (Level 2) only.

isis password *password* {**level-1** | **level-2**}
no isis password {**level-1** | **level-2**}

To configure the authentication password for an interface, use the **isis password** interface configuration command. To disable authentication for IS-IS, use the **no** form of this command.

password	Authentication password you assign for an interface.
level-1	Configures the authentication password for Level 1 independently. For Level 1 routing, the router acts as a station router only.
level-2	Configures the authentication password for Level 2 independently. For Level 2 routing, the router acts as an area router only.

isis priority *value* {**level-1** | **level-2**}
no isis priority {**level-1** | **level-2**}

To configure the priority of designated routers, use the **isis priority** interface configuration command. To reset the default priority, use the **no** form of this command.

value	Sets the priority of a router and is a number from 0 to 127. The default value is 64.
level-1	Sets the priority of a router for Level 1 independently.
level-2	Sets the priority of a router for Level 2 independently.

[**no**] **isis retransmit-interval** *seconds*

To configure the time between retransmission of IS-IS link-state PDU (LSP) retransmission for point-to-point links, use the **isis retransmit-interval** interface configuration command. To restore the default value, use the **no** form of this command.

seconds	Time in seconds between retransmission of IS-IS LSP retransmissions. It is an integer that should be greater than the expected round-trip delay between any two routers on the attached network. The default is 5 seconds.

[**no**] **match as-path** *path-list-number*

To match a BGP autonomous system path access list, use the **match as-path** route-map configuration command. To remove a path list entry, use the **no** form of this command.

path-list-number	Autonomous system path access list. An integer from 1 through 199.

[**no**] **match community-list** *community-list-number* [**exact**]

To match a BGP community, use the **match community-list** route-map configuration command. To remove the community list entry, use the **no** form of this command.

community-list-number	Community list number in the range from 1 through 99.
exact	(Optional) Indicates an exact match is required. All of the communities and only those communities in the community list must be present.

[**no**] **match interface** *type number...type number*

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** route-map configuration command. To remove the **match interface** entry, use the **no** form of this command.

type	Interface type.
number	Interface number.

[**no**] **match ip address** *access-list-number...access-list-number*

To distribute any routes that have a destination network number address that is permitted by a standard access list, use the **match ip address** route-map configuration command. To remove the **match ip address** entry, use the **no** form of this command.

access-list-number	Number of an access list. It can be an integer from 1 through 99.

[**no**] **match ip next-hop** *access-list-number...access-list-number*

To redistribute any routes that have a next-hop router address passed by one of the access lists specified, use the **match ip next-hop** route-map configuration command. To remove the next-hop entry, use the **no** form of this command.

access-list-number	Number of an access list. It can be an integer from 1 through 99.

[**no**] **match ip route-source** *access-list-number...access-list-number*

To redistribute routes that have been advertised by routers at the address specified by the access lists, use the **match ip route-source** route-map configuration command. To remove the route-source entry, use the **no** form of this command.

access-list-number	Number of an access list. It can be an integer from 1 through 99.

[**no**] **match metric** *metric-value*

To redistribute routes with the metric specified, use the **match metric** route-map configuration command. To remove the entry, use the **no** form of this command.

metric-value	Route metric. This may be an IGRP five-part metric. A metric value from 0 through 4294967295.

[**no**] **match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**}

To redistribute routes of the specified type, use the **match route-type** route-map configuration command. To remove the route-type entry, use the **no** form of this command.

local	Locally generated BGP routes.
internal	OSPF intra-area and interarea routes or Enhanced IGRP internal routes.
external [**type-1** | **type-2**]	OSPF external routes, or enhanced IGRP external routes. For OSPF, **external type-1** matches only type 1 external routes and **external type-2** matches only type 2 external routes.
level-1	IS-IS Level 1 routes.
level-2	IS-IS Level 2 routes.

[**no**] **match tag** *tag-value...tag-value*

To redistribute routes in the routing table that match the specified tags, use the **match tag** command. To remove the tag entry, use the **no** form of this command.

tag-value	List of one or more route tags. An integer from 0 through 4294967295.

mbranch {*group-address* | *group-name*} *branch-address* [*ttl*]

To trace a branch of a multicast tree for a specific group, use the **mbranch** privileged EXEC command.

group-address	Address of the multicast group. This is a multicast IP address in four-part dotted notation.
group-name	Name of the multicast group, as defined in the DNS hosts table or with the **ip host** command.

branch-address Address of a router that is a member of the group. This is a unicast IP address in four-part dotted notation.

ttl (Optional) Time-to-live value, in seconds, that is used in trace request packets sent to the branch router. The default value is 30 seconds.

[**no**] **metric holddown**

To keep new IGRP routing information from being used for a certain period of time, use the **metric holddown** router configuration command. To disable this feature, use the **no** form of this command.

[**no**] **metric maximum-hops** *hops*

To have the IP routing software to advertise as unreachable those routes with a hop count higher than is specified by the command (IGRP only), use the **metric maximum-hops** router configuration command. To reset the value to the default, use the **no** form of this command.

hops Maximum hop count (in decimal). The default value is 100 hops; the maximum number of hops that can be specified is 255. The default is 100.

metric weights *tos k1 k2 k3 k4 k5*
no metric weights

To allow the tuning of the IGRP or Enhanced IGRP metric calculations, use the **metric weights** router configuration command. To reset the values to their defaults, use the **no** form of this command.

tos Type of service. Currently, it must always be zero.

k1–k5 Constants that convert an IGRP or Enhanced IGRP metric vector into a scalar quantity. The default values are as follows: *k1* = 0; k2 = 0; *k3* = 1; *k4* = 0; *k5* = 0.

mrbranch {*group-address* | *group-name*} *branch-address* [*ttl*]

To trace a branch of a multicast tree for a group in the reverse direction, use the **mrbranch** EXEC command.

group-address	Address of the multicast group. This is a multicast IP address in four-part dotted notation.
group-name	Name of the multicast group, as defined in the DNS hosts table or with the **ip host** command.
branch-address	Address of a router that is a member of the group. This is a unicast IP address in four-part dotted notation.
ttl	(Optional) Time-to-live value, in hops, that is used in trace request packets sent to the branch router. The default value is 30.

[**no**] **neighbor** *ip-address*

To define a neighboring router with which to exchange routing information, use this form of the **neighbor** router configuration command. To remove an entry, use the **no** form of this command.

ip-address	IP address of a peer router with which routing information will be exchanged.

[**no**] **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*]

To configure OSPF routers interconnecting to nonbroadcast networks, use this form of the **neighbor** router configuration command. To remove a configuration, use the **no** form of this command.

ip-address	Interface IP address of the neighbor.
priority *number*	(Optional) 8-bit number indicating the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0.
poll-interval *seconds*	(Optional) Unsigned integer value reflecting the poll interval. RFC 1247 recommends that this value should be much larger than the hello interval. The default is 120 seconds.

[**no**] **neighbor** {*address* | *tag*} **advertisement-interval** *seconds*

To set the minimum interval between the sending of BGP routing updates, use the **neighbor advertisement-interval** router configuration command. To remove an entry, use the **no** form of this command.

address	Neighbor address.
tag	Neighbor tag.
seconds	Time in seconds. Integer from 0 through 600. The default is 30 for external peers and 5 for internal peers.

[**no**] **neighbor any** [*access-list-number*]

To control how neighbor entries are added to the routing table for both EGP and BGP, use the **neighbor any** router configuration command. To remove a configuration, use the **no** form of this command.

access-list-number	(Optional) Access list number the neighbor *must* be accepted by to be allowed to peer with the EGP or BGP process. If no list is specified, any neighbor will be allowed to peer with the router.

[**no**] **neighbor any third-party** *ip-address* [**internal** | **external**]

To configure an EGP process that determines which neighbors are treated as the next hop in EGP advertisements, use the **neighbor any third-party** router configuration command. To remove a configuration, use the **no** form of this command.

ip-address	IP address of the third-party router that is to be the next hop in EGP advertisements.
internal	(Optional) Indicates that the third-party router should be listed in the internal section of the EGP update.
external	(Optional) Indicates that the third-party router should be listed in the external section of the EGP update.

[**no**] **neighbor** *template-name* **configure-neighbors**

To have the router treat temporary neighbors that have been accepted by a template as if they had been configured manually, use the **neighbor configure-neighbors** router configuration command. To restore the default, use the **no** form of this command.

template-name	User-selectable designation that identifies a particular template. This can be an arbitrary word.

[**no**] **neighbor** *ip-address* **distribute-list** *access-list-number* {**in** | **out**}

To distribute BGP neighbor information as specified in an access list, use the **neighbor distribute-list** router configuration command. To remove an entry, use the **no** form of this command.

ip-address	Neighbor's IP address.
access-list-number	Predefined access list number. Only standard access lists can be used with this command.
in	Access list is applied to incoming advertisements to that neighbor.
out	Access list is applied to outgoing advertisements from that neighbor.

neighbor *ip-address* **ebgp-multihop**
no neighbor *ip-address*

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** router configuration command. To return to the default, use the **no** form of this command.

ip-address	IP address of the BGP-speaking neighbor.

[**no**] **neighbor** *ip-address* **filter-list** *access-list-number* {**in** | **out** | **weight** *weight*}

To set up BGP filter, use the **neighbor filter-list** router configuration command. To disable this function, use the **no** form of this command.

ip-address	IP address of the neighbor.
access-list-number	Number of an access for the autonomous system path. You define this access list with the **ip as-path access-list** command.

in	Access list to incoming routes.
out	Access list to outgoing routes.
weight *weight*	Assigns a relative importance to incoming routes matching autonomous system paths. Acceptable values are 0 to 65535.

neighbor *template-name* **neighbor-list** *access-list-number*
no neighbor *template-name* **neighbor-list**

To configure BGP to support anonymous neighbor peers by configuring a neighbor template, use the **neighbor neighbor-list** router configuration command. To delete a template, use the **no** form of this command.

template-name	User-selectable designation that identifies a particular template (an arbitrary word).
access-list-number	Number of an access list. It can be a number in the range 1 through 99.

[**no**] **neighbor** *ip-address* **next-hop-self**

To disable next-hop processing of BGP updates on the router, use the **neighbor next-hop-self** router configuration command. To disable this feature, use the **no** form of this command.

ip-address	IP address of the BGP-speaking neighbor.

[**no**] **neighbor** *ip-address* **remote-as** *number*

To add an entry to the BGP neighbor table, use the **neighbor remote-as** router configuration command. To remove an entry from the table, use the **no** form of this command.

ip-address	Neighbor’s IP address.
number	AS to which the neighbor belongs.

[**no**] **neighbor** {*address* | *tag*} **route-map** *route-map-name* {**in** | **out**}

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** router configuration command. To remove a route map, use the **no** form of this command.

address	Neighbor's IP address.
tag	Neighbor tag.
route-map-name	Name of route map.
in	Apply to incoming routes.
out	Apply to outgoing routes.

[**no**] **neighbor** *ip-address* **send-community**

To specify that a COMMUNITIES attribute should be sent to a BGP neighbor, use the **neighbor send-community** router configuration command. To remove the entry, use the **no** form of this command.

ip-address	Neighbor's IP address.

[**no**] **neighbor** *ip-address* **third-party** *third-party-ip-address*
[**internal** | **external**]

To send updates regarding EGP third-party routers, use the **neighbor third-party** router configuration command. To disable these updates, use the **no** form of this command.

ip-address	IP address of the EGP peer.
third-party-ip-address	Address of the third-party router on the network shared by the Cisco router and the EGP peer specified by *ip-address*.
internal	(Optional) Indicates that the third-party router should be listed in the internal section of the EGP update. This is the default.

external	(Optional) Indicates that the third-party router should be listed in the external section of the EGP update.

[**no**] **neighbor** *ip-address* **update-source** *interface*

To have the router allow internal BGP sessions to use any operational interface for TCP connections, use the **neighbor update-source** router configuration command. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

ip-address	IP address of the BGP-speaking neighbor.
interface	Loopback interface.

[**no**] **neighbor** *ip-address* **version** *value*

To configure the router to accept only a particular version, use the **neighbor version** router configuration command. To use the default version level of a neighbor, use the **no** form of this command.

ip-address	IP address of the BGP-speaking neighbor.
version *value*	Version number. The version can be set to 2 to force the router to only use Version 2 with the specified neighbor. The default is to use Version 4 of BGP and dynamically negotiate down to Version 2 if requested.

[**no**] **neighbor** *ip-address* **weight** *weight*

To assign a weight to a neighbor connection, use the **neighbor weight** router configuration command. To remove a weight assignment, use the **no** form of this command.

ip-address	Neighbor's IP address.
weight *weight*	Weight to assign. Acceptable values are 0 to 65535. Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

[**no**] **net** *network-entity-title*

To configure a Network Entity Title (NET) for the routing process, use the **net** router configuration command. To remove a NET, use the **no** form of this command.

network-entity-title	NET that specifies the area address and the system ID for an IS-IS routing process. This argument can be either an address or a name.

[**no**] **network** *network-number* **mask** *network-mask*

To specify the list of networks for the BGP routing process, use this form of the network router configuration command. To remove an entry, use the **no** form of this command.

network-number	IP address of the network.
mask *network-mask*	(Optional) Network mask address.

[**no**] **network** *network-number*

To specify the list of networks for the EGP routing process, use this form of the **network** router configuration command. To remove an entry, use the **no** form of this command.

network-number	IP address of a peer router with which routing information will be exchanged.

[**no**] **network** *network-number*

To specify a list of networks for the Enhanced IGRP, IGRP, or RIP routing process, use the **network** router configuration command. To remove a network from the list, use the **no** form of this command.

network-number	IP address of the directly connected network.

[**no**] **network** *address wildcard-mask* **area** *area-id*

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area** router configuration command. To disable OSPF routing for interfaces defined with the *address wildcard-mask* pair, use the **no** form of this command.

address	IP address.
wildcard-mask	IP-address-type mask that includes “don’t care” bits.
area-id	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. If you intend to associate areas with IP subnets, you can specify a subnet address as the *area-id*.

[**no**] **network** *address* **backdoor**

To specify a backdoor route to a BGP border router that will provide better information about the network, use the **network backdoor** router configuration command. To remove an address from the list, use the **no** form of this command.

address	IP address of the network to which you want a backdoor route.

[**no**] **network** *address* **weight** *weight*

To assign an absolute weight to a BGP network, use the **network weight** command. To delete an entry, use the **no** form of the command.

address	IP address of the network.
weight *weight*	Absolute weight. Integer from 0 to 65535. By default, *weight* is unmodified and is zero unless it has been modified by other router configuration commands.

[**no**] **offset-list** {**in** | **out**} *offset* [*access-list-number* | [*type number*]]

To add an offset to incoming and outgoing metrics to routes learned via RIP and IGRP, use the **offset-list** router configuration command. To remove an offset list, use the **no** form of this command.

in	Applies the access list to incoming metrics.
out	Applies the access list to outgoing metrics.
offset	Positive offset to be applied to metrics for networks matching the access list. If the offset is zero, no action is taken.

access-list-number	(Optional) Access list to be applied. If unspecified, the argument supplied to *offset* is applied to all metrics. If *offset* is zero, no action is taken. For IGRP, the offset is added to the delay component only. Must be a standard access list.
type	(Optional) Interface type to which the offset-list is applied.
number	(Optional) Interface number to which the offset-list is applied.

[**no**] **ospf auto-cost-determination**

To control how OSPF calculates default metrics for the interface, use the **ospf auto-cost-determination** router configuration command. To disable this feature, use the **no** form of this command.

[**no**] **passive-interface** *type number*

To disable sending routing updates on an interface, use the **passive-interface** router configuration command. To reenable the sending of routing updates, use the **no** form of this command.

type	Interface type.
number	Interface number.

[**no**] **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**weight** *weight*] [**subnets**]

To redistribute routes from one routing domain into another routing domain, use the **redistribute** router configuration command. To disable redistribution, use the **no** form of this command.

protocol

Source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **egp**, **igrp**, **isis**, **ospf**, **static** [**ip**], **connected** and **rip**.

The keyword **static** [**ip**] is used to redistribute IP static routes. The optional **ip** keyword is used when redistributing into IS-IS.

The keyword **connected** refers to routes which are established automatically by virtue of having enabled IP on an interface. For routing protocols such as OSPF and IS-IS, these routes will be redistributed as external to the autonomous system.

process-id

(Optional) For **bgp**, **egp**, or **igrp**, this is an autonomous system number, which is a 16-bit decimal number.
For **isis**, this is an optional *tag* that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing.
For **ospf**, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number.
For **rip**, no *process-id* value is needed.

level-1 For IS-IS, Level 1 routes are redistributed into other IP routing protocols independently.

level-1-2 For IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.

level-2 For IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.

metric *metric-value* (Optional) Metric used for the redistributed route. If a value is not specified for this option, and no value is specified using the **default-metric** router configuration command, the default metric value is 0. Use a value consistent with the destination protocol.

metric-type *type-value* (Optional) For OSPF, the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values:

1—Type 1 external route

2—Type 2 external route

If a **metric-type** is not specified, the router adopts a Type 2 external route.

For IS-IS, it can be one of two values:

internal—IS-IS metric which is < 63.

external—IS-IS metric which is > 64 < 128.

The default is **internal**.

match {**internal** | **external 1** | **external 2**}
(Optional) For OSPF, the criteria by which OSPF routes are redistributed into other routing domains. It an be one of the following:

internal—Routes that are internal to a specific autonomous system.

external 1—Routes that are external to the autonomous system, but are imported into OSPF as type 1 external route.

external 2—Routes that are external to the autonomous system, but are imported into OSPF as type 2 external route.

tag *tag-value*
(Optional) 32-bit decimal value attached to each external route. This is not used by the OSPF protocol itself. It may be used to communicate information between Autonomous System Boundary Routers. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used.

route-map
(Optional) Route map should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.

map-tag
(Optional) Identifier of a configured route map.

weight *weight*
Network weight when redistributing into BGP. An integer between 0 and 65535.

subnets
(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

[**no**] **route-map** *map-tag* [[**permit** | **deny**] | *sequence-number*]

To define the conditions for redistributing routes from one routing protocol into another, use the **route-map** global configuration command and the route-map configuration commands **match** and **set**. To delete an entry, use the **no route-map** command.

map-tag — Defines a meaningful name for the route map. The **redistribute** router configuration command uses this name to reference this route map. Multiple route maps may share the same map tag name.

permit — (Optional) If the match criteria are met for this route map, and **permit** is specified, the route is redistributed as controlled by the set actions. If the match criteria are not met, and **permit** is specified, the next route map with the same map-tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.

deny — (Optional) If the match criteria are met for the route map, and **deny** is specified, the route is not redistributed, and no further route maps sharing the same map tag name will be examined.

sequence-number — (Optional) Number that indicates the position a new route map is to have in the list of route maps already configured with the same name. If given with the **no** form of this command, it specifies the position of the route map that should be deleted.

[**no**] **router bgp** *autonomous-system*

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** global configuration command. To remove a routing process, use the **no** form of this command.

autonomous-system	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.

[**no**] **router egp** *remote-as*

To configure the Exterior Gateway Protocol (EGP) routing process, use the **router egp** global configuration command. To turn off an EGP routing process, use the **no router egp** command.

remote-as	Autonomous system number the router expects its peers to be advertising in their EGP messages.

[**no**] **router egp 0**

To specify that a router should be considered a core gateway, use the **router egp 0** global configuration command. To disable this function, use the **no** form of this command.

[**no**] **router eigrp** *autonomous-system-number*

To configure the IP Enhanced IGRP routing process, use the **router eigrp** global configuration command. To shut down the routing process on the specified autonomous system, use the **no** form of this command.

autonomous-system-number	Number of the autonomous system. It identifies the routes to the other IP Enhanced IGRP routers and is used to tag the routing information.

[**no**] **router igrp** *autonomous-system*

To configure the Interior Gateway Routing Protocol (IGRP) routing process, use the **router igrp** global configuration command. To shut down an IGRP routing process, use the **no** form of this command.

autonomous-system Number of a process that identifies the routes to the other IGRP routers. It is also used to tag the routing information. If you have an autonomous system number, you can use it for the process number.

[**no**] **router isis** [*tag*]

To enable the IS-IS routing protocol and to specify an IS-IS process for IP, use the **router isis** global configuration command. To disable IS-IS routing, use the **no** form of this command.

tag (Optional) Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP router processes for a given router.

[**no**] **router ospf** *process-id*

To configure an OSPF routing process, use the **router ospf** global configuration command. To terminate an OSPF routing process, use the **no** form of this command.

process-id Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

[**no**] **router rip**

To configure the Routing Information Protocol (RIP) routing process, use the **router rip** global configuration command. To turn off the RIP routing process, use the **no** form of this command.

[**no**] **set automatic-tag**

To automatically compute the tag value, use the **set automatic-tag** route-map configuration command. To disable this function, use the **no** form of this command.

[**no**] **set community** *community-number* [**additive**]

To set the BGP COMMUNITIES attribute, use the **set community** route-map configuration command. To delete the entry, use the **no** form of this command.

community-number	Valid values are 1 through 4294967200, **internet**, **no-export**, or **no-advertise**.
additive	(Optional) Add the community to the already existing communities.

[**no**] **set level** {**level-1** \| **level-2** \| **level-1-2** \| **stub-area** \| **backbone**}

To indicate where to import routes, use the **set level** route-map configuration command. To delete an entry, use the **no** form of this command.

level-1	Import into a Level 1 area.
level-2	Import into Level 2 subdomain. For IS-IS destinations, this is the default.
level-1-2	Import into Level 1 and Level 2.
stub-area	Import into OSPF NSSA area.
backbone	Import into OSPF backbone area. For OSPF destinations, this is the default.

[**no**] **set local-preference** *value*

To specify a preference value for autonomous system path, use the **set local-preference** route-map configuration command. To delete an entry, use the **no** form of this command.

value	Preference value. An integer from 0 through 4294967295. The default is 100.

[**no**] **set metric** *metric-value*

To set the metric value for the destination routing protocol, use the **set metric** route-map configuration command. To return to the default metric value, use the **no** form of this command.

metric-value	Metric value or IGRP bandwidth in kilobits per second. An integer from 0 through 294967295.

[**no**] **set metric-type** {**internal** | **external** | **type-1** | **type-2**}

To set the metric type for the destination routing protocol, use the **set metric-type** route-map command. To return to the default, use the **no** form of this command.

internal	IS-IS internal metric.
external	IS-IS external metric.
type-1	OSPF external type 1 metric.
type-2	OSPF external type 2 metric.

[**no**] **set next-hop** *next-hop*

To specify the address of the next hop, use the **set next-hop** route-map configuration command. To delete an entry, use the **no** form of this command.

next-hop	IP address of the next hop router.

set origin {**igp** | **egp** *autonomous-system* | **incomplete**}

To set the BGP origin code, use the **set origin** route-map configuration command. To delete an entry, use the **no** form of this command.

igp	Remote EGP.
egp	Local IGP.
autonomous-system	Remote autonomous system. This is an integer from 0 through 65535.
incomplete	Unknown heritage.

[**no**] **set tag** *tag-value*

To set a tag value of the destination routing protocol, use the **set tag** route-map configuration command. To delete the entry, use the **no** form of this command.

tag-value	Name for the tag. Integer from 0 through 4294967295.

[**no**] **set weight** *weight*

To specify the BGP weight for the routing table, use the **set weight** route-map configuration command. To delete an entry, use the **no** form of this command.

weight	Weight value. From 0 through 65535.

show ip bgp [*network*] [*network-mask*] [**subnets**]

To display entries in the BGP routing table, use the **show ip bgp** EXEC command.

network	(Optional) Network number, entered to display a particular network in the BGP routing table.
network-mask	(Optional) Displays all BGP routes matching the address/mask pair.
subnets	(Optional) Displays route and more specific routes.

show ip bgp cidr-only

To display routes with non natural network masks, use the **show ip bgp cidr-only** privileged EXEC command.

show ip bgp community *community-number* [**exact**]

To display routes that belong to specified BGP communities, use the **show ip bgp community** EXEC command.

community-number	Valid value is community number in the range from 1 through 4294967200, **internet**, **no-export**, or **no-advertise**.
exact	(Optional) Displays only routes that have exactly the same specified communities.

show ip bgp community-list *community-list-number* [**exact**]

To display routes that are permitted by the BGP community list, use the **show ip bgp community-list** EXEC command.

community-list-number	Community list number in the range from 1 through 99.
exact	(Optional) Displays only routes that have an exact match.

show ip bgp filter-list *access-list-number*

To display routes that conform to a specified filter list, use the **show ip bgp filter-list** privileged EXEC command.

access-list-number	Number of an access list. It can be a number from 1 through 199.

show ip bgp neighbors [*address* [**routes** \| **paths**]]

To display information about the TCP and BGP connections to individual neighbors, use the **show ip bgp neighbors** EXEC command.

address	(Optional) Address of the neighbor whose routes you have learned from.
routes	(Optional) Displays routes to specified neighbors.
paths	(Optional) Displays autonomous system paths to specified neighbor.

show ip bgp paths

To display all the BGP paths in the database, use the **show ip bgp paths** EXEC command.

show ip bgp regexp *regular-expression*

To display routes matching the regular expression, use the **show ip bgp regexp** privileged EXEC command.

regular-expression	Regular-expression to match the BGP autonomous system paths.

show ip bgp summary

To display the status of all BGP connections, use the **show ip bgp summary** EXEC command.

show ip dvmrp route [*ip-address*]

To display the contents of the DVMRP routing table, use the **show ip dvmrp route** EXEC command.

ip-address	(Optional) IP address of an entry in the DVMRP routing table.

show ip egp

To display statistics about EGP connections and neighbors, use the **show ip egp** EXEC command.

show ip eigrp neighbors [*type number*]

To display the neighbors discovered by IP Enhanced IGRP, use the **show ip eigrp neighbors** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.

show ip eigrp topology [*autonomous-system-number* | [[*ip-address*] *mask*]]

To display the IP Enhanced IGRP topology table, use the **show ip eigrp topology** EXEC command.

autonomous-system-number	(Optional) Autonomous system number.
ip-address	(Optional) IP address. When specified with a mask, a detailed description of the entry is provided.
mask	(Optional) Subnet mask.

show ip eigrp traffic [*autonomous-system-number*]

To display the number of IP Enhanced IGRP packets sent and received, use the **show ip eigrp traffic** EXEC command.

autonomous-system-number	(Optional) Autonomous system number.

show ip igmp groups [*group-name* | *group-address* | *type number*]

To display the multicast groups that are directly connected to the router and that were learned via IGMP, use the **show ip igmp groups** EXEC command.

group-name	(Optional) Name of the multicast group, as defined in the DNS hosts table.
group-address	(Optional) Address of the multicast group. This is a multicast IP address in four-part dotted notation.
type	(Optional) Interface type.
number	(Optional) Interface number.

show ip igmp interface [*type number*]

To display multicast-related information about an interface, use the **show ip igmp interface** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.

show ip irdp

To display IRDP values, use the **show ip irdp** EXEC command.

show ip mroute [*group-name* | *group-address*] [**summary**] [**count**]
show ip mroute [*group-name* [*source-address*] | *group-address*
[*source-address*]]

To display the contents of the IP multicast routing table, use the **show ip mroute** EXEC command.

group-name (Optional) Name of the multicast group, as defined in the DNS hosts table.

group-address (Optional) Address of the multicast group. This is a multicast IP address in four-part dotted notation.

summary (Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.

count (Optional) Displays statistics about the group, source router, and multicast packets.

source-address (Optional) Address of a router that is a member of the multicast group.

show ip ospf [*process-id*]

To display general information about OSPF routing processes, use the **show ip ospf** EXEC command.

process-id (Optional) Process ID. If this argument is included, only information for the specified routing process is displayed.

show ip ospf border-routers

To display the internal OSPF routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the **show ip ospf border-routers** privileged EXEC command.

show ip ospf [*process-id area-id*] **database**
show ip ospf [*process-id area-id*] **database** [**router**] [*link-state-id*]
show ip ospf [*process-id area-id*] **database** [**network**] [*link-state-id*]
show ip ospf [*process-id area-id*] **database** [**summary**] [*link-state-id*]
show ip ospf [*process-id area-id*] **database** [**asbr-summary**]
[*link-state-id*]
show ip ospf [*process-id*] **database** [**external**] [*link-state-id*]
show ip ospf [*process-id area-id*] **database** [**database-summary**]

Use the **show ip ospf database** EXEC command to display lists of information related to the OSPF database for a specific router. The various forms of this command deliver information about different OSPF link state advertisements.

process-id	(Optional) Internally used identifier. It is locally assigned and can be any positive integer number. The number used here is the number assigned administratively when enabling the OSPF routing process.
area-id	(Optional) Area number associated with the OSPF address range defined in the **network** router configuration command used to define the particular area.

link-state-id (Optional) Portion of the IP environment that is being described by the advertisement. The value entered depends on the advertisement's LS type. It must be entered in the form of an IP address.

When the link state advertisement is describing a network, the *link-state-id* can take one of two forms:

—Network's IP address (as in type 3 summary link advertisements and autonomous system external link advertisements).

—Derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.)

When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID.

When an autonomous system external advertisement (LS Type of 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).

router (Optional) Displays information about router link states.

network (Optional) Displays information about network link states.

summary (Optional) Displays summary information about network link states.

asbr-summary (Optional) Displays summary information about Autonomous System Boundary Router link states.

external (Optional) Displays information about autonomous system external link states.

database-summary (Optional) Displays database summary information and totals.

show ip ospf interface [*type number*]

To display OSPF-related interface information, use the **show ip ospf interface** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.

show ip ospf neighbor [*type number*] [*neighbor-id*] **detail**

To display OSPF-neighbor information on a per-interface basis, use the **show ip ospf neighbor** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.
neighbor-id	(Optional) Neighbor ID.
detail	Display all neighbors given in detail (list all neighbors).

show ip ospf virtual-links

To display parameters about and the current state of OSPF virtual links, use the **show ip ospf virtual-links** EXEC command.

show ip pim interface [*type number*]

To display information about interfaces configured for PIM, use the **show ip pim interface** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.

show ip pim neighbor [*type number*]

To list the PIM neighbors discovered by the router, use the **show ip pim neighbor** EXEC command.

type	(Optional) Interface type.
number	(Optional) Interface number.

show ip pim rp [*group-name* | *group-address*]

To display the rendezvous point (RP) routers associated with a sparse-mode multicast group, use the **show ip pim rp** EXEC command.

group-name	(Optional) Name of the multicast group, as defined in the DNS hosts table.
group-address	(Optional) Address of the multicast group. This is a multicast IP address in four-part dotted notation.

show ip protocols

To display the parameters and current state of the active routing protocol process, use the **show ip protocols** EXEC command.

show ip route [*address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]]

Use the **show ip route** EXEC command to display the current state of the routing table.

address	(Optional) Address about which routing information should be displayed.
mask	(Optional) Argument for a subnet mask.

longer-prefixes (Optional) The *address* and *mask* pair becomes a prefix and any routes that match that prefix are displayed.

protocol (Optional) Name of a routing protocol; or the keyword **connected**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.

process-id (Optional) Number used to identify a process of the specified protocol.

show ip route summary

To display the current state of the routing table, use the **show ip route summary** EXEC command.

show ip route supernets-only

To display information about supernets, use the **show ip route supernets-only** privileged EXEC command.

show isis database [level-1] [level-2] [l1] [l2] [detail] [lspid]

To display the IS-IS link state database, use the **show isis database** EXEC command.

level-1 (Optional) Displays the IS-IS link state database for Level 1.

level-2 (Optional) Displays the IS-IS link state database for Level 2.

l1 (Optional) Abbreviation for the option **level-1**.

l2 (Optional) Abbreviation for the option **level-2**.

detail (Optional) When specified, the contents of each LSP is displayed. Otherwise, a summary display is provided.

lspid (Optional) Link-state protocol ID. When specified, the contents of a single LSP is displayed by its ID number.

show route-map [*map-name*]

To display configured route-maps, use the **show route-map** EXEC command.

map-name (Optional) Name of a specific route-map.

[**no**] **summary-address** *address mask* {**level-1** | **level-1-2** | **level-2**}

Use the **summary-address** router configuration command to create aggregate addresses for IS-IS or OSPF. The **no summary-address** command restores the default.

address Summary address designated for a range of addresses.

mask IP subnet mask used for the summary route.

level-1 Only routes redistributed into Level 1 are summarized with the configured address/mask value. This keyword does not apply to OSPF.

level-1-2 The summary router is injected into both a Level 1 area and a Level 2 subdomain. This keyword does not apply to OSPF.

level-2 Routes learned by Level 1 routing will be summarized into the Level 2 backbone with the configured address/mask value. This keyword does not apply to OSPF.

[**no**] **synchronization**

To disable the synchronization between BGP and your IGP, use the **synchronization** router configuration command. To enable a router to advertise a network route without waiting for the IGP, use the **no** form of this command.

[**no**] **table-map** *route-map-name*

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** router configuration command. To disable this function, use the **no** form of the command.

route-map-name	Route map name, from **route-map** command.

timers basic *update invalid holddown flush* [*sleeptime*]
no timers basic

To adjust EGP, RIP, or IGRP network timers, use the **timers basic** router configuration command. To restore the default timers, use the **no** form of this command.

update Rate in seconds at which updates are sent. This is the fundamental timing parameter of the routing protocol.

invalid Interval of time in seconds after which a route is declared invalid; it should be three times the value of *update*. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.

holddown Interval in seconds during which routing information regarding better paths is suppressed. It should be at least three times the value of *update*. A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible.

flush Amount of time in seconds that must pass before the route is removed from the routing table; the interval specified must be at least the sum of *invalid* and *holddown*. If it is less than this sum, the proper holddown interval cannot elapse, which results in a new route being accepted before the holddown interval expires.

sleeptime (Optional) For IGRP only, interval in milliseconds for postponing routing updates in the event of a flash update. The *sleeptime* value should be less than the *update* time. If the *sleeptime* is greater than the *update* time, routing tables will become unsynchronized.

timers bgp *keepalive holdtime*
no timers bgp

To adjust BGP network timers, use the **timers bgp** router configuration command. To reset the BGP timing defaults, use the **no** form of this command.

keepalive Frequency, in seconds, with which the router sends *keepalive* messages to its peer. The default is 60 seconds.

holdtime Interval, in seconds, after not receiving a *keepalive* message that the router declares a peer dead. The default is 180 seconds.

timers egp *hello polltime*
no timers egp

To adjust EGP Hello and polltime network timers, use the **timers egp** router configuration command. The **no timers egp** command resets the EGP timing defaults.

hello Frequency, in seconds, with which the router sends hello messages to its peer. The default is 60 seconds.

polltime Interval, in seconds, for how frequently to exchange updates. The default is 180 seconds.

[**no**] **timers spf** *spf-delay spf-holdtime*

To configure the delay time between when OSPF receives a topology change and when it starts a Shortest Path First (SPF) calculation, and the hold time between two consecutive SPF calculations, use the **timers spf** router configuration command. To return to the default timer values, use the **no** form of this command.

spf-delay Delay time, in seconds, between when OSPF receives a topology change and when it starts a SPF. calculation. It can be an integer from 0 to 65535. The default time is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started immediately.

spf-holdtime Minimum time, in seconds, between two consecutive SPF calculations. It can be an integer from 0 to 65535. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two consecutive SPF calculations can be done one immediately after the other.

[**no**] **traffic share** {**balanced** | **min**}

To control how traffic is distributed among routes when there are multiple routes for the same destination network that have different costs, use the **traffic-share** router configuration command. To disable this function, use the **no** form of the command.

balanced	Distributes traffic proportionately to the ratios of the metrics.
min	Uses routes that have minimum costs.

[**no**] **validate-update-source**

To have the router to validate the source IP address of incoming routing updates for RIP and IGRP routing protocols, use the **validate-update-source** router configuration command. To disable this function, use the **no** form of this command.

variance *multiplier*
no variance

To control load balancing in an IP Enhanced IGRP-based internetwork, use the **variance** router configuration command. To reset the variance to the default value, use the **no** form of this command.

multiplier	Metric value used for load balancing. It can be a value from 1 to 128. The default is 1, which means equal-cost load balancing.

ISO CLNS Commands

This chapter describes the function and displays the syntax of each ISO CLNS command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **area-password** [*password*]

Use the **area-password** router configuration command to configure the area authentication password. The **no** form of this command disables the password.

password	Password you assign.

clear clns cache

Use the **clear clns cache** EXEC command to clear and reinitialize the CLNS routing cache.

clear clns es-neighbors

Use the **clear clns es-neighbors** EXEC command to remove ES neighbor information from the adjacency database.

clear clns is-neighbors

Use the **clear clns is-neighbors** EXEC command to remove IS neighbor information from the adjacency database.

clear clns neighbors

Use the **clear clns neighbors** EXEC command to remove CLNS neighbor information from the adjacency database.

clear clns route

Use the **clear clns route** EXEC command to remove all of the dynamically derived CLNS routing information.

[**no**] **clns access-group** *name* [**in** | **out**]

Use the **clns access-group** interface configuration command to filter transit CLNS traffic going either into or out of the router or both on a per-interface basis. Use the **no** form of this command to disable filtering of transit CLNS packets.

name	Name of the filter set or expression to apply.
in	(Optional) Filter should be applied to CLNS packets entering the router.
out	(Optional) Filter should be applied to CLNS packets leaving the router. If you do not specify an **in** or **out** keyword, **out** is assumed.

[**no**] **clns adjacency-filter** {**es** | **is**} *name*

Use the **clns adjacency-filter** interface configuration command to filter the establishment of CLNS end system (ES) and intermediate system (IS) adjacencies. Use the **no** form of this command to disable this filtering.

es	End system adjacencies are to be filtered.
is	Intermediate system adjacencies are to be filtered.
name	Name of the filter set or expression to apply.

[**no**] **clns checksum**

Use the **clns checksum** interface configuration command to enable checksum generation when ISO CLNS routing software sources a CLNS packet. Use the **no** form of this command to disable checksum generation.

[**no**] **clns cluster-alias**

Use the **clns cluster-alias** interface configuration command to allow multiple systems to advertise the same system ID as other systems in end-system hello messages. The **no** form of this command disables cluster aliasing.

clns configuration-time *seconds*
no clns configuration-time

Use the **clns configuration-time** global configuration command to specify the rate at which ES hellos (ESHs) and IS hellos (ISHs) are sent. You can restore the default value by specifying the **no** form of this command.

seconds	Rate in seconds at which ESH and ISH packets are sent. The default is 60 seconds.

clns congestion-threshold *number*
no clns congestion-threshold

Use the **clns congestion-threshold** interface configuration command to set the congestion experienced bit if the output queue has more than the specified number of packets in it. A *number* value of zero or the **no** form of the command prevents this bit from being set. Use the **no** form of this command to remove the parameter setting and set it to 0.

number	Number of packets that are allowed in the output queue before the system sets the congestion-experienced bit. The value zero (0) prevents this bit from being set. The default is 4.

[**no**] **clns dec-compatible**

Use the **clns dec-compatible** interface configuration command to allow ISHs sent and received to ignore the N-selector byte. Use the **no** form of this command to disable this feature.

[**no**] **clns enable**

Use the **clns enable** interface configuration command if you do not intend to perform any static or dynamic routing on an interface, but intend to pass ISO CLNS packet traffic to end systems. Use the **no** form of this command to disable ISO CLNS on a particular interface.

[**no**] **clns erpdu-interval** *milliseconds*

Use the **clns erpdu-interval** interface configuration command to determine the minimum interval time, in milliseconds, between error PDUs (ERPDUs). A *milliseconds* value of zero or the **no** form of this command turns off the interval and effectively sets no limit between ERPDUs.

milliseconds	Minimum interval time (in milliseconds) between ERPDUs. The default is 10 milliseconds.

[**no**] **clns esct-time** *seconds*

Use the **clns esct-time** interface configuration command to supply an ES Configuration Timer (ESCT) option in a transmitted IS hello packet that tells the end system how often it should transmit ES hello packet protocol data units (PDUs). Use the **no** form of this command to restore the default value and disable this feature.

seconds	Time, in seconds, between ESH PDUs. Range is from 0 through 65535. The default is 0 seconds.

clns es-neighbor *nsap snpa*
no clns es-neighbor *nsap*

Use the **clns es-neighbor** interface configuration command to list all end systems that will be used when you manually specify the NSAP-to-SNPA mapping. The SNPAs are the MAC addresses. Use the **no** form of this command to delete the ES neighbor.

nsap	Specific NSAP to map to the MAC address.
snpa	Data link (MAC) address .

clns filter-expr *ename term*
clns filter-expr *ename* **not** *term*
clns filter-expr *ename term* **or** *term*
clns filter-expr *ename term* **and** *term*
clns filter-expr *ename term* **xor** *term*
no clns filter-expr *ename*

Use one or more **clns filter-expr** global configuration commands to combine CLNS filter sets and CLNS address templates into complex logical NSAP pattern-matching expressions. The **no** form of this command deletes the expression. There are many forms of this command.

ename — Alphanumeric name to apply to this filter expression.

term — Filter expression term. A term can be any of the following:

ename—Another, previously defined, filter expression.

sname (or **destination** *sname*)—A previously defined filter set name, with the filter set applied to the destination NSAP address.

source *sname*—A previously defined filter set name, with the filter set applied to the source NSAP address.

clns filter-set *sname* [**permit** | **deny**] *template*
no clns filter-set *sname*

Use one or more **clns filter-set** global configuration commands to build a list of CLNS address templates with associated permit and deny conditions for use in CLNS filter expressions. CLNS filter expressions are used in the creation and use of CLNS access lists. The **no** form of this command deletes the entire filter set.

sname	Alphanumeric name to apply to this filter set.
permit | **deny**	(Optional) Addresses matching the pattern specified by *template* are to be permitted or denied. If neither **permit** nor **deny** is specified, **permit** is assumed.
template	Address template, template alias name, or the keyword **default**. Address templates and alias names are described under the description of the **clns template-alias** global configuration command. The **default** keyword denotes a zero-length prefix and matches any address.

clns holding-time *seconds*
no clns holding-time

Use the **clns holding-time** global configuration command to allow the sender of an ESH or ISH to specify the length of time you consider the information in the hello packets to be valid. You can restore the default value (300 seconds or 5 minutes) by using the **no** form of this command.

seconds	Length of time in seconds during which the information in the hello packets is considered valid. The default is 300 seconds (5 minutes).

clns host *name nsap*

Use the **clns host** global configuration command to define a name-to-NSAP mapping that can then be used with commands requiring NSAPs.

name	Desired name for the NSAP. The first character can be either a letter or a number, but if you use a number, the operations you can perform are limited.
nsap	NSAP that the name maps to.

clns is-neighbor *nsap snpa*
no clns is-neighbor *nsap*

Use the **clns is-neighbor** interface configuration command to list all intermediate systems that will be used when you manually specify the NSAP-to-SNPA mapping. The SNPAs are the MAC addresses. Use the **no** form of this command to delete the specified IS neighbor.

nsap	NSAP address of a specific intermediate system to enter as a neighbor to a specific MAC address.
snpa	Data link (MAC) address.

clns mtu *size*
no clns mtu

Use the **clns mtu** interface configuration command to set the MTU packet size for the interface. The **no** form of this command restores the default and maximum packet size.

size	Maximum packet size in bytes. The minimum value is 512; the default and maximum packet size depends on the interface type.

[**no**] **clns net** {*net-address* | *name*}

Use the **clns net** global configuration command to assign a static address for a router. If a router is configured to support ISO CLNS but is not configured to dynamically route CLNS packets using ISO-IGRP or IS-IS, use this command to assign an address to the router. The **no** form of this command removes any previously configured NET or NSAP address.

net-address	Network Entity Title (NET). See this command in the *Router Products Command Reference* publication for the algorithm used.
name	CLNS host name to be associated with this interface.

[**no**] **clns net** {*nsap-address* | *name*}

Use this form of the **clns net** command as an interface configuration command to assign an NSAP address or name to a router interface. If a router is configured to support ISO CLNS, but is not configured to dynamically route CLNS packets using a ISO-IGRP or IS-IS, use this command to assign an address to the router. The **no** form of this command removes any previously configured NSAP address.

nsap-address	Specific NSAP address.
name	Name to be associated with this interface.

clns packet-lifetime *seconds*
no clns packet-lifetime

Use the **clns packet-lifetime** global configuration command to specify the initial lifetime for locally generated packets. The **no** form of this command removes the parameter’s settings.

seconds	Packet lifetime in seconds. The default is 32 seconds.

[**no**] **clns rdpdu-interval** *milliseconds*

Use the **clns rdpdu-interval** interface configuration command to determine the minimum interval time, in milliseconds, between redirect PDUs (RDPDUs). A *milliseconds* value of zero or the **no** form of this command turns off the interval rate and effectively sets no limit between RDPDUs.

milliseconds	Minimum interval time (in milliseconds) between RDPDUs. The default is 100 milliseconds.

clns route *nsap-prefix type number* [*snpa-address*]
no clns route *nsap-prefix*

Use this form of the **clns route** global configuration command to create an interface static route. The **no** form of the command removes this route.

nsap-prefix	Network service access point prefix. This value is entered into a static routing table and used to match the beginning of a destination NSAP. The longest NSAP-prefix entry that matches is used.
type	Interface type.
number	Interface unit number.
snpa-address	(Optional) Optional for serial links; required for multiaccess networks.

clns route *nsap-prefix* {*next-hop-net* | *name*}
no clns route *nsap-prefix*

Use this form of the **clns route** global configuration command to enter a specific static route. NSAPs that start with *nsap-prefix* are forwarded to *next-hop-net* or the *name* of the next hop. The **no** form of this command removes this route.

nsap-prefix	Network service access point prefix. This value is entered into a static routing table and used to match the beginning of a destination NSAP. The longest NSAP-prefix entry that matches is used.
next-hop-net	Next-hop Network Entity Title. This value is used to establish the next hop of the route for forwarding packets.
name	Name of the next hop node. This value can be used instead of the next-hop NET to establish the next hop of the route for forwarding packets.

clns route default *nsap-prefix type number*
no clns route default

Use this form of the **clns route default** global configuration command to configure a default zero-length prefix rather than type an NSAP prefix. The **no** form of this command removes this route.

nsap-prefix	Network service access point prefix that is a default zero-length prefix.
type	Interface type. Specify the interface immediately followed by the unit number; there is no space between the two. For example, ethernet3.
number	Interface unit number.

clns route *nsap-prefix* **discard**
no clns route *nsap-prefix*

Use this form of the **clns route discard** global configuration command to tell a router explicitly to discard packets with NSAP addresses that match the specified *nsap-prefix*. The **no** form of this command removes this route.

nsap-prefix	Network service access point prefix. This value is entered into a static routing table and used to match the beginning of a destination NSAP. The longest NSAP-prefix entry that matches is used.
discard	Explicitly tells a router to discard packets with NSAPs that match the specified *nsap-prefix*.

[**no**] **clns route-cache**

Use the **clns route-cache** interface configuration command to allow fast switching through the cache. To disable fast switching, use the **no** form of this command.

[**no**] **clns router isis** [*tag*]

Use the **clns router isis** interface configuration command to enable IS-IS routing for OSI on a specified interface. Use the **no** form of this command with the appropriate area tag to disable IS-IS on the interface.

tag	(Optional) Meaningful name for a routing process. If not specified, a null tag is assumed. It must be unique among all CLNS router processes for a given router. Use the same text for the argument *tag* as specified in the **router isis** global configuration command.

clns router iso-igrp *tag* [**level 2**]
no clns router iso-igrp *tag*

Use the **clns router iso-igrp** interface configuration command to specify ISO-IGRP routing on a specified interface. Use the **no** form of this command with the appropriate tag to disable ISO-IGRP routing on the interface.

tag	Meaningful name for routing process. It must be unique among all CLNS router processes for a given router. This tag should be the same as defined for the routing process in the **router iso-igrp** global configuration command.
level 2	(Optional) Allows the interface to advertise Level 2 information.

[**no**] **clns routing**

Use the **clns routing** global configuration command to enable routing of CLNS packets. Use the **no** form of this command to disable CLNS routing.

[**no**] **clns security pass-through**

Use the **clns security pass-through** global configuration command to allow the router to pass packets that have security options set. To revert to the default, use the **no** form of this command.

[**no**] **clns send-erpdu**

Use the **clns send-erpdu** interface configuration command to allow CLNS to send an error PDU when the routing software detects an error in a data PDU. To disable this function, use the **no** form of this command.

[**no**] **clns send-rdpdu**

Use the **clns send-rdpdu** interface configuration command to allow CLNS to send redirect PDUs (RDPDUs) when a better route for a given host is known. To disable this function, use the **no** form of this command.

[**no**] **clns split-horizon**

Use the **clns split-horizon** interface configuration command to implement split horizon for ISO-IGRP updates. The **no** form of this command disables this feature.

clns template-alias *name template*
no clns template-alias *name*

Use one or more **clns template-alias** global configuration commands to build a list of alphanumeric aliases of CLNS address templates for use in the definition of CLNS filter sets. The **no** form of this command deletes the alias.

name	Alphanumeric name to apply as an alias for the template.
template	Address template. See this command in the *Router Products Command Reference* publication for more information.

[**no**] **clns want-erpdu**

Use the **clns want-erpdu** global configuration command to specify whether to request error PDUs on packets sourced by the router. The **no** form of this command removes the parameter’s settings.

[**no**] **distance** *value* [**clns**]

Use the **distance** router configuration command to configure the administrative distance for CLNS routes learned. The **no** form of this command restores the administrative distance to the default.

value	Administrative distance, indicating the trustworthiness of a routing information source. This argument has a numerical value between 0 and 255. A higher relative value indicates a lower trustworthiness rating. Preference is given to routes with smaller values. Defaults are: static routes—10; ISO-IGRP routes—100; IS-IS routes—110. The default, if unspecified, is 110.
clns	(Optional) CLNS-derived routes for IS-IS.

[**no**] **domain-password** [*password*]

Use the **domain-password** router configuration command to configure the routing domain authentication password. The **no** form of this command disables the password.

password	Password you assign

[**no**] **ip domain-lookup nsap**

Use the **ip domain-lookup nsap** global configuration command to allow Domain Name System (DNS) queries for CLNS addresses. To disable this feature, specify the **no** form of this command.

[**no**] **is-type** {**level-1** | **level-1-2** | **level-2-only**}

Use the **is-type** router configuration command to configure the IS-IS level at which the router is to operate. The **no** form of this command resets the parameter to the default.

level-1	Causes the router to act as a station router.
level-1-2	Causes the router to act as both a station router and an area router. This is the default.
level-2-only	Causes the router to act as an area router only.

[**no**] **isis adjacency-filter** *name* [**match-all**]

Use the **isis adjacency-filter** interface configuration command to filter the establishment of IS-IS adjacencies. Use the **no** form of this command to disable filtering of the establishment of IS-IS adjacencies.

name	Name of the filter set or expression to apply.
match-all	(Optional) All NSAP addresses must match the filter in order to accept the adjacency. If not specified (the default), only one address need match the filter in order for the adjacency to be accepted.

isis circuit-type {**level-1** | **level-1-2** | **level-2-only**}
no isis circuit-type

Use the **isis circuit-type** interface configuration command to configure the type of adjacency desired for the specified interface. The **no** form of this command resets the circuit type to Level l and Level 2.

level-1 — Level 1 adjacency can be established if there is at least one area address in common between this system and its neighbors.

level-1-2 — Level 1 and 2 adjacency is established if the neighbor is also configured as **level-1-2** and there is at least one area in common. If there is no area in common, a Level 2 adjacency is established. This is the default.

level-2-only — Level 2 adjacency is established on the circuit. If the neighboring router is a Level 1 only router, no adjacency will be established.

[**no**] **isis csnp-interval** *seconds* {**level-1** | **level-2**}

Use the **isis csnp-interval** interface configuration command to configure the IS-IS complete sequence number PDUs (CSNP) interval for the specified interface. The **no** form of this command restores the default value.

seconds — Interval of time in seconds between transmission of CSNPs on multiaccess networks. (Only applies for the designated router.) The default is 10 seconds.

level-1 — Interval of time between transmission of CSNPs for Level 1 independently.

level-2 — Interval of time between transmission of CSNPs for Level 2 independently.

[**no**] **isis hello-interval** *seconds* {**level-1** | **level-2**}

Use the **isis hello-interval** interface configuration command to specify the length of time in seconds between hello packets that the router sends on the specified interface. The **no** form of this command restores the default value.

seconds	Unsigned integer value. A value three times the hello interval *seconds* is advertised as the *holdtime* in the hello packets transmitted. It must be the same for all routers attached to a common network. With smaller hello intervals, topological changes are detected faster, but there is more routing traffic. The default is 10 seconds.
level-1	Configure the hello interval for Level 1 independently. Use this on X.25, SMDS, and Frame Relay multiaccess networks.
level-2	Configure the hello interval for Level 2 independently. Use with X.25, SMDS, and Frame Relay multiaccess networks.

isis metric *default-metric delay-metric expense-metric error-metric*
{**level-1** | **level-2**}
no isis metric {**level-1** | **level-2**}

Use the **isis metric** interface configuration command to configure the metric (or cost) for the specified interface. The **no** form of this command restores the default metric value.

default-metric	Metric used for the redistributed route. The range is from 0 through 63. The default value is 10.
delay-metric	Not supported.
expense-metric	Not supported.

error-metric	Not supported.
level-1	The router acts as a station router (Level 1) only.
level-2	The router acts as an area router (Level 2) only.

isis password *password* {**level-1** | **level-2**}
no isis password {**level-1** | **level-2**}

Use the **isis password** interface configuration command to configure the authentication password for a specified interface. The **no** form of this command disables authentication for IS-IS.

password	Authentication password you assign for an interface.
level-1	Configure the authentication password for Level 1 independently. For Level 1 routing, the router acts as a station router only.
level-2	Configure the authentication password for Level 2 independently. For Level 2 routing, the router acts as an area router only.

isis priority *value* {**level-1** | **level-2**}
no isis priority {**level-1** | **level-2**}

Use the **isis priority** interface configuration command to configure the priority of this system for designated router election. The **no** form of this command resets priority to 64.

value	Priority of a router; a number from 0 through 127. The default is 64.
level-1	Set priority of a router for Level 1 independently.
level-2	Set priority of a router for Level 2 independently.

[**no**] **isis retransmit-interval** *seconds*

Use the **isis retransmit-interval** interface configuration command to configure the number of seconds between retransmission of IS-IS link-state PDU (LSP) retransmission for point-to-point links. The **no** form of this command restores the default value.

seconds Integer that should be greater than the expected round-trip delay between any two routers on the attached network. The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links. The default is 5 seconds.

[**no**] **iso-igrp adjacency-filter** *name*

Use the **iso-igrp adjacency-filter** interface configuration command to filter the establishment of ISO-IGRP adjacencies. Use the **no** form of this command to disable filtering of the establishment of ISO-IGRP adjacencies.

name Name of the filter set or expression to apply.

[**no**] **match clns address** *name* [*name...name*]

To define the address match criterion, use the **match clns address** route-map configuration command; routes that have a network address matching one or more of the names—and that satisfy all other defined match criteria—will be redistributed. To remove the match criterion, use the **no** form of this command.

name Name of a standard address list, filter set, or expression.

[**no**] **match clns next-hop** *name* [*name...name*]

Use the **match clns next-hop** route-map configuration command to define the next-hop match criterion; routes that have a next-hop router address matching one of the names—and that satisfy all other defined match criteria—will be redistributed.

name	Name of an access list, filter set, or expression.

[**no**] **match clns route-source** *name* [*name..name*]

Use the **match clns route-source** route-map configuration command to define the route-source match criterion; routes that have been advertised by routers at the address specified by the name—and that satisfy all other defined match criteria—will be redistributed. Use the **no** form of this command to remove the specified match criterion.

name	Name of filter set or expression.

[**no**] **match interface** *type number* [*type number...type number*]

Use the **match interface** route-map configuration command to define the interface match criterion; routes that have the next hop out one of the interfaces specified—and that satisfy all other defined match criteria—will be redistributed. Use the **no** form of this command to remove the specified match criterion.

type	Interface type.
number	Interface unit number.

[**no**] **match metric** *metric-value*

Use the **match metric** route-map configuration command to define the metric match criterion; routes that have the specified metric—and that satisfy all other defined match criteria—will be redistributed. Use the **no** form of this command to remove the specified match criterion.

metric-value	Route metric. This can be an IGRP five-part metric.

[**no**] **match route-type** {**level-1** | **level-2**}

Use the **match route-type** route-map configuration command to define the route-type match criterion; routes that have the specified route type—and that satisfy all other defined match criteria—will be redistributed. Use the **no** form of the command to remove the specified match criterion.

level-1	IS-IS Level 1 routes.
level-2	IS-IS Level 2 routes.

metric weights *qos k1 k2 k3 k4 k5*
no metric weights

Use the **metric weights** router configuration command to specify different metrics for the ISO-IGRP routing protocol on CLNS. This command allows you to configure the metric constants used in the ISO-IGRP composite metric calculation of reliability and load. Use the **no metric weights** command to return the five *k* constants to their default values.

qos	Quality of service. QOS defines transmission quality and availability of service. The value must be 0, the *default metric* value.
k1, *k2*, *k3*, *k4*, *k5*	Values that apply to ISO-IGRP for the default metric QOS. The *k* values are metric constants used in the ISO-IGRP equation that converts an IGRP metric vector into a scalar quantity. They are numbers from 0 through 127; higher numbers mean a greater multiplier effect. The defaults are *k1* = 1**;** *k2* = 0; *k3* = 1; *k4* = 0; *k5* = 0.

[**no**] **net** *network-entity-title*

Use the **net** router configuration command to configure a Network Entity Title (NET) for the specified routing process. The **no** form of this command removes a specific NET; you must specify the NET.

network-entity-title	Area addresses for the ISO-IGRP or IS-IS area.

ping clns {*host* | *address*}

Use the **ping** user and privileged EXEC command to send ISO CLNS echo packets to test the reachability of a remote host over a connectionless OSI network.

clns	CLNS protocol.
host	Host name of system to ping.
address	Address of system to ping.

[**no**] **redistribute** *protocol* [*tag*] [**route-map** *map-tag*]
redistribute {**static** [**clns** | **ip**]}

Use the **redistribute** router configuration command to redistribute routing information from one domain into another routing domain. The **no** form of this command disables redistribution, or disables any of the specified keywords.

protocol — Type of other routing protocol that is to be redistributed as a source of routes into the current routing protocol being configured. The keywords supported are **iso-igrp**, **isis**, and **static** [**clns**].
The keyword **static** [**clns**] is used to redistribute CLNS prefix static routes. This causes the router to inject any static CLNS routes into the domain. The optional **clns** keyword is used when redistributing into IS-IS.

tag — (Optional) Meaningful name for a routing process.

route-map *map-tag* — (Optional) A route map should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported. The argument *map-tag* is the identifier of a configured route map.

static — The keyword **static** is used to redistribute static routes. When used without the optional keywords, this causes the router to inject any OSI static routes into an OSI domain.

clns — (Optional) The **clns** keyword is used when redistributing OSI static routes into an IS-IS domain.

ip — (Optional) The **ip** keyword is used when redistributing IP into an IS-IS domain.

[**no**] **route-map** *map-tag* [[**permit** | **deny**] | *sequence-number*]

Use the **route-map** global configuration command, and the route-map configuration commands **match** and **set**, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which redistribution is allowed for the current **route-map**. The **set** commands specify the *set actions*—the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no** form of this command deletes the route map.

map-tag	Meaningful name for the route map. The **redistribute** command uses this name to reference this route map. Multiple route-maps can share the same map tag name. Can either be an expression or a filter set.
permit	If the match criteria are met for this route map, and **permit** is specified, the route is redistributed as controlled by the set actions. If the match criteria are not met, and **permit** is specified, the next route map with the same map-tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.
deny	If the match criteria are met for the route map, and **deny** is specified, the route is not redistributed, and no further route maps sharing the same map tag name will be examined.
sequence-number	Number that indicates the position a new route map is to have in the list of route maps already configured with the same name. If given with the **no** form of the command, it specifies the position of the route map that should be deleted.

[**no**] **router isis** [*tag*]

Use the **router isis** global configuration command to enable the IS-IS routing protocol on your router and to configure the IS-IS routing process. This command identifies the area the router will work in and lets the router know that it will be routing dynamically rather than statically. The **no** form of this command with the appropriate tag disables IS-IS routing for the system.

tag	(Optional) Meaningful name for a routing process. If it is not specified, a null tag is assumed. The argument *tag* must be unique among all CLNS router processes for a given router. The *tag* argument is used later as a reference to this process.

[**no**] **router iso-igrp** [*tag*]

Use the **router iso-igrp** global configuration command to identify the area the router will work in and let it know that it will be routing dynamically using the ISO-IGRP protocol. The **no** form of this command with the appropriate tag disables ISO-IGRP routing for the system.

tag	(Optional) Meaningful name for a routing process. For example, you could define a routing process named *Finance* for the Finance department, and another routing process named *Marketing* for the Marketing department. If not specified, a null tag is assumed. The *tag* argument must be unique among all CLNS router processes for a given router.

[**no**] **set level** {**level-1** | **level-2** | **level-1-2**}

Use the **set level** route-map configuration command to specify the routing level of routes to be advertised into a specified area of the routing domain. Use the **no** form of this command to disable advertising the specified routing level into a specified area.

level	Redistributed routes are advertised into this specified area of the routing domain. For IS-IS destinations, the default value is **level-2**.
level-1	Inserted in IS-IS Level 1 LSPs.
level-2	Inserted in IS-IS Level 2 LSPs.
level-1-2	Inserted into both Level 1 and Level 2 IS-IS LSPs.

[**no**] **set metric** *metric-value*

Use the **set metric** route-map configuration command to set the metric value to give the redistributed routes.

metric	Metric value to give the redistributed routes. There is no default value.
metric-value	Route metric. This can be an IGRP five-part metric.

[**no**] **set metric-type** {**internal** | **external**}

Use the **set metric-type** route-map configuration command to set the metric type to give redistributed routes.

metric-type	Metric type to give redistributed routes. There is no default value.
internal	IS-IS internal metric.
external	IS-IS external metric.

[**no**] **set tag** *tag-value*

Use **set tag** route-map configuration command to set a tag value to associate with the redistributed routes.

tag Tag value to associate with the redistributed route. If not specified, the default action is to *forward* the tag in the source routing protocol onto the new destination protocol.

tag-value Name for the tag.

show clns

Use the **show clns** EXEC command to display information about the CLNS network.

show clns cache

Use the **show clns cache** EXEC command to display the CLNS routing cache. The cache contains an entry for each destination that has packet switching enabled. The output of this command includes entries showing each destination for which the router has switched a packet in the recent past. This includes the router.

show clns es-neighbors [*type number*] [**detail**]

Use the **show clns es-neighbors** EXEC command to list the ES neighbors (end-system adjacencies) that this router knows about.

type (Optional) Interface type.

number (Optional) Interface unit number.

detail (Optional) When specified, the areas associated with the End Systems are displayed. Otherwise, a summary display is provided.

show clns filter-expr [*name*] [**detail**]

Use the **show clns filter-expr** EXEC command to display one or all currently defined CLNS filter expressions.

name	(Optional) Name of the filter expression to display. If none is specified, all are displayed.
detail	(Optional) When specified, expressions are evaluated down to their most primitive filter set terms before being displayed.

show clns filter-set [*name*]

Use the **show clns filter-set** EXEC command to display one or all currently defined CLNS filter sets.

name	(Optional) Name of the filter set to display. If none is specified, all are displayed.

show clns interface [*type number*]

Use the **show clns interface** EXEC command to list the CLNS-specific information about each interface.

type	(Optional) Interface type.
number	(Optional) Interface unit number.

show clns is-neighbors [*type number*] [**detail**]

Use the **show clns is-neighbors** EXEC command to display IS-IS related information for IS-IS router adjacencies. Neighbor entries are sorted according to the area in which they are located.

type	(Optional) Interface type.
number	(Optional) Interface unit number.
detail	(Optional) When specified, the areas associated with the Intermediate Systems are displayed. Otherwise, a summary display is provided.

show clns neighbors [*type number*] [**detail**]

The **show clns neighbors** EXEC command displays both ES and IS neighbors.

type	(Optional) Interface type.
number	(Optional) Interface unit number.
detail	(Optional) When specified, the area addresses advertised by the neighbor in the hello messages is displayed. Otherwise, a summary display is provided.

show clns protocol [*domain* \| *area-tag*]

Use the **show clns protocol** EXEC command to list the protocol-specific information for each ISO-IGRP routing process in the router. There will always be at least two routing processes, a Level 1 and a Level 2, and there can be more.

domain	(Optional) A particular ISO-IGRP routing domain.
area-tag	(Optional) A particular IS-IS area.

show clns route [*nsap*]

Use the **show clns route** EXEC command to display all of the destinations to which this router knows how to route packets.

The **show clns route** command shows the IS-IS Level 2 routing table as well as static and ISO-IGRP learned prefix routes. This table stores IS-IS area addresses and prefix routes. Destinations are sorted by category.

nsap	(Optional) CLNS Network Service Access Point address.

show clns traffic

Use the **show clns traffic** EXEC command to list the CLNS packets this router has seen.

show isis database [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [*lspid*]

Use the **show isis database** EXEC command to display the IS-IS link state database. A summary display is provided if no options are specified.

level-1	(Optional) Displays the IS-IS link state database for Level 1.
level-2	(Optional) Displays the IS-IS link state database for Level 2.
l1	(Optional) Abbreviation for the option **level-1**.
l2	(Optional) Abbreviation for the option **level-2**.
detail	(Optional) When specified, the contents of each LSP is displayed. Otherwise, a summary display is provided.
lspid	(Optional) Link-state protocol ID (LSPID). Displays the contents of the specified link state packet. The LSPID must be of the form xxxx.xxxx.xxxx.yy-zz or name.yy-zz. For a description of these values, see the table in the “Usage Guidelines” for this command in the *Router Products Command Reference* publication.

show isis routes

Use the **show isis route**s EXEC command to display the IS-IS Level 1 forwarding table for IS-IS learned routes.

show route-map [*map-name*]

Use the **show route-map** EXEC command to display all route-maps configured or only the one specified.

map-name	(Optional) Name of a specific route-map.

[**no**] **timers basic** *update-interval holddown-interval invalid-interval*

Use the **timers basic** router configuration command to configure ISO-IGRP timers. The **no** form of this command restores the default values.

update-interval	Time, in seconds, between the sending of routing updates. The default value is 90 seconds.
holddown-interval	Time, in seconds, a system or area router is kept in holddown state, during which routing information regarding better paths is suppressed. (A router enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.) When the holddown interval expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default value is 145 seconds.
invalid-interval	Time, in seconds, that a route remains in the routing table after it has been determined that it is not reachable. After that length of time, the route is removed from the routing table. The default value is 135 seconds.

trace

You can use the **trace** privileged EXEC command to trace routes on a router configured with the ISO CLNS protocol.

trace clns *destination*

Use the **trace clns** user EXEC command to discover the CLNS routes the router's packets will actually take when traveling to their destination.

destination	Destination address or host name on the command line. The default parameters for the appropriate protocol are assumed and the tracing action begins.

which-route {*nsap-address* \| *clns-name*}

Use the **which-route** EXEC command if you want to know which next-hop router will be used or if you have multiple processes running and want to troubleshoot your configuration. This command displays the routing table in which the specified CLNS destination is found.

nsap-address	CLNS destination network address.
clns-name	Destination host name.

Novell IPX Commands

This chapter describes the function and displays the syntax of each Novell IPX command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **access-list** *access-list-number* {**deny** | **permit**}
source-network[**.***source-nod*e [*source-node-mask*]]
[*destination-network*[**.***destination-node* [*destination-node-mask*]]]

To define a standard IPX access list, use the standard version of the **access-list** global configuration command. To remove a standard access list, use the **no** form of this command.

access-list-number — Number of the access list. This is a decimal number from 800 to 899.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

source-network — Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of 0 matches the local network. A network number of –1 matches all networks.

You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can just enter AA.

source-node (Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

source-node-mask (Optional) Mask to be applied to *source-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

destination-network (Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of 0 matches the local network. A network number of –1 matches all networks.

You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

destination-node (Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

destination-node-mask (Optional) Mask to be applied to *destination-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

[**no**] **access-list** *access-list-number* {**deny** | **permit**} *protocol*
[*source-network*][[[.*source-node*] *source-node-mask*] |
[**.***source-node source-network-mask***.***source-node-mask*]]
[*source-socket*] [*destination.network*][[[**.***destination-node*]
destination-node-mask] | [**.***destination-node*
destination-network-mask.destination-nodemask]]
[*destination-socket*]

To define an extended Novell IPX access list, use the extended version of the **access-list** global configuration command. To remove an extended access list, use the no form of this command.

access-list-number	Number of the access list. This is a decimal number from 900 to 999.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Number of an IPX protocol type, in decimal. This also is sometimes referred to as the packet type. The IPX protocol numbers table in the *Router Products Command Reference* publication lists some IPX protocol numbers.
source-network	(Optional) Number of the network from which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of 0 matches the local network. A network number of –1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can just enter AA.

source-node

(Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

source-network-mask

(Optional) Mask to be applied to *source-network*. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by *source-node-mask*.

source-node-mask

(Optional) Mask to be applied to *source-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

source-socket

Socket number from which the packet is being sent, in hexadecimal. The IPX socket numbers table in the *Router Products Command Reference* publication lists some IPX protocol numbers.

destination-network

(Optional) Number of the network to which the packet is being sent. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of 0 matches the local network. A network number of –1 matches all networks.

You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA.

destination-node (Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

destination-network-mask (Optional) Mask to be applied to *destination-network*. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask. The mask must immediately be followed by a period, which must in turn immediately be followed by *destination-node-mask*.

destination-node-mask (Optional) Mask to be applied to *destination-node*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

destination-socket (Optional) Socket number to which the packet is being sent, in hexadecimal. The IPX socket numbers table in the *Router Products Command Reference* publication lists some IPX socket numbers.

[**no**] **access-list** *access-list-number* {**deny** | **permit**} *network*[**.***node*] [*network***.***node-mask*] [*service-type* [*server-name*]]

To define an access list for filtering Service Advertisement Protocol (SAP) requests, use the SAP filtering form of the **access-list** global configuration command. To remove the access list, use the **no** form of this command.

access-list-number Number of the SAP access list. This is a decimal number from 1000 to 1099.

deny Denies access if the conditions are matched.

permit Permits access if the conditions are matched.

network — Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of 0 matches the local network. A network number of –1 matches all networks.

You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

node — (Optional) Node on *network*. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

*network***.***node-mask* — (Optional) Mask to be applied to *network* and *node*. Place ones in the bit positions to be masked.

service-type — (Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services. The IPX SAP services table in the *Router Products Command Reference* publication lists examples of service types.

server-name — (Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (“ ”) to enclose strings containing embedded spaces. You can use an asterisk (*) at the end of the name as a wildcard to match one or more trailing characters.

[**no**] **area-address** *address mask*

To define a set of network numbers to be part of the current NLSP area, use the **area-address** router configuration command. To remove a set of network numbers from the current NLSP area, use the **no** form of this command.

address	Network number prefix. This is a 32-bit hexadecimal number.
mask	Mask that defines the length of the network number prefix. This is a 32-bit hexadecimal number.

clear ipx accounting [**checkpoint**]

To delete all entries in the accounting database when IPX accounting is enabled, use the **clear ipx accounting** EXEC command. If the keyword is not specified, all entries in the active database are deleted.

checkpoint	(Optional) Clears the checkpointed database.

clear ipx cache

To delete entries from the IPX fast-switching cache, use the **clear ipx cache** EXEC command.

clear ipx nlsp neighbors

To delete all NLSP adjacencies from the router’s adjacency database, use the **clear ipx nlsp neighbors** EXEC command.

clear ipx route [*network* | *****]

To delete routes from the IPX routing table, use the **clear ipx route** EXEC command.

network	(Optional) Number of the network whose routing table entry you want to delete. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can just enter AA.
*****	(Optional) Deletes all routes in the routing table.

clear ipx sse

To have the Cisco 7000 series route processor recompute the entries in the IPX SSE fast-switching cache, use the **clear ipx sse** EXEC command.

clear sse

To reinitialize the route processor on the Cisco 7000 series, use the **clear sse** EXEC command.

[**no**] **distribute-list** *access-list-number* **in** [*interface-name*]

To filter networks received in updates, use the **distribute-list in** router configuration command. To change or cancel the filter, use the **no** form of this command.

access-list-number	Standard IPX access list number in the range 800 to 899. The list explicitly specifies which networks are to be received and which are to be suppressed.
in	Applies the access list to incoming routing updates.

interface-name	(Optional) Interface on which the access list should be applied to incoming updates. If no interface is specified, the access list is applied to all incoming updates.

[**no**] **distribute-list** *access-list-number* **out** [*interface-name* | *routing-process*]

To suppress networks from being advertised in updates, use the **distribute-list out** router configuration command. To cancel this function, use the **no** form of this command.

access-list-number	Standard IPX access list number in the range 800 to 899. The list explicitly specifies which networks are to be sent and which are to be suppressed in routing updates.
out	Applies the access list to outgoing routing updates.
interface-name	(Optional) Interface on which the access list should be applied to outgoing updates. If no interface is specified, the access list is applied to all outgoing updates.
routing-process	(Optional) Name of a particular routing process (**rip** or **eigrp** *autonomous-system-number*).

[**no**] **ipx access-group** *access-list-number*

To apply a generic output filter to an interface, use **ipx access-group** interface configuration command. To remove the access list, use the **no** form of this command.

access-list-number Number of the access list. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, *access-list-number* is a decimal number from 900 to 999.

[**no**] **ipx accounting**

To enable IPX accounting, use the **ipx accounting** interface configuration command. To disable IPX accounting, use the **no** form of this command.

[**no**] **ipx accounting-list** *number mask*

To filter the networks for which IPX accounting information is kept, use the **ipx accounting-list** global configuration command. To remove the filter, use the **no** form of this command.

number Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.

mask Network mask.

[**no**] **ipx accounting-threshold** *threshold*

To set the maximum number of accounting database entries, use the **ipx accounting-threshold** global configuration command. To restore the default, use the **no** form of this command.

threshold	Maximum number of entries (source and destination address pairs) that the router can accumulate. The default is 512.

ip accounting-transits *count*
no ip accounting-transits

To set the maximum number of transit entries that will be stored in the IPX accounting database, use the **ipx accounting-transits** global configuration command. To disable this function, use the **no** form of this command.

count	Number of transit entries that will be stored in the IPX accounting database. The default is 0.

[**no**] **ipx advertise-default-route-only** *network*

To advertise only the default route via the specified network, use the **ipx advertise-default-route-only** interface configuration command. To advertise all known routes out the interface, use the **no** form of this command.

network	Number of the network via which to advertise the RIP default route. This is the only network advertised.

ipx backup-server-query-interval *interval*
no ipx backup-server-query-interval

To change the time between successive queries of each IPX Enhanced IGRP neighbor’s backup server table, use the **ipx backup-server-query-interval** global configuration command. To restore the default time, use the **no** form of this command.

interval	Minimum time, in seconds, between successive queries of each Enhanced IGRP neighbor’s backup server table. The default is 15 seconds.

[**no**] ipx default-route

To forward towards the default network, if known, all packets for which a route to the destination network is unknown, use the **ipx default-route** global configuration command. To discard all packets for which a route to the destination network is unknown, use the **no** form of this command.

ipx delay *ticks*
no ipx delay

To set the tick count, use the **ipx delay** interface configuration command. To reset the default increment in the delay field, use the **no** form of this command.

ticks	Number of IBM clock ticks of delay to use. One clock tick is 1/18th of a second (approximately 55 milliseconds). The default is determined from the delay configured on the interface with the **delay** command. It is (interface delay + 333) / 334.

ipx down *network*
no ipx down

To administratively shut down an IPX network, use the **ipx down** interface configuration command. To restart the network, use the **no** form of this command.

network Number of the network to shut down. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

[**no**] **ipx gns-reply-disable**

To disable the sending of replies to IPX GNS queries, use the **ipx gns-reply-disable** interface configuration command. To return to the default, use the **no** form of this command.

ipx gns-response-delay [*milliseconds*]
no ipx gns-response-delay

To change the delay when responding to Get Nearest Server (GNS) requests, use the **ipx gns-response-delay** global configuration command. To return to the default delay, use the **no** form of this command.

milliseconds (Optional) Time, in milliseconds, that the router waits after receiving a Get Nearest Server request from an IPX client before responding with a server name to that client. The default is zero, which indicates no delay.

[**no**] **ipx gns-round-robin**

To rotate using a round-robin selection method through a set of eligible servers when responding to Get Nearest Server (GNS) requests, use the **ipx gns-round-robin** global configuration command. To use the most recently learned server, use the **no** form of this command.

[**no**] **ipx hello-interval eigrp** *autonomous-system-number seconds*

To configure the interval between IPX Enhanced IGRP hello packets, use the **ipx hello-interval eigrp** interface configuration command. To restore the default interval, use the **no** form of this command.

autonomous-system-number Autonomous system number. It can be a decimal integer from 1 to 65535.

seconds Interval between hello packets, in seconds. The default interval is 5 seconds, which is one-third of the default hold time.

[**no**] **ipx helper-address** *network***.***node*

To forward broadcast packets (except type 20 propagation packets) to a specified server, use the **ipx helper-address** interface configuration command. To disable this function, use the **no** form of this command.

network Network on which the target IPX server resides. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A network number of –1 indicates all-nets flooding. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.

node Node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). A node number of FFFF.FFFF.FFFF matches all servers.

[**no**] **ipx helper-list** *access-list-number*

To assign an access list to an interface to control broadcast traffic (including type 20 propagation packets), use the **ipx helper-list** interface configuration command. To remove the access list from an interface, use the **no** form of this command.

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, it is a decimal number from 900 to 999.

[**no**] **ipx hold-time eigrp** *autonomous-system-number seconds*

To specify the length of time a neighbor should consider IPX Enhanced IGRP hello packets valid, use the **ipx hold-time eigrp** interface configuration command. To restore the default time, use the **no** form of this command.

autonomous-system-number	IPX Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.
seconds	Hold time, in seconds. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The default hold time is 15 seconds, which is three times the hello interval.

[**no**] **ipx input-network-filter** *access-list-number*

To control which networks are added to the router’s routing table, use the **ipx input-network-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

access-list-number Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, it is a decimal number from 900 to 999.

[**no**] **ipx input-sap-filter** *access-list-number*

To control which services are added to the router’s SAP table, use the **ipx input-sap-filter** interface configuration command. To remove the filter, use the **no** form of this command.

access-list-number Number of the SAP access list. All incoming packets are filtered by the entries in this access list. The argument *access-list-number* is a decimal number from 1000 to 1099.

ipx internal-network *network-number*
no internal-network [*network-number*]

To set an internal network number for use by NLSP and IPXWAN, use the **ipx internal-network** global configuration command. To remove an internal network number, use the **no** form of this command.

network-number Number of the internal network.

ipx ipxwan [*local-node* {*network-number* | **unnumbered**}
local-server-name retry-interval retry-limit]
no ipxwan

To configure the IPXWAN protocol on a serial interface, use the **ipx ipxwan** interface configuration command. To disable the IPXWAN protocol, use the **no** form of this command.

local-node

(Optional) Primary network number of the router. This is an IPX network number that is unique across the entire internet. On NetWare 3.*x* servers, the primary network number is called the internal network number. The router with the higher number is determined to be the link master. A value of 0 causes the router to use the configured internal network number.

network-number

(Optional) IPX network number to be used if this router is the one determined to be the link master. The number is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. A value 0 is equivalent to specifying the keyword **unnumbered**.

You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.

unnumbered

(Optional) Specifies that no IPX network number is defined for the link. This is equivalent to specifying a value of 0 for the *network-number* argument.

local-server-name (Optional) Name of the local router. It can be up to 47 characters long, and can contain uppercase letters, digits, underscores (_), hyphens (–), and at signs (@). On NetWare 3.*x* servers, this is the router name. For our routers, this is the name of the router as configured via the **hostname** command (that is, the name that precedes the standard prompt, which is an angle bracket (>) for EXEC mode or a pound sign (#) for privileged EXEC mode).

retry-interval (Optional) Retry interval, in seconds. This interval defines how often the router will retry the IPXWAN startup negotiation if a startup failure occurs. Retries will occur until the retry limit defined by the *retry-limit* argument is reached. It can be a value from 1 through 600. The default is 20 seconds.

retry-limit (Optional) Maximum number of times the router retries the IPXWAN startup negotiation before taking the action defined by the **ipx ipxwan error** command. It can be a value from 1 through 100. The default is 3.

[**no**] **ipx ipxwan error** [**shutdown** | **reset** | **resume**]

To define how to handle IPXWAN when a serial link fails, use the **ipx ipxwan error** interface configuration command. To restore the default, use the **no** form of this command.

reset (Optional) Resets the link when it fails. This is the default action.

resume (Optional) When a link fails, IPXWAN ignores the failure, takes no special action, and resumes the connection.

shutdown (Optional) Shuts down the link when it fails.

[**no**] **ipxwan static**

To negotiate static routes on a link configured for IPXWAN, use the **ipx ipxwan static** interface configuration command. To disable static route negotiation, use the **no** form of this command.

[**no**] **ipx link-delay** *microseconds*

To specify the link delay, use the **ipx link-delay** interface configuration command. To return to the default link delay, which is no delay, use the **no** form of this command.

microseconds Delay, in microseconds. The default is no link delay (a delay of 0).

[**no**] **ipx maximum-hops** *hops*

To set the maximum hop count allowed for IPX packets, use the **ipx maximum-hop** global configuration command. To return to the default number of hops, use the **no** form of this command.

hops Maximum number of hops considered to be reachable by non-RIP routing protocols. Also, maximum number of routers that an IPX packet can traverse before being dropped. It can be a value from 16 through 254. The default is 16 hops.

ipx maximum-paths *paths*
no ipx maximum-paths

To set the maximum number of equal-cost paths the router uses when forwarding packets, use the **ipx maximum-paths** global configuration command. To restore the default value, use the **no** form of this command.

paths Maximum number of equal-cost paths which the router will use. It can be an integer from 1 to 512. The default is 1.

[**no**] **ipx netbios input-access-filter** {**host** | **bytes**} *name*

To control incoming IPX NetBIOS messages, use the **ipx netbios input-access-filter** interface configuration command. To remove the filter, use the **no** form of this command.

host Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.

bytes Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.

name Name of a NetBIOS access list.

[**no**] **ipx netbios output-access-filter** {**host** | **bytes**} *name*

To control outgoing NetBIOS messages, use the **ipx netbios output-access-filter** interface configuration command. To remove the filter, use the **no** form of this command.

host Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.

bytes Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.

name Name of a previously defined NetBIOS access list.

ipx network *number* [**encapsulation** *encapsulation-type* [**secondary**]]
no ipx network *number* [**encapsulation** *encapsulation-type*]

To enable IPX routing on a particular interface and to optionally select the type of encapsulation (framing), use the **ipx network** interface configuration command. To disable IPX routing, use the **no** form of this command.

number	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.

encapsulation *encapsulation-type*

(Optional) Type of encapsulation. It can be one of the following values:

- **arpa** (for Ethernet interfaces only)—Use Novell’s Ethernet_II encapsulation. This encapsulation is recommended for networks that handle both TCP/IP and IPX traffic.
- **hdlc** (for serial interfaces only)—Use HDLC encapsulation.
- **novell-ether** (for Ethernet interfaces only)—Use Novell’s “Ethernet_802.3” encapsulation, which consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by NetWare Version 3.11.
- **sap** (for Ethernet interfaces)—Use Novell’s Ethernet_802.2 encapsulation, which consists of a standard 802.3 MAC header followed by an 802.2 LLC header. This is the default encapsulation used by NetWare Version 4.0.
  (for Token Ring interfaces)—This encapsulation consists of a standard 802.5 MAC header followed by an 802.2 LLC header.
  (for FDDI interfaces)—This encapsulation consists of a standard FDDI MAC header followed by an 802.2 LLC header.
- **snap** (for Ethernet interfaces)—Use Novell Ethernet_Snap encapsulation, which consists of a standard 802.3 MAC header followed by an 802.2 SNAP LLC header.
  (for Token Ring and FDDI interfaces)— This encapsulation consists of a standard 802.5 or FDDI MAC header followed by an 802.2 SNAP LLC header.

secondary (Optional) Indicates an additional (secondary) network configured after the first (primary) network.

[**no**] **ipx nlsp csnp-interval** *seconds*

To configure the NLSP complete sequence number PDU (CSNP) interval, use the **ipx nlsp csnp-interval** interface configuration command. To restore the default value, use the **no** form of this command.

seconds Time, in seconds, between the transmission of CSNPs on multiaccess networks. This interval applies to the designated router only. The interval can be a number in the range 1 to 600. The default is 30 seconds.

[**no**] **ipx nlsp enable**

To enable NLSP routing on the primary network configured on this interface or subinterface, use the **ipx nlsp enable** interface configuration command. To disable NLSP routing on the primary network configured on this interface or subinterface, use the **no** form of this command.

[**no**] **ipx nlsp hello-interval** *seconds*

To configure the interval between the transmission of hello packets, use the **ipx nlsp hello-interval** interface configuration command. To restore the default value, use the **no** form of this command.

seconds Time, in seconds, between the transmission of hello packets on the interface. It can be a decimal integer in the range 1 to 1600. The default is 10 seconds for the designated router and 20 seconds for nondesignated routers.

[**no**] **ipx nlsp metric** *metric-number*

To configure the NLSP cost for an interface, use the **ipx nlsp metric** interface configuration command. To restore the default cost, use the **no** form of this command.

metric-number Metric value for the interface. It can be a decimal integer from 0 to 63. The default varies based on the throughput of the link connected to the interface.

[**no**] **ipx nlsp priority** *priority-number*

To configure the election priority of the specified interface for designated router election, use the **ipx nlsp priority** interface configuration command. To restore the default priority, use the **no** form of this command.

priority-number Election priority of the designated router for the specified interface. This can be a number in the range 0 to 127. This value is unitless. The default is 44.

[**no**] **ipx nlsp retransmit-interval** *seconds*

To configure the link-state packet (LSP) retransmission interval on WAN links, use the **ipx nlsp retransmit-interval** interface configuration command. To restore the default interval, use the **no** form of this command.

seconds LSP retransmission interval, in seconds. This can be a number in the range 1 to 30. The default is 5 seconds.

[**no**] **ipx nlsp rip** [**on** | **off** | **auto**]

To configure RIP compatibility when NLSP is enabled, use the **ipx nlsp rip** interface configuration command. To restore the default, use the **no** form of this command.

on (Optional) Always generates and sends RIP periodic traffic.

off (Optional) Never generates and sends RIP periodic traffic.

auto (Optional) Sends RIP periodic traffic only if another RIP router in sending periodic RIP traffic. This is the default.

[**no**] **ipx nlsp sap** [**on** | **off** | **auto**]

To configure SAP compatibility when NLSP in enabled, use the **ipx nlsp sap** interface configuration command. To restore the default, use the **no** form of this command.

on (Optional) Always generates and sends SAP periodic traffic.

off (Optional) Never generates and sends SAP periodic traffic.

auto (Optional) Sends SAP periodic traffic only if another SAP router in sending periodic SAP traffic. This is the default.

[**no**] **ipx output-gns-filter** *access-list-number*

To control which servers are included in the Get Nearest Server (GNS) responses sent by the router, use the **ipx output-gns-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

access-list-number	Number of the SAP access list. All outgoing GNS packets are filtered by the entries in this access list. The argument *access-list-number* is a decimal number from 1000 to 1099.

[**no**] **ipx output-network-filter** *access-list-number*

To control the list of networks included in routing updates sent out an interface, use the **ipx output-network-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, it is a decimal number from 900 to 999.

ipx output-rip-delay *delay*
no ipx output-rip-delay

To adjust the delay between the individual packets sent in a multiple-packet routing update, use the **ipx output-rip-delay** interface configuration command. To return to the default value, use the **no** form of this command.

delay	Delay, in milliseconds, between packets in a multipacket RIP update. The default delay is 0 (that is, no delay). The delay recommended by Novell is 55 ms.

ipx output-sap-delay *delay*
no ipx output-sap-delay

To set a delay between packets sent in a multipacket Service Advertisement Protocol (SAP) update, use the **ipx output-sap-delay** interface configuration command. To disable the delay mechanism, use the **no** form of this command.

delay	Delay, in milliseconds, between packets in a multipacket SAP update. The default delay is 0 (that is, no delay). The delay recommended by Novell is 55 ms.

[**no**] **ipx output-sap-filter** *access-list-number*

To control which services are included in Service Advertisement Protocol (SAP) updates sent by the router, use the **ipx output-sap-filter** interface configuration command. To remove the filter, use the **no** form of this command.

access-list-number	Number of the SAP access list. All outgoing service advertisements are filtered by the entries in this access list. The argument *access-list-number* is a decimal number from 1000 to 1099.

[**no**] **ipx pad-process-switched-packets**

To control whether odd-length packets are padded so as to be sent as even-length packets on an interface, use the **ipx pad-process-switched-packets** interface configuration command. To disable padding, use the **no** form of this command.

[**no**] **ipx ping-default** {**cisco** | **novell**}

To select the ping type that the router transmits, use the **ipx ping-default** global configuration command. To return to the default ping type, use the **no** form of this command.

cisco	Transmits standard Cisco pings. This is the default.
novell	Transmits standard Novell pings.

[**no**] **ipx rip-max-packetsize** *bytes*

To configure the maximum packet size of RIP updates sent out the interface, use the **ipx rip-max-packetsize** interface configuration command. To restore the default packet size, use the **no** form of this command.

bytes	Maximum packet size in bytes. The default is 432 bytes, which allows for 50 routes at 8 bytes each plus a 32-byte IPX RIP header.

[**no**] **ipx rip-multiplier** *multiplier*

To configure the interval at which a network's or server's RIP entry ages out, use the **ipx rip-multiplier** interface configuration command. To restore the default interval, use the **no** form of this command.

multiplier	Multiplier used to calculate the interval at which to age out RIP routing table entries. This can be any positive integer. The value you specify is multiplied by the RIP update interval to determine the aging-out interval. The default is three times the RIP update interval.

ipx route {*network* | **default**} *network***.***node* [**floating-static**]
no ipx route

To add a static route to the routing table, use the **ipx route** global configuration command. To remove a route from the routing table, use the **no** form of this command.

network — Network to which you want to establish a static route.

This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can just enter AA.

default — Default network number as defined by the **ipx default-route** global configuration command.

*network***.***node* — Router to which to forward packets destined for the specified network.

The argument *network* is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.

The argument *node* is the node number of the target router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

floating-static — (Optional) Specifies that this route is a floating-static route. This is a static route that can be overridden by a dynamically learned route.

[**no**] **ipx route-cache** [**cbus** | **sse**]

To enable IPX fast switching and autonomous switching, use the **ipx route-cache** interface configuration command. To disable fast switching, use the **no** form of this command. If no keywords are specified, fast switching is enabled. By default, fast switching is enabled, and autonomous switching and SSE switching are disabled.

cbus	(Optional) Enables IPX autonomous switching.
sse	(Optional) Enables SSE fast switching.

ipx router {**eigrp** *autonomous-system-number* | **nlsp** | **rip**}

To specify the routing protocol to use, use the **ipx router** global configuration command.

eigrp *autonomous-system-number*	Enables the Enhanced IGRP routing protocol. The argument *autonomous-system-number* is the IPX Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.
nlsp	Enables the NLSP routing protocol.
rip	Enables the RIP routing protocol. It is on by default.

ipx router-filter *access-list-number*
no ipx router-filter

To control the routers from which packets are accepted, use the **ipx router-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

access-list-number Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, it is a decimal number from 900 to 999.

[**no**] **ipx router-sap-filter** *access-list-number*

To filter Service Advertisement Protocol (SAP) messages received from a particular router, use the **ipx router-sap-filter** interface configuration command. To remove the filter, use the **no** form of this command.

access-list-number Number of the access list. All incoming service advertisements are filtered by the entries in this access list. The argument *access-list-number* is a decimal number from 1000 to 1099.

ipx routing [*node*]
no ipx routing

To enable IPX routing, use the **ipx routing** global configuration command. To disable IPX routing, use the **no** form of this command.

node (Optional) Node number of the router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). It must not be a multicast address.

If you omit *node*, the router uses the hardware MAC address currently assigned to it as its node address. This is the MAC address of the first Ethernet, Token Ring, or FDDI interface card. If no satisfactory interfaces are present in the router (such as only serial interfaces), you must specify *node*.

[**no**] **ipx sap** *service-type name network***.***node socket hop-count*

To specify static Service Advertisement Protocol (SAP) entries, use the **ipx sap** global configuration command. To remove static SAP entries, use the **no** form of this command.

service-type SAP service-type number. The sample IPX SAP services table in the *Router Products Command Reference* lists some IPX SAP services.

name Name of the server that provides the service.

*network***.***node* Network number and node address of the server.

The argument *network* is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter just AA.

The argument *node* is the node number of the target Novell server. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

socket Socket number for this service. The IPX socket numbers table in the *Router Products Command Reference* publication lists some IPX socket numbers.

hop-count Number of hops to the server.

[**no**] **ipx sap-incremental** [**eigrp** *autonomous-system-number*] [**rsup-only**]

To send SAP updates only when a change occurs in the SAP table, use the **ipx sap-incremental eigrp** interface configuration command. To send periodic SAP updates, use the **no** form of this command.

autonomous-system-number (Optional) IPX Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.

rsup-only (Optional) Indicates that the system uses Enhanced IGRP on this interface to carry reliable SAP update information only. RIP routing updates are used, and Enhanced IGRP routing updates are ignored.

ipx sap-interval *interval*
no ipx sap-interval

To configure less frequent Service Advertisement Protocol (SAP) updates over slow links, use the **ipx sap-interval** interface configuration command. To return to the default value, use the **no** form of this command.

interval Interval, in minutes, between SAP updates sent by the router. The default value is 1 minute. If *interval* is 0, periodic updates are never sent.

[**no**] **ipx sap-max-packetsize** *bytes*

To configure the maximum packet size of SAP updates sent out the interface, use the **ipx sap-max-packetsize** interface configuration command. To restore the default packet size, use the **no** form of this command.

bytes Maximum packet size in bytes. The default is 480 bytes, which allows for seven servers (64 bytes each) plus a 32-byte IPX SAP header.

[**no**] **ipx sap-multiplier** *multiplier*

To configure the interval at which a network's or server's SAP entry ages out, use the **ipx sap-multiplier** interface configuration command. To restore the default interval, use the **no** form of this command.

multiplier Multiplier used to calculate the interval at which to age out SAP routing table entries. This can be any positive integer. The value you specify is multiplied by the SAP update interval to determine the aging-out interval. The default is three times the SAP update interval.

ipx sap-queue-maximum *number*
no ipx sap-interval

To configure the maximum length of the queue of pending input SAP GNS requests and SAP query packets, use the **ipx sap-queue-maximum** global configuration command. To return to the default value, use the **no** form of this command.

number Maximum length of the queue of pending SAP requests. By default, there is no limit to the number of pending SAP requests that the router stores in this queue.

[**no**] **ipx source-network-update**

To repair corrupted network numbers, use the **ipx source-network-update** interface configuration command. To disable this feature, use the **no** form of this command.

[**no**] **ipx split-horizon eigrp** *autonomous-system-number*

To configure split horizon, use the **ipx split-horizon eigrp** interface configuration command. To disable split horizon, use the **no** form of this command.

autonomous-system-number IPX Enhanced IGRP autonomous system number. It can be a decimal integer from 1 to 65535.

[**no**] **ipx throughput** *bits-per-second*

To configure the throughput, use the **ipx throughput** interface configuration command. To restore the default throughput, use the **no** form of this command.

bits-per-second Throughput, in bits per second. No default throughput is defined.

[**no**] **ipx type-20-helpered**

To forward IPX type 20 propagation packet broadcasts to specific network segments, use the **ipx type-20-helpered** interface configuration command. To disable this function, use the **no** form of this command.

[**no**] **ipx type-20-input-checks**

To restrict the acceptance of IPX type 20 propagation packet broadcasts, use the **ipx type-20-input-checks** global configuration command. To remove these restrictions, use the **no** form of this command.

[**no**] **ipx type-20-output-checks**

To restrict the forwarding of IPX type 20 propagation packet broadcasts, use the **ipx type-20-output-checks** global configuration command. To remove these restrictions, use the **no** form of this command.

[**no**] **ipx type-20-propagation**

To forward IPX type 20 propagation packet broadcasts to other network segments, use the **ipx type-20-propagation** interface configuration command. To disable both the reception and forwarding of type 20 broadcasts on an interface, use the **no** form of this command.

ipx update-time *interval*
no ipx update-time

To adjust the IPX routing update timers, use the **ipx update-time** interface configuration command. To restore the default value, use the **no** form of this command.

interval	Interval, in seconds, at which IPX routing updates are sent. The default is 60 seconds. The minimum interval is 10 seconds.

[**no**] **ipx watchdog-spoof**

To have the router respond to a server's watchdog packets on behalf of a remote client, use the **ipx watchdog-spoof** interface configuration command. To disable spoofing, use the **no** form of this command.

[**no**] **lsp-gen-interval** *seconds*

To set the minimum interval at which link-state packets (LSPs) are generated, use the **lsp-gen-interval** router configuration command. To restore the default interval, use the **no** form of this command.

seconds	Minimum interval, in seconds. It can be a number in the range 0 through 120. The default is 5 seconds.

[**no**] **lsp-mtu** *bytes*

To set the maximum size of a link-state packet (LSP), use the **lsp-mtu** router configuration command. To restore the default MTU size, use the **no** form of this command.

bytes	MTU size, in bytes. It can be a decimal number in the range 512 through 4096. The default is 512 bytes.

[**no**] **lsp-refresh-interval** *seconds*

To set the link-state packet (LSP) refresh interval, use the **lsp-refresh-interval** router configuration command. To restore the default refresh interval, use the **no** form of this command.

seconds	Refresh interval, in seconds. It can be a value in the range 1 through 50000 seconds. The default is 7200 seconds.

[**no**] **max-lsp-lifetime** *seconds*

To set the maximum time that link-state packets (LSPs) persist, use the **max-lsp-lifetime** router configuration command. To restore the default time, use the **no** form of this command.

seconds	Lifetime of LSP, in seconds. It can be a number in the range 1 through 50000 seconds. The default is 7500 seconds.

[**no**] **netbios access-list host** *name* {**deny** | **permit**} *string*
[**no**] **netbios access-list bytes** *name* {**deny** | **permit**} *offset byte-pattern*

To define an IPX NetBIOS access list filter, use the **netbios access-list** interface configuration command. To remove a filter, use the **no** form of the command.

host — Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list host** commands.

bytes — Indicates that the following argument is the name of a NetBIOS access filter previously defined with one or more **netbios access-list bytes** commands.

name — Name of the access list being defined. The name can be an alphanumeric string.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

string — Character string that identifies one or more NetBIOS host names. It can be up to 14 characters long. The argument *string* can include the following wildcard characters:

- *—Match one or more characters. You can use this wildcard character only at the end of a string.
- ?—Match any single character.

offset	Decimal number that indicates the number of bytes into the packet at which the byte comparison should begin. An offset of 0 indicates the beginning of the NetBIOS packet header, which is at the end of the IPX header.
byte-pattern	Hexadecimal pattern that represents the byte pattern to match. It can be up to 16 bytes (32 digits) long and must be an even number of digits. The argument *byte-pattern* can include the following wildcard character: • **—Match any digits for that byte.

[**no**] **network** {*network-number* | **all**}

To enable IPX Enhanced IGRP on the router, use the **network** IPX-router configuration command. To disable IPX Enhanced IGRP on the router, use the **no** form of this command.

network-number	IPX network number.
all	Enables the routing protocol for all IPX networks configured on the router.

ping [**ipx**] [*address*]

To check host reachability and network connectivity, use the **ping** privileged EXEC command.

ipx	(Optional) Specifies the IPX protocol.
address	(Optional) Address of system to ping.

ping ipx {*host* | *address*}

To check host reachability and network connectivity, use the **ping ipx** user EXEC command.

ipx	Specifies the IPX protocol.

host	Host name of system to ping.
address	Address of system to ping.

[**no**] **redistribute** {**rip** | **eigrp** *autonomous-system-number* | **connected** | **static** | **floating-static**}

To redistribute from one routing domain into another, and vice versa, use the **redistribute** IPX-router configuration command. To disable this feature, use the **no** form of this command.

rip	Specifies the RIP protocol.
eigrp *autonomous-system-number*	Specifies the Enhanced IGRP protocol and the autonomous system number. It can be a decimal integer from 1 to 65535.
connected	Specifies connected routes.
static	Specifies static routes.
floating-static	Specifies a floating static route. This is a static route that can be overridden by a dynamically learned route.

show ipx accounting [**checkpoint**]

To display the active accounting or checkpointed database, use the **show ipx accounting** EXEC command.

checkpoint	(Optional) Displays entries in the checkpointed database.

show ipx cache

To display the contents of the IPX fast-switching cache, use the **show ipx cache** EXEC command.

show ipx eigrp neighbors [**servers**] [*autonomous-system-number* | *interface*]

To display the neighbors discovered by Enhanced IGRP, use the **show ipx eigrp neighbors** EXEC command.

servers	(Optional) Displays the server list advertised by each neighbor. This is displayed only if the **ipx sap incremental** command is enabled on the interface on which the neighbor resides.
autonomous-system-number	(Optional) Autonomous system number. It can be a decimal integer from 1 to 65535.
interface	(Optional) Interface type and number.

show ipx eigrp topology [*network-number*]

To display the IPX enhanced IGRP topology table, use the **show ipx eigrp topology** EXEC command.

network-number	(Optional) IPX network number whose topology table entry to display

show ipx interface [*type number*]

To display the status of the IPX interfaces configured in the router and the parameters configured on each interface, use the **show ipx interface** privileged EXEC command.

type	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), FDDI, loopback, null, serial, Token Ring, or tunnel.
number	(Optional) Interface number.

show ipx nlsp database [*lspid*] [**detail**]

To display the entries in the link-state packet (LSP) database, use the **show ipx nlsp database** EXEC command.

lspid	(Optional) Link-state protocol ID (LSPID). You must specify this in the format *xxxx.xxxx.xxxx.yy-zz* or *name.yy-zz*.
detail	(Optional) Displays the contents of the LSP database entries. If you omit this keyword, only a summary display is shown.

show ipx nlsp neighbors [*interface*] [**detail**]

To display the router's NLSP neighbors and their states, use the **show ipx nlsp neighbors** EXEC command.

interface	(Optional) Interface type and number.
detail	(Optional) Displays detailed information about the neighbor. If you omit this keyword, only a summary display is shown.

show ipx route [*network*] [**default**] [**detailed**]

To display the contents of the IPX routing table, use the **show ipx route** user EXEC command.

network	(Optional) Number of the network whose routing table entry you want to display. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can just enter AA.
default	(Optional) Displays the default route.
detailed	(Optional) Displays detailed route information.

show ipx servers [**sorted** [**name** | **net** | **type**]]

To list the IPX servers discovered through SAP advertisements, use the **show ipx servers** user EXEC command.

unsorted	(Optional) Does not sort entries when displaying IPX servers.
sorted	(Optional) Sorts the display of IPX servers according to the keyword that follows.
name	(Optional) Displays the IPX servers alphabetically by server name.
net	(Optional) Displays the IPX servers numerically by network number.
type	(Optional) Displays the IPX servers numerically by SAP service type. This is the default.

show ipx traffic

To display information about the number and type of IPX packets transmitted and received by the router, use the **show ipx traffic** user EXEC command.

[**no**] **spf-interval** *seconds*

To control how often the router performs the Shortest Path First (SPF) calculation, use the **spf-interval** router configuration command. To restore the default interval, use the **no** form of this command.

seconds	Minimum amount of time between Shortest Path First (SPF) calculations, in seconds. It can be a number in the range 1 through 120. The default is 5 seconds.

XNS Commands

This chapter describes the function and displays the syntax of each XNS command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

access-list *access-list-number* {**deny** | **permit**}
source-network[**.***source-address* [*source-address-mask*]]
[*destination-network*[**.***destination-address*
[*destination-address-mask*]]]
no access-list *access-list-number*

To define a standard XNS access list, use the standard version of the **access-list** global configuration command. To remove a standard access list, use the **no** form of this command.

access-list-number	Number of the access list. This is a decimal number from 400 to 499.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

source-network Number of the network from which the packet is being sent. This is a 32-bit decimal number. You can omit leading zeros. A network number of –1 matches all networks.

Note that you enter the network number in decimal, and this number is expressed in decimal format in our configuration files and routing tables. However, the router internally converts the network number into hexadecimal. Network analyzers also display the network number in hexadecimal.

source-address (Optional) Host on *source-network* from which the packet is being sent. This is a 48-bit hexadecimal value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

source-address-mask (Optional) Mask to be applied to *source-address*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

destination-network (Optional) Number of the network to which the packet is being sent. This is a 32-bit decimal number. A network number of –1 matches all networks.

You can omit leading zeros from the network number.

Note that you enter the network number in decimal, and this number is expressed in decimal format in our configuration files and routing tables. However, the router internally converts the network number into hexadecimal. Network analyzers also display the network number in hexadecimal.

destination-address (Optional) Host on *destination-network* to which the packet is being sent. This is a 48-bit hexadecimal value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

destination-address-mask (Optional) Mask to be applied to *destination-address*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

[**no**] **access-list** *access-list-number* {**deny** | **permit**} *protocol*
[*source-network*[**.***source-host*
[*source-network-mask.*]*source-host-mask*] *source-socket*
[*destination-network* [**.***destination-host*
[*destination-network-mask.destination-host-mask*]
destination-socket[/**pep**]]]

To define an extended XNS access list, use the extended version of the **access-list** global configuration command. To remove an extended access list, use the **no** form of this command.

access-list-number Number of the access list. This is a decimal number from 500 to 599.

deny Denies access if the conditions are matched.

permit Permits access if the conditions are matched.

protocol Number of an XNS protocol, in decimal. See the documentation accompanying your host's XNS implementation for a list of protocol numbers.

source-network (Optional) Number of the network from which the packet is being sent. This is a 32-bit decimal number. A network number of –1 matches all networks.

You can omit leading from the network number.

Note that you enter the network number in decimal, and this number is expressed in decimal format in our configuration files and routing tables. However, the router internally converts the network number into hexadecimal. This means, for instance, that a network analyzer will display the network number in hexadecimal.

source-host
(Optional) Host on *source-network* from which the packet is being sent. This is a 48-bit hexadecimal value represented as a dotted triplet of 4-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

source-network-mask
(Optional) Mask to be applied to *source-network*. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask.

The mask must immediately be followed by a period, which must in turn immediately be followed by *source-host-mask*.

source-host-mask
(Optional) Mask to be applied to *source-host*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

source-socket
Number of the socket from which the packet is being sent. This is a 16-bit decimal value. See the documentation accompanying your host's XNS implementation for a list of socket numbers.

destination-network (Optional) Number of the network to which the packet is being sent. This is a 32-bit decimal number. A network number of –1 matches all networks.

You can omit leading zeros from the network number.

Note that you enter the network number in decimal, and this number is expressed in decimal format in our configuration files and routing tables. However, the router internally converts the network number into hexadecimal. This means, for instance, that a network analyzer will display the network number in hexadecimal.

destination-host (Optional) Host on *destination-network* to which the packet is being sent. This is a 48-bit hexadecimal value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

destination-network-mask (Optional) Mask to be applied to *destination-network*. This is an eight-digit hexadecimal mask. Place ones in the bit positions you want to mask.

The mask must immediately be followed by a period, which must in turn immediately be followed by *destination-host-mask*.

destination-host-mask (Optional) Mask to be applied to *destination-host*. This is a 48-bit value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). Place ones in the bit positions you want to mask.

destination-socket	(Optional) Number of the socket to which the packet is being sent. This is a 16-bit decimal value. See the documentation accompanying your host's XNS implementation for a list of socket numbers.
pep	(Optional) Packet Exchange Protocol type. PEP is a connectionless-oriented protocol that uses XNS Type 4 IDP frames.

ping xns *address*

To check host reachability and network connectivity, use the **ping** user EXEC command.

xns	Specifies the XNS protocol.
address	Address of system to ping.

ping

To check host reachability and network connectivity, use the **ping** privileged EXEC command.

show xns cache

To display the contents of the XNS fast-switching cache, use the **show xns cache** EXEC command.

show xns interface [*type number*]

To display the status of the XNS interfaces configured in the router and the parameters configured on each interface, use the **show xns interface** EXEC command.

type	(Optional) Interface type. It can be one of the following types: asynchronous, dialer, Ethernet (IEEE 802.3), loopback, null, serial, or tunnel.
number	(Optional) Interface number.

show xns route [*network*]

To display the contents of the XNS routing table, use the **show xns route** EXEC command.

network	(Optional) Number of the network that the route is to. This is a 32-bit decimal number. You can omit leading zeros.

show xns traffic

To display information about the number and type of XNS packets transmitted and received by the router, use the **show xns traffic** EXEC command.

[**no**] **xns access-group** *access-list-number*

To apply a generic filter to an interface, use the **xns access-group** interface configuration command. To remove the access list, use the **no** form of this command.

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 400 to 499. For extended access lists, *access-list-number* is a decimal number from 500 to 599.

[**no**] **xns encapsulation** {**snap** | **ub** | **3com**}

To select the type of encapsulation used on a Token Ring interface, use the **xns encapsulation** interface configuration command. To disable the encapsulation, use the **no** form of this command.

snap	802.2 LLC encapsulation. This is the default encapsulation type. Use this encapsulation type with IBM Token Ring networks.
ub	Ungermann-Bass encapsulation.
3com	3Com encapsulation. Use this encapsulation type when older 3Com Corporation products are present on the network.

[**no**] **xns flood broadcast allnets**

To flood broadcast packets whose destination address is –1.FFFF.FFFF.FFFF, use the **xns flood broadcast allnets** interface configuration command. To disable this type of flooding, use the **no** form of this command.

[**no**] **xns flood broadcast net-zero**

To flood packets whose destinations address is 0.FFFF.FFFF.FFFF, use the **xns flood broadcast net-zero** interface configuration command. To disable this type of flooding, use the **no** form of this command.

[**no**] **xns flood specific allnets**

To flood packets whose destination address is –1.*specific-host*, use the **xns flood specific allnets** interface configuration command. To disable this type of flooding, use the **no** form of this command.

[**no**] **xns forward-protocol** *protocol*

To forward packets of a specific XNS protocol to a helper address, use the **xns forward-protocol** global configuration command. To disable the forwarding of these packets, use the **no** form of this command.

protocol	Number of an XNS protocol, in decimal. See the documentation accompanying your host's XNS implementation for a list of protocol numbers.

xns hear-rip [*access-list-number*]
no xns hear-rip

To receive RIP updates, use the **xns hear-rip** interface configuration command. To disable the receipt of RIP updates, use the **no** form of this command.

access-list-number	(Optional) Number of the access list. This list defines the routes the router is to learn through standard RIP. The list is applied to individual routes within the RIP packet, not to the address of the packet's sender. For standard access lists, *access-list-number* is a decimal number from 400 to 499. For extended access lists, *access-list-number* is a decimal number from 500 to 599.

[**no**] **xns helper-address** *network***.***host*

To forward broadcast packets to a specified server, use the **xns helper-address** interface configuration command. To disable this function, use the **no** form of this command.

network Network on which the target XNS server resides. This is a 32-bit decimal number.

host Host number of the target XNS server. This is a 48-bit hexadecimal value represented as a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). The host must be directly connected to one of the router's directly attached networks. A number of FFFF.FFFF.FFFF indicates all hosts on the specified network.

[**no**] **xns input-network-filter** *access-list-number*

To control which networks are added to the routing table, use the **xns input-network-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

access-list-number Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 400 to 499. For extended access lists, it is a decimal number from 500 to 599.

xns maximum-paths *number*
no xns maximum-paths

To set the maximum number of paths the router uses when sending packets, use the **xns maximum-paths** global configuration command. To restore the default value, use the **no** form of this command.

number	Maximum number of equal-cost paths from which the router chooses. It can be a number from 1 to 512. The default is 1.

xns network *number*
no xns network

To enable XNS routing on a particular interface by assigning a network number to the interface, use the **xns network** interface configuration command. To disable XNS routing on an interface, use the **no** form of this command.

number	Network number. This is a 32-bit decimal number. You can omit leading zeros.

[**no**] **xns output-network-filter** *access-list-number*

To control the list of networks included in routing updates sent out an interface, use the **xns output-network-filter** interface configuration command. To remove the filter from the interface, use the **no** form of this command.

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 400 to 499. For extended access lists, it is a decimal number from 500 to 599.

[**no**] **xns route** *network network.host*

To add a static route to the XNS routing table, use the **xns route** global configuration command. To remove a route from the routing table, use the **no** form of this command.

network — Network to which you want to establish a static route. This is a 32-bit decimal number. You can omit leading zeros.

network.host — Router to which to forward packets destined for the specified network.

The argument *network* is a 32-bit decimal number. You can omit leading zeros.

The argumen*t host* is the host number of the target router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*).

[**no**] **xns route-cache**

To enable XNS fast switching, use the **xns route-cache** interface configuration command. To disable fast switching, use the **no** form of this command.

[**no**] **xns router-filter** *access-list-number*

To control the routers from which packets are accepted, use the **xns router-filter** interface configuration command. To remove the filters from the interface, use the **no** form of this command.

access-list-number — Number of the access list. All incoming packets defined with either standard or extended access lists are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 400 to 499. For extended access lists, it is a decimal number from 500 to 599.

xns routing [*address*]
no xns routing

To enable XNS routing, use the **xns routing** global configuration command. To disable XNS routing, use the **no** form of this command.

address	(Optional) Host number of the router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers (*xxxx.xxxx.xxxx*). It must not be a multicast address. If you omit *address*, the router uses the address of the first IEEE-compliant (Token Ring, FDDI, or Ethernet) interface MAC address it finds in its interface list. The router uses the address 0123.4567.abcd for non-IEEE–compliant interfaces.

[**no**] **xns ub-emulation**

To enable Ungermann-Bass Net/One routing, use the **xns ub-emulation** global configuration command. To disable Net/One routing and restore standard routing mode, use the **no** form of this command.

xns update-time *interval*
no xns update-time

To set the XNS routing update timers, use the **xns update-time** interface configuration command. To restore the default value, use the **no** form of this command.

interval	Interval, in seconds, at which XNS routing updates are sent. The minimum interval is 10 seconds, and the maximum is 2,493,644 seconds, which is about 29 days. The default is 30 seconds.

Transparent Bridging Commands

This chapter describes the function and displays the syntax of transparent bridging commands. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

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

Use the **access-list** global configuration command to establish MAC address access lists. Use the **no** form of this command to remove a single access list entry.

access-list-number	Integer from 700 to 799 that you select for the list.
permit	Permits the frame.
deny	Denies the frame.
address mask	48-bit MAC addresses written in dotted triplet form. The ones bits in the *mask* argument are the bits to be ignored in *address*.

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

Use the **access-list** global configuration command to provide extended access lists that allow finer granularity of control. These lists allow you to specify both source and destination addresses and arbitrary bytes in the packet.

access-list-number — Integer from 1100 through 1199 that you assign to identify one or more **permit**/**deny** conditions as an extended access list. Note that a list number in the range 1100 through 1199 distinguishes an extended access list from other access lists.

permit — Allows a connection when a packet matches an access condition. The router stops checking the extended access list after a match occurs. All conditions must be met to make a match.

deny — Disallows a connection when a packet matches an access condition. The router stops checking the extended access list after a match occurs. All conditions must be met to make a match.

source — MAC Ethernet address in the form *xxxx.xxxx.xxxx*.

source-mask — Mask of MAC Ethernet source address bits to be ignored. The router uses the *source* and *source-mask* arguments to match the source address of a packet.

destination — MAC Ethernet value used for matching the destination address of a packet.

destination-mask — Mask of MAC Ethernet destination address bits to be ignored. The router uses the *destination* and *destination-mask* arguments to match the destination address of a packet.

offset — Range of values that must be satisfied in the access list. Specified in decimal or in hexadecimal format in the form 0x*nn*. The offset is the number of bytes from the destination address field; it is not an offset from the start of the packet. The number of bytes you need to offset from the destination address varies depending on the media encapsulation type you are using.

size — Range of values that must be satisfied in the access list. Must be an integer 1 through 4.

operator — Compares arbitrary bytes within the packet. Can be one of the following keywords:

lt—less than

gt—greater than

eq—equal

neq—not equal

and—bitwise and

xor—bitwise exclusive or

nop—address match only

operand — Compares arbitrary bytes within the packet. The value to be compared to or masked against.

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

Use the **access-list** global configuration command to build type-code access lists. Use the **no** form of this command to remove a single access list entry.

access-list-number — User-selectable number between 200 and 299 that identifies the list.

permit — Permits the frame.

deny Denies the frame.

type-code 16-bit hexadecimal number written with a leading “0x”; for example, 0x6000. You can specify either an Ethernet type code for Ethernet-encapsulated packets, or a DSAP/SSAP pair for 802.3 or 802.5-encapsulated packets. Ethernet type codes are listed in the appendix “Ethernet Type Codes” in the *Router Products Command Reference* publication.

wild-mask 16-bit hexadecimal number whose ones bits correspond to bits in the *type-code* argument that should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be at least 0x0101. This is because these two bits are used for purposes other than identifying the SAP codes.)

[**no**] **bridge** *bridge-group* **acquire**

Use the **bridge acquire** global configuration command to use the system default behavior of forwarding any frames for stations that it has learned about dynamically. Use the **no** form of this command to change the default behavior.

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

bridge *bridge-group* **address** *mac-address* {**forward** | **discard**}
[*interface*]
no bridge *bridge-group* **address** *mac-address*

Use the **bridge address** global configuration command to filter frames with a particular MAC layer station source or destination address. Use the **no** form of this command followed by the MAC address to disable the forwarding ability.

bridge-group — Group number you assigned to the spanning tree. Must be the same as that specified in the **bridge protocol** command.

mac-address — 48-bit dotted-triplet hardware address such as that displayed by the EXEC **show arp** command, for example, 0800.cb00.45e9. It is either a station address, the broadcast address, or a multicast destination address.

forward — Frame sent from or destined to the specified address is forwarded as appropriate.

discard — Frame sent from or destined to the specified address is discarded without further processing.

interface — (Optional) Interface specification, such as Ethernet 0. It is added after the **forward** keyword to indicate the interface on which that address can be reached.

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

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

bridge-group	Number of the bridge group to which the interface belongs.
circuit-group	Number of the circuit group to which the interface belongs.
milliseconds	Forward delay interval. It must be a value in the range 0 through 10000 milliseconds.

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

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

bridge-group	Number of the bridge group to which the interface belongs.
circuit-group	Number of the circuit group to which the interface belongs.

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

Use the **bridge domain** global configuration command to establish a domain by assigning it a decimal value between 1 and 10. Use the **no** form of this command to return to the default single bridge domain.

bridge-group Bridge group number specified in the **bridge protocol ieee** command. The **dec** keyword is not valid for this command.

domain-number Domain number you choose. The default domain number is zero; this is the domain number required when communicating to IEEE bridges that do not support this domain extension.

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

Use the **bridge forward-time** global configuration command to specify the forward delay interval for the router. Use the **no** form of this command to return the default interval.

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

seconds Forward delay interval. It must be a value in the range 10 through 200 seconds. The default is 30 seconds.

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

Use the **bridge hello-time** global configuration command to specify the interval between Hello Bridge Protocol Data Units (BPDUs). Use the **no** form of this command to return the default interval.

bridge-group	Bridge group number specified in the **bridge protocol** command.
seconds	Any value between 1 and 10 seconds. The default is 1 second.

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

Use the **bridge lat-service-filtering** global configuration command to specify LAT group-code filtering. Use the **no** form of this command to disable the use of LAT service filtering on the bridge group.

bridge-group	Bridge group in which this special processing is to take place.

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

Use the **bridge max-age** global configuration command to change the interval the bridge will wait to hear BPDUs from the root bridge. If a bridge does not hear BPDUs from the root bridge within this specified interval, it assumes that the network has changed and will recompute the spanning-tree topology. Use the **no** form of this command to return the default interval.

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

[**no**] **bridge** *bridge-group* **multicast-source**

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

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

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

Use the **bridge priority** global configuration command to configure the priority of an individual bridge, or the likelihood that it will be selected as the root bridge.

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

number The lower the number, the more likely the bridge will be chosen as root. When the IEEE spanning-tree protocol is enabled on the router, *number* ranges from 0 through 65535; the default is 32768. When the Digital spanning-tree protocol is enabled, *number* ranges from 0 through 255; the default is 128.

[**no**] **bridge** *bridge-group* **protocol** {**ieee** | **dec**}

Use the **bridge protocol** global configuration command to define the type of spanning-tree protocol. Use the **no** form of this command, with the appropriate keywords and arguments, to delete the specified bridge group.

bridge-group Number in the range 1 through 9 that you choose to refer to a particular set of bridged interfaces. Frames are bridged only among interfaces in the same group.

ieee IEEE Ethernet spanning-tree protocol.

dec Digital spanning-tree protocol.

[**no**] **bridge-group** *bridge-group*

Use the **bridge-group** interface configuration command to assign each network interface to a bridge group. Use the **no** form of this command to remove the interface from the bridge group.

bridge-group	Number of the bridge group to which the interface belongs. The value must be in the range 1 through 9.

[**no**] **bridge-group** *bridge-group* **aging-time** *seconds*

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

bridge-group	Number of the bridge group to which the interface belongs.
seconds	Aging-time interval, in the range 0 to 1000000 seconds.

[**no**] **bridge-group** *bridge-group* **cbus-bridging**

Use the **bridge-group cbus-bridging** interface configuration command to enable autonomous bridging on a ciscoBus II-resident interface. Use the **no** form of this command to disable autonomous bridging.

bridge-group	Number of the bridge group to which the interface belongs.

[**no**] **bridge-group** *bridge-group* **circuit-group** *circuit-group*

Use the **bridge-group circuit-group** interface configuration command to assign each network interface to a group. Use the **no** form of this command to remove the interface from the bridge group.

bridge-group	Number of the bridge group to which the interface belongs.
circuit-group	Circuit group number. The range is 1 through 9.

bridge-group *bridge-group* **input-address-list**
no bridge-group *bridge-group* **input-address-list** *access-list-number*

Use the **bridge-group input-address-list** interface configuration command to assign an access list to a particular interface. This access list is used to filter packets received on that interface based on their MAC source addresses. Use the **no** form of this command to remove an access list from an interface.

bridge-group	Bridge group number defined by the **bridge-group** command. It must be in the range 1 through 9.
access-list-number	Access list number you assigned with the bridge **access-list** command. It must be in the range 700 through 799.

[**no**] **bridge-group** *bridge-group* **input-lat-service-deny** *group-list*

Use the **bridge-group input-lat-service-deny** interface configuration command to specify the group codes by which to deny access upon input. Use the **no** form of this command to remove this access condition.

bridge-group	Bridge group number defined by the **bridge-group** command. It must be a value in the range 1 through 9.
group-list	List of LAT service groups. Single numbers and ranges are permitted. Specify a zero (0) to disable the LAT group code for the bridge group.

[**no**] **bridge-group** *bridge-group* **input-lat-service-permit** *group-list*

Use the **bridge-group input-lat-service-permit** interface configuration command to specify the group codes by which to permit access upon input. Use the **no** form of this command to remove this access condition.

bridge-group	Bridge group number defined in the **bridge-group** command. It must be a value in the range 1 through 9.
group-list	LAT service groups. Single numbers and ranges are permitted. Specify a zero (0) to disable the LAT group code for the bridge group.

[**no**] **bridge-group** *bridge-group* **input-lsap-list** *access-list-number*

Use the **bridge-group input-lsap-list** interface configuration command to filter IEEE 802.2-encapsulated packets on input. Use the **no** form of this command to disable this capability.

bridge-group	Bridge group number defined in the **bridge-group** command. It must be a value in the range 1 through 9.
access-list-number	Access list number assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

[**no**] **bridge-group** *bridge-group* **input-pattern** *access-list-number*

Use the **bridge-group input-pattern** interface configuration command to associate an extended access list with a particular interface in a particular bridge group. Use the **no** form of this command to disable this capability.

bridge-group	The bridge group number defined in the **bridge-group** command. It must be a value in the range 1 through 9.
access-list-number	Access list number assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the interface.

[**no**] **bridge-group** *bridge-group* **input-type-list** *access-list-number*

Use the **bridge-group input-type-list** interface configuration command to filter Ethernet- and SNAP-encapsulated packets on input. Use the **no** form of this command to disable this capability.

bridge-group	Bridge group number defined in the **bridge-group** command.
access-list-number	Access list number assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

[**no**] **bridge-group** *bridge-group* **lat-compression**

Use the **bridge-group lat-compression** interface configuration command to reduce the amount of bandwidth that LAT traffic consumes on the serial interface by specifying a LAT-specific form of compression. Use the **no** form of this command to disable LAT compression on the bridge group.

bridge-group	Bridge group number defined in the **bridge-group** command.

[**no**] **bridge-group** *bridge-group* **output-address-list**
access-list-number

Use the **bridge-group output-address-list** interface configuration command to assign an access list to a particular interface for filtering the MAC destination addresses of packets that would ordinarily be forwarded out that interface. Use the **no** form of this command to remove an access list from an interface.

bridge-group	Bridge group number in the range 1 through 9, defined in the **bridge-group** command.
access-list-number	Access list number assigned with the bridge **access-list** command.

[**no**] **bridge-group** *bridge-group* **output-lat-service-deny** *group-list*

Use the **bridge-group output-lat-service-deny** interface configuration command to specify the group codes by which to deny access upon output. Use the **no** form of this command to cancel the specified group codes.

bridge-group	Bridge group number in the range 1 through 9, specified in the **bridge-group** command.
group-list	List of LAT groups. Single numbers and ranges are permitted.

[**no**] **bridge-group** *bridge-group* **output-lat-service-permit** *group-list*

Use the **bridge-group output-lat-service-permit** interface configuration command to specify the group codes by which to permit access upon output. Use the **no** form of this command to cancel specified group codes.

bridge-group	Bridge group number in the range 1 through 9, specified in the **bridge-group** command.
group-list	LAT service advertisements.

[**no**] **bridge-group** *bridge-group* **output-lsap-list** *access-list-number*

Use the **bridge-group output-lsap-list** interface configuration command to filter IEEE 802-encapsulated packets on output. Use the **no** form of this command to disable this capability.

bridge-group	Bridge group number in the range 1 through 9, specified in the **bridge-group** command.
access-list-number	Access list number assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

[**no**] **bridge-group** *bridge-group* **output-pattern-list** *access-list-number*

Use the **bridge-group output-pattern-list** interface configuration command to associate an extended access list with a particular interface. Use the **no** form of this command to disable this capability.

bridge-group	Bridge group number in the range 1 through 9, specified in the **bridge-group** command.
access-list-number	Extended access list number assigned with the extended **access-list** command. Specify a zero (0) to disable the application of the access list on the interface.

[**no**] **bridge-group** *bridge-group* **output-type-list** *access-list-number*

Use the **bridge-group output-type-list** interface configuration command to filter Ethernet- and SNAP-encapsulated packets on output. Use the **no** form of this command to disable this capability.

bridge-group	Bridge group number in the range 1 through 9, specified in the **bridge-group** command.
access-list-number	Access list number assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group. This access list is applied just before sending out a frame to an interface.

[**no**] **bridge-group** *bridge-group* **path-cost** *cost*

Use the **bridge-group path-cost** interface configuration command to set a different path cost. Use the **no** form of this command to choose the default path cost for the interface.

bridge-group	Bridge group number specified in the **bridge-group** command.
cost	Path cost can range from 1 through 65535, with higher values indicating higher costs. This range applies regardless of whether the IEEE or Digital spanning-tree protocol has been specified.

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

Use the **bridge-group priority** interface configuration command to set an interface priority when two bridges tie for position as the root bridge. The priority you set breaks the tie.

bridge-group	Bridge group number specified in the **bridge-group** command.
number	Priority number ranging from 0 through 255 (Digital), or 0 through 64000 (IEEE). The defaults are: 128—Digital spanning-tree protocol 32768—IEEE spanning-tree protocol

[**no**] **bridge-group** *bridge-group* **spanning-disabled**

Use the **bridge-group spanning-disabled** interface configuration command to disable the spanning tree on a given interface.

bridge-group	Bridge group number of the interface, specified in the **bridge-group** command.

[**no**] **bridge-group** *bridge-group* **sse**

Use the **bridge-group sse** interface configuration command to enable Cisco's silicon switching engine (SSE) switching function. Use the **no** form of this command to disable SSE switching.

bridge-group	Bridge group number in the range 1 through 9, specified in the **bridge-group** command.

clear bridge *bridge-group*

Use the **clear bridge** EXEC command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any statically or system-configured entries.

bridge-group	Bridge group number in the range 1 through 9, specified in the bridge-group command.

clear sse

Use the **clear sse** privileged EXEC command to reinitialize the Silicon Switch Processor (SSP) on the Cisco 7000 series.

encapsulation sde *said*

Use the **encapsulation sde** subinterface configuration command to enable IEEE 802.10 Secure Data Exchange (SDE) encapsulation of transparently bridged traffic on a specified interface within an assigned bridge group.

said	Security Association Identifier. The valid range is 0 through 0xFFF.

ethernet-transit-oui [**90-compatible** | **standard** | **cisco**]
no ethernet-transit-oui

Use the **ethernet-transit-oui** interface configuration command to choose the Organizational Unique Identifier (OUI) code to be used in the encapsulation of Ethernet Type II frames across Token Ring backbone networks. Various versions of this OUI code are used by Ethernet/Token Ring translational bridges. The default OUI form is **90-compatible**, which can be chosen with the **no** form of this command.

90-compatible	(Optional) Default OUI form.
standard	(Optional) Standard OUI form.
cisco	(Optional) Cisco’s OUI form.

frame-relay map bridge *dlci* **broadcast**
no frame-relay map bridge *dlci*

Use the **frame-relay map bridge broadcast** global configuration command to bridge over a Frame Relay network. Use the **no** form of this command to delete the mapping entry.

dlci	DLCI number in the range 16 through 1007.

[**no**] **ip routing**

Use the **ip routing** global configuration command to enable IP routing. Use the **no** form of this command to disable IP routing so that you can then bridge IP.

show bridge [*bridge-group*] [*interface*]
show bridge [*bridge-group*] [*address* [*mask*]]

Use the **show bridge** privileged EXEC command to view classes of entries in the bridge forwarding database.

bridge-group	(Optional) Number you chose that specifies a particular spanning tree.
interface	(Optional) Specific interface, such as Ethernet 0.
address	(Optional) 48-bit canonical (Ethernet ordered) MAC address. This may be entered with an optional mask of bits to be ignored in the address, which is specified with the *mask* argument.
mask	(Optional) Bits to be ignored in the address. You must specify the *address* argument if you want to specify a mask.

show bridge [*bridge-group*] **circuit-group** [[*circuit-group*]
[*src-mac-address*] [*dst-mac-address*]]

Use the **show bridge circuit-group** EXEC command to display the interfaces configured in each circuit group and show whether they are currently participating in load distribution.

bridge-group	(Optional) Number that specifies a particular bridge group.

circuit-group	(Optional) Number that specifies a particular circuit group.
src-mac-address	(Optional) 48-bit canonical (Ethernet ordered) source MAC address.
dst-mac-address	(Optional) 48-bit canonical (Ethernet ordered) destination MAC address.

show bridge group [verbose]

Use the **show bridge group** privileged EXEC command to display the status of each bridge group.]

verbose	(Optional) Displays detailed information.

show bridge vlan

Use the **show bridge vlan** privileged EXEC command to view virtual LAN subinterfaces.

show span

Use the **show span** privileged EXEC command to display the spanning-tree topology known to the router/bridge.

show sse summary

Use the **show sse summary** EXEC command to display a summary of Silicon Switch Processor (SSP) statistics.

x25 map bridge *x.121-address* **broadcast** [*options-keywords*]
no x25 map bridge

Use the **x25 map bridge broadcast** interface configuration command to configure the bridging of packets in X.25 frames. Use the **no** form of this command to disable the Internet-to-X.121 mapping.

x.121-address	The X.121 address.
options-keywords	(Optional) The services that can be added to this map; these services are listed in the “Setting Address Mappings” section of the *Router Products Configuration Guide*.

Source-Route Bridging Commands

This chapter describes the function and displays the syntax of each source-route bridging command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

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

Use the **access-expression** interface configuration command to define an access expression. Use the **no** form of this command to remove the access expression from the given interface. You use this command in conjunction with the **access-list** interface configuration command.

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

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

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

access-list-number — Integer that identifies the access list. If the *type-code* and *wild-mask* arguments are included, this integer ranges from 200 through 299, indicating that filtering is by protocol type. If the *address* and *mask* arguments are included, this integer ranges from 700 through 799, indicating that filtering is by vendor code.

permit — Permits the frame.

deny — Denies the frame.

type-code — 16-bit hexadecimal number written with a leading 0x; for example, 0x6000. Specify either a Link Service Access Point (LSAP) type code for 802-encapsulated packets or a SNAP type code for SNAP-encapsulated packets. (LSAP, sometimes called SAP, refers to the type codes found in the DSAP and SSAP fields of the 802 header.)

wild-mask — 16-bit hexadecimal number whose ones bits correspond to bits in the *type-code* argument. The *wild-mask* indicates which bits in the *type-code* argument should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be 0x0101 because these two bits are used for purposes other than identifying the SAP code.)

address — 48-bit Token Ring address written in dotted triplet form. This field is used for filtering by vendor code.

mask	48-bit Token Ring address written in dotted triplet form. The ones bits in *mask* are the bits to be ignored in *address*. This field is used for filtering by vendor code.

[**no**] **bridge** *bridge-group* **protocol ibm**

Use the **bridge protocol ibm** global configuration command to create a bridge group that runs the automatic spanning tree function. Use the **no** form of this command to cancel the previous assignment.

bridge-group	Number in the range 1 through 9 that you choose to refer to a particular set of bridged interfaces. Frames are bridged only among interfaces in the same group.

clear netbios-cache

Use the **clear netbios-cache** EXEC command to clear the entries of all dynamically learned NetBIOS names. This command will not remove statically defined name cache entries.

clear rif-cache

Use the **clear rif-cache** EXEC command to clear the entire RIF cache.

clear source-bridge

Use the **clear source-bridge** EXEC command to clear the source-bridge statistical counters.

clear sse

Use the **clear sse** privileged EXEC command to reinitialize the Silicon Switch Processor (SSP) on the Cisco 7000 series.

ethernet-transit-oui {**standard** | **90-compatible** | **cisco**}
no ethernet-transit-oui

Use the **ethernet-transit-oui** interface configuration command to choose the Organizational Unique Identifier (OUI) code to be used in the encapsulation of Ethernet Type II frames across Token Ring backbone networks. Various versions of this OUI code are used by Ethernet/Token Ring translational bridges. The **standard** keyword is used when you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity. Use the **no** form of this command to return the default OUI code.

standard	(Optional) Standard OUI form.
90-compatible	(Optional) Default OUI form.
cisco	(Optional) Cisco's OUI form.

lnm alternate *number*
no lnm alternate

Use the **lnm alternate** interface configuration command to specify the threshold reporting link number. In order for a LAN Reporting Manager (LRM) to change parameters, it must be attached to the reporting link with the lowest reporting link number, and that reporting link number must be lower than this threshold reporting link number. Use the **no** form of this command to restore the default of 0.

number	Threshold reporting link number. It must be in the range 0 through 3. The default is 0.

[**no**] **lnm crs**

Use the **lnm crs** interface configuration command to monitor the current logical configuration of a Token Ring. Use the **no** form of this command to disable this function.

lnm loss-threshold *number*
no lnm loss-threshold

Use the **lnm loss-threshold** interface configuration command to set the threshold at which the router sends a message informing all attached LNMs that it is dropping frames. Use the **no** form of this command to return to the default value.

number	A single number expressing the percentage loss rate in hundredths of a percent. The valid range is 0 through 9999. The default is 10 (.10 percent).

lnm password *number string*
no lnm password *number*

Use the **lnm password** interface configuration command to set the password for the reporting link. Use the **no** form of this command to return the password to its default value of 00000000.

number	Number of the reporting link to which to apply the password. This value should be in the range 0 through 3.
string	Password you enter at the keyboard. In order to maintain compatibility with LNM, the parameter *string* should be a six- to eight-character string of the type listed in the "Usage Guidelines" section for this command in the *Router Product Command Reference* publication.

[**no**] **lnm rem**

Use the **lnm rem** interface configuration command to monitor errors reported by any station on the ring. Use the **no** form of this command to disable this function.

[**no**] **lnm rps**

Use the **lnm rps** interface configuration command to ensure that all stations on a ring are using a consistent set of reporting parameters. Use the **no** form of this command to disable this function.

[**no**] **lnm snmp-only**

Use the **lnm snmp-only** global configuration command to prevent any LNM stations from modifying parameters in the router. Use the **no** form of this command to allow modifications.

lnm softerr *milliseconds*
no lnm softerr

Use the **lnm softerr** interface configuration command to set the time interval in which the router will accumulate error messages before sending them. Use the **no** form of this command to return to the default value.

milliseconds	Time interval in tens of milliseconds between error messages. The valid range is 0 through 65535. The default is 200 milliseconds (2 seconds).

[**no**] **locaddr-priority** *list-number*

Use the **locaddr-priority** interface configuration command to assign a remote source-route bridging (RSRB) priority group to an input interface. Use the **no** form of this command to remove the RSRB priority group assignment from the interface.

list-number	Priority list number of the input interface.

[**no**] **locaddr-priority-list** *list-number address-number queue-keyword* [*dsap ds*] [*dmac dm*]

Use the **locaddr-priority-list** global configuration command to map logical units (LUs) to queuing priorities as one of the steps to establishing queuing priorities based on LU addresses. Use the **no** form of this command to remove that RSRB priority queuing assignment. You use this command in conjunction with the **priority list** command.

list-number	Arbitrary integer between 1 and 10 that identifies the LU address priority list selected by the user.
address-number	Value of the LOCADDR= parameter on the LU macro, which is a one-byte address of the LU in hex.
queue-keyword	Priority queue name; one of **high**, **medium**, **normal**, or **low**.
dsap ds	(Optional) Indicates that the next argument, *ds*, represents the destination service access point address. The argument *ds* is a hexadecimal value.
dmac dm	(Optional) Indicates that the next argument, *dm*, is the destination MAC address. The argument *dm* is a dotted triple of four-digit hexadecimal numbers.

mac-address *ieee-address*

Use the **mac-address** interface configuration command to set the MAC layer address of the Cisco Token Ring.

ieee-address	48-bit IEEE MAC address written as a dotted triplet of four-digit hexadecimal numbers.

[**no**] **multiring** {*protocol-keyword* | **all** | **other**}

Use the **multiring** interface configuration command to enable collection and use of RIF information. Use the **no** form of this command with the appropriate keyword to disable the use of RIF information for the protocol specified.

protocol-keyword	Specifies a protocol; see the keyword list in the "Usage Guidelines" section for this command in the *Router Products Command Reference* publication.
all	Enables the multiring for *all* frames.
other	Enables the multiring for *any* routed frame not included in the previous list of supported protocols.

[**no**] **netbios access-list bytes** *name* {**permit** | **deny**} *offset pattern*

Use the **netbios access-list bytes** global configuration command to define the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets. Use the **no** form of this command to remove an entire list or the entry specified with the *pattern* argument.

name	Name of the access list being defined.
permit	Permits the condition.

deny	Denies the condition.
offset	Decimal number indicating the number of bytes into the packet where the byte comparison should begin. An offset of zero points to the very beginning of the NetBIOS header. Therefore, the NetBIOS delimiter string (0xffef), for example, begins at offset 2.
pattern	Hexadecimal string of digits representing a byte pattern. The argument *pattern* must conform to certain conventions. These conventions are listed in the "Usage Guidelines" section for this command in the *Router Products Command Reference* publication.

[**no**] **netbios access-list host** *name* {**permit** | **deny**} *pattern*

Use the **netbios access-list host** global configuration command to assign the name of the access list to a station or set of stations on the network. The NetBIOS station access list contains the station name to match, along with a permit or deny condition. Use the **no** form of this command to remove either an entire list or just a single entry from a list, depending upon the argument given for *pattern*.

name	Name of the access list being defined.
permit	Permits the condition.
deny	Denies the condition.
pattern	A set of characters. The characters can be the name of the station, or a combination of characters and pattern-matching symbols that establish a pattern for a set of NetBIOS station names. This combination can be especially useful when stations have names with the same characters, such as a prefix. For available pattern-matching symbols, see the table in the "Usage Guidelines" section of the *Router Products Command Reference* publication.

[**no**] **netbios enable-name-cache**

Use the **netbios enable-name-cache** interface configuration command to enable NetBIOS name caching. Use the **no** form of this command to disable the name-cache behavior.

[**no**] **netbios input-access-filter bytes** *name*

Use the **netbios input-access-filter bytes** interface configuration command to define a byte access list filter on incoming messages. The actual access filter byte offsets and patterns used are defined in one or more **netbios-access-list bytes** commands. Use the **no** form of this command with the appropriate name to remove the entire access list.

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list bytes** global configuration commands.

[**no**] **netbios input-access-filter host** *name*

Use the **netbios input-access-filter host** interface configuration command to define a station access list filter on incoming messages. The access lists of station names are defined in **netbios access-list host** commands. Use the **no** form of this command with the appropriate argument to remove the entire access list.

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list host** global configuration commands.

netbios name-cache *mac-address netbios-name* {*interface-name* |
ring-group *group-number*}
no netbios name-cache *mac-address netbios-name*

Use the **netbios name-cache** global configuration command to define a static NetBIOS name-cache entry, tying the server with the name *netbios-name* to the *mac-address*, and specifying that the server is accessible either locally via the *interface-name* specified, or remotely, via the **ring-group** *group-number* specified. Use the **no** form of this command to remove the entry.

mac-address	The MAC address.
netbios-name	Server name linked to the MAC address.
interface-name	Name of the interface by which the server is accessible locally.
ring-group	Specifies that the link is accessible remotely.
group-number	Number of the ring group by which the server is accessible remotely. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

netbios name-cache name-len *length*

Use the **netbios name-cache name-len** global configuration command to specify how many characters of the NetBIOS type name the name cache will validate.

length	The length of the NetBIOS type name. The default length is 15 characters. The range is 8 to 16 characters.

netbios name-cache proxy-datagram *seconds*

Use the **netbios name-cache proxy-datagram** global configuration command to enable the router to act as a proxy and send NetBIOS datagram type frames.

seconds	Time interval, in seconds, that the router forwards a route broadcast datagram type packet. The valid range is any number greater than 0.

netbios name-cache query-timeout *seconds*
no netbios name-cache query-timeout

Use the **netbios name-cache query-timeout** global configuration command to specify the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame. During this dead time, the router drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process. Use the **no** form of this command to bring the time back to the default of 6 seconds.

seconds “Dead” time period in seconds. The default is 6 seconds.

netbios name-cache recognized-timeout *seconds*
no netbios name-cache recognized-timeout

Use the **netbios name-cache recognized-timeout** global configuration command to specify the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame. During this dead time, the router drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is only effective at the time of the login negotiation process. Use the **no** form of this command to bring the time back to the default of 6 seconds.

seconds “Dead” time period in seconds. The default is 6 seconds.

[**no**] **netbios name-cache timeout** *minutes*

Use the **netbios name-cache timeout** global configuration command to enable NetBIOS name caching and to set the time that entries can remain in the NetBIOS name cache. Use the **no** form of this command to bring the time back to the default of 15 minutes.

minutes Time, in minutes, that entries can remain in the NetBIOS name cache. Once the time expires, the entry will be deleted from the cache. The default is 15 minutes.

[**no**] **netbios output-access-filter bytes** *name*

Use the **netbios output-access-filter bytes** interface configuration command to define a byte access list filter on outgoing messages. Use the **no** form of this command to remove the entire access list.

name Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list bytes** global configuration commands.

[**no**] **netbios output-access-filter host** *name*

Use the **netbios output-access-filter host** interface configuration command to define a station access list filter on outgoing messages. Use the **no** form of this command to remove the entire access list.

name Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list host** global configuration commands.

[**no**] **priority-group** *list*

Use the **priority-group** interface configuration command to assign a specified priority list to an interface. Use the **no** form of this command to cancel the assignment.

list Priority list number assigned to the interface.

priority-list *list-number* **protocol** *protocol-name queue-keyword*
no priority-list *list-number address-number queue-keyword*

Use the **priority-list** global configuration command to establish queuing priorities based upon the protocol type as one of the steps to establishing queuing priorities based on logical unit (LU) addresses. Use the **no** form of this command to remove the priority list. Use this command in conjunction with the **locaddr-priority-list** command.

list-number Arbitrary integer between 1 and 10 that identifies the LU address priority list selected by the user.

protocol	Keyword indicating you want the priority list to be based on a protocol type.
protocol-name	Protocol you are using. In most cases, this will be **ip**.
queue-keyword	Priority queue name; one of **high**, **medium**, **normal**, or **low**.

rif *mac-address rif-string* {*interface-name* | **ring-group** *ring*}
no rif *mac-address* {*interface-name* | **ring-group** *ring*}

Use the **rif** global configuration command to enter static source-route information into the RIF cache. If a Token Ring host does not support the use of IEEE 802.2 TEST or XID datagrams as explorer packets, you might need to add static information to the RIF cache of the router/bridge. Use the **no** form of this command to remove an entry from the cache.

mac-address	12-digit hexadecimal string written as a dotted triplet; for example, 0010.0a00.20a6.
rif-string	Series of 4-digit hexadecimal numbers separated by a period (.). This RIF string is inserted into the packets sent to the specified MAC address.
interface-name	Interface name (for example, tokenring0) that indicates the origin of the RIF.
ring-group	Specifies the origin of the RIF is a ring group.
ring	Ring group number that indicates the origin of the RIF. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

rif timeout *minutes*
no rif timeout

Use the **rif timeout** global configuration command to determine the number of minutes an inactive RIF entry is kept. RIF information is maintained in a cache whose entries are aged. Use the **no** form of this command to restore the default.

minutes	Number of minutes the RIF entry is kept. The value must be greater than 0. The default is 15 minutes.

rif validate-age *seconds*

Use the **rif validate-age** global configuration command to define the validation time when the router is acting as a proxy for the **netbios name-query** command or for explorer frames.

seconds	Interval, in seconds, at which a proxy is sent. The valid range is any number greater than 0. The default is 2 seconds.

rsrb remote-peer *ring-group* **tcp** *ip-address* **lsap-output-list**
access-list-number
rsrb remote-peer *ring-group* **fst** *ip-address* **lsap-output-list**
access-list-number
rsrb remote-peer *ring-group* **interface** *interface-name* **lsap-output-list**
access-list-number

Use the **rsrb remote-peer lsap-output-list** global configuration command to define SAP filters by LSAP address on the remote source-route bridging WAN interface.

ring-group	Virtual ring number of the remote peer.
tcp	Indicates TCP encapsulation.
fst	Indicates FST encapsulation.
ip-address	IP address.

interface	Indicates direct encapsulation.
interface-name	Interface name.
access-list-number	Number of the access list.

rsrb remote-peer *ring-group* **tcp** *ip-address* **netbios-output-list** *name*
rsrb remote-peer *ring-group* **fst** *ip-address* **netbios-output-list** *name*
rsrb remote-peer *ring-group* **interface** *interface-name*
netbios-output-list *host*

Use the **rsrb remote-peer netbios-output-list** global configuration command to filter packets by NetBIOS station name on a remote source-route bridging WAN interface.

ring-group	Virtual ring number of the remote peer.
tcp	Indicates TCP encapsulation.
fst	Indicates FST encapsulation.
ip-address	IP address.
name	Name of a NetBIOS access filter previously defined with one or more **netbios access-list host** global configuration commands.
interface	Indicates direct encapsulation.
interface-name	Interface name.
host	Host name.

sap priority *number*

Use the **sap-priority** interface configuration command to define a priority list on an interface.

number	Priority list number you specified in the **sap-priority-list** command.

sap-priority-list *number queue-keyword* [**dsap** *ds*] [**ssap** *ss*] [**dmac** *dm*] [**smac** *sm*]

Use the **sap-priority-list** global configuration command to define a priority list.

number	Arbitrary integer between 1 and 10 that identifies the priority list.
queue-keyword	Priority queue name or a remote source-route bridge TCP port name.
dsap *ds*	(Optional) Indicates that the next argument, *ds,* represents the destination service access point address. The argument *ds* is a hexadecimal number.
ssap *ss*	(Optional) Indicates that the next argument, *ss,* represents the source service access point address. The argument *ss* is a hexadecimal number.
dmac *dm*	(Optional) Indicates that the next argument, *dm,* represents the destination MAC address. The argument *dm* is written as a dotted triple of four-digit hexadecimal numbers.
smac *sm*	(Optional) Indicates that the next argument, *sm,* represents the source MAC address. The argument *sm* is written as a dotted triple of four-digit hexadecimal numbers.

show controllers token

Use the **show controllers token** privileged EXEC command to display information about memory management, error counters, and the board itself. Depending on the board being used, the output can vary. This command also displays proprietary information. Thus, the information that **show controllers token** displays is of primary use to our technical personnel. Information that is useful to users can be obtained with the **show interfaces tokenring** command.

show interfaces tokenring [*unit*]

Use the **show interfaces tokenring** privileged EXEC command to display information about the Token Ring interface and the state of source-route bridging.

unit	(Optional) Interface number. If you do not provide a value for the *unit* argument, the command will display statistics for all Token Ring interfaces.

show lnm bridge

Use the **show lnm bridge** privileged EXEC command to display all currently configured bridges and all parameters that are related to the bridge as a whole, not to one of its interfaces.

show lnm config

Use the **show lnm config** privileged EXEC command to display the logical configuration of all bridges configured in a router. This information is needed to configure an LNM Management Station to communicate with a router. This is especially important when the router is configured as a multiport bridge, thus employing the concept of a virtual ring.

show lnm interface [*interface*]

Use the **show lnm interface** privileged EXEC command to display all LNM-related information about a specific interface, or about all interfaces.

interface	(Optional) Number of a specific interface for which LNM-related information is to be displayed.

show lnm ring [*ring-number*]

Use the **show lnm ring** privileged EXEC command to display all LNM information about a specific Token Ring, or about all Token Rings. If a specific interface is requested, it also displays a list of all currently active stations on that interface.

ring-number	(Optional) Number of a specific Token Ring. It can be a value in the range 1 through 4095.

show lnm station [*address*]

Use the **show lnm station** privileged EXEC command to display LNM-related information about a specific station, or about all known stations on all rings. If a specific station is requested, it also displays a detailed list of that station's current MAC-level parameters.

address	(Optional) Address of a specific LNM station.

show local-ack

Use the **show local-ack** privileged EXEC command to display the current state of any current Local Acknowledgment for both LLC2 and SDLLC connections, as well as any configured passthrough rings.

show netbios-cache

Use the **show netbios-cache** privileged EXEC command to display a list of NetBIOS cache entries.

show rif

Use the **show rif** privileged EXEC command to display the current contents of the RIF cache.

show source-bridge

Use the **show source-bridge** privileged EXEC command to display the current source bridge configuration and miscellaneous statistics.

show span

Use the **show span** EXEC command to display the spanning-tree topology known to the router.

source-bridge *local-ring bridge-number target-ring*
no source-bridge

Use the **source-bridge** interface configuration command to configure an interface for source-route bridging. Use the **no** form of this command to disable source bridging on a particular interface.

local-ring	Ring number for this interface's Token Ring. It must be a decimal number between 1 and 4095 that uniquely identifies a network segment or ring within the bridged Token Ring network.
bridge-number	Number that uniquely identifies the bridge connecting the local and target rings. It must be a decimal number between 1 and 15.
target-ring	Decimal ring number of the destination ring on this router/bridge. It also must be unique within the bridged Token Ring network. The target ring can also be a ring group.

[**no**] **source-bridge cos-enable**

Use the **source-bridge cos-enable** global configuration command to force the router to read the contents of the Format Identification 4 (FID 4) frames to prioritize traffic when using TCP. Use the **no** form of this command to disable prioritizing.

[**no**] **source-bridge enable-80d5**

Use the **source-bridge enable-80d5** global configuration command to change the router's Token Ring to Ethernet translation behavior. Use the **no** form of this command to restore the default behavior.

[**no**] **source-bridge explorer-fastswitch**

Use the **source-bridge explorer-fastswitch** global configuration command to enable explorer fast switching. To disable explorer fast switching, use the **no** form of this command.

source-bridge explorer-maxrate *maxrate*
no source-bridge explorer-maxrate

Use the **source-bridge explorer-maxrate** global configuration command to set the maximum byte rate of explorers per ring. To reset the default rate, use the **no** form of this command.

maxrate	Number in the range 1000 through -1.

[**no**] **source-bridge explorerq-depth** *depth*

Use the **source-bridge explorerq-depth** global configuration command to set the maximum explorer queue depth. To reset the default value, use the **no** form of this command.

depth	The maximum number of incoming packets. The valid range is 1 through 500. The default is 30.

[**no**] **source-bridge fst-peername** *local-interface-address*

Use the **source-bridge fst-peername** global configuration command to set up a Fast Sequenced Transport (FST) peer name. Use the **no** form of this command to disable the IP address assignment.

local-interface-address	IP address to assign to the local router.

[**no**] **source-bridge input-address-list** *access-list-number*

Use the **source-bridge input-address-list** interface configuration command to assign an access list to a particular input interface for filtering the Token Ring or IEEE 802.2 source addresses. This command filters packets coming into the router. Use the **no** form of this command to remove the application of the access list.

access-list-number	Number of the access list. The value must be in the range 700 through 799.

source-bridge input-lsap-list *access-list-number*

Use the **source-bridge input-lsap-list** interface configuration command to filter, on input, FDDI and IEEE 802-encapsulated packets which include the destination service access point (DSAP) and source service access point (SSAP) fields in their frame formats. The access list specifying the type codes to be filtered is given by this variation of the **source-bridge** interface configuration command.

access-list-number	Number of the access list. This access list is applied to all IEEE 802 or FDDI frames received on that interface prior to the source-routing process. Specify zero (0) to disable the filter. The value must be in the range 200 through 299.

source-bridge input-type-list *access-list-number*

Use the **source-bridge input-type-list** interface configuration command to filter SNAP-encapsulated packets on input.

access-list-number	Number of the access list. This access list is applied to all SNAP frames received on that interface prior to the source-routing process. Specify zero (0) to disable the application of the access list on the bridge group. The value must be in the range 200 through 299.

source-bridge keepalive *seconds*
no source-bridge keepalive

Use the **source-bridge keepalive** interface configuration command to assign the keepalive interval of the remote source-bridging peer. Use the **no** form of this command to cancel previous assignments.

seconds	Keepalive interval in seconds. The valid range is 10 through 300. The default is 30 seconds.

source-bridge largest-frame *ring-group size*
no source-bridge largest-frame *ring-group*

Use the **source-bridge largest-frame** global configuration command to configure the largest frame size that is used to communicate with any peers in the ring group. Use the **no** form of this command to cancel previous assignments.

ring-group	Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.
size	Maximum frame size.

[**no**] **source-bridge old-sna**

Use the **source-bridge old-sna** interface configuration command to rewrite the RIF headers of explorer packets sent by the PC/3270 emulation program to go beyond the local ring. Use the **no** form of this command to disable this compatibility mode.

[**no**] **source-bridge output-address-list** *access-list-number*

Use the **source-bridge output-address-list** interface configuration command to assign an access list to a particular output interface packet for filtering the Token Ring or IEEE 802.2 source (rather than destination) addresses. This command filters packets sent out from the router. Use the **no** form of this command to remove the application of the access list.

access-list-number Number of the access list. The value must be in the range 700 through 799.

source-bridge output-lsap-list *access-list-number*

Use the **source-bridge output-lsap-list** interface configuration command to filter, on output, FDDI and IEEE 802-encapsulated packets which include the destination service access point (DSAP) and source service access point (SSAP) fields in their frame formats.

access-list-number Number of the access list. This access list is applied just before sending out a frame to an interface. Specify zero (0) to disable the filter. The value must be in the range 200 through 299.

source-bridge output-type-list *access-list-number*

Use the **source-bridge output-type-list** interface configuration command to filter SNAP-encapsulated frames by type code on output.

access-list-number Number of the access list. This access list is applied just before sending out a frame to an interface. Specify zero (0) to disable the application of the access list on the bridge group. The value must be in the range 200 through 299.

[**no**] **source-bridge passthrough** *ring-group*

Use the **source-bridge passthrough** global configuration command to configure some sessions on a few rings to be locally acknowledged and the remaining to pass through. Use the **no** form of this command to disable passthrough on all the rings and allow the session to be locally acknowledged.

ring-group	Ring group number. This ring is either the start ring or destination ring of the two IBM end machines for which the passthrough feature is to be configured. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

[**no**] **source-bridge proxy-explorer**

Use the **source-bridge proxy-explorer** interface configuration command to configure the interface to respond to any explorer packets from a source node that meet the conditions described in the "Usage Guidelines" section for this command in the *Router Products Command Reference* publication. Use the **no** form of this command to cancel responding to explorer packets with proxy explorers.

[**no**] **source-bridge proxy-netbios-only**

Use the **source-bridge proxy-netbios-only** interface configuration command to enable proxy explorers for the NetBIOS name-caching function. Use the **no** form of this command to disable the NetBIOS name-caching function.

source-bridge remote-peer *ring-group* **fst** *ip-address* [**lf** *size*]
no source-bridge remote-peer *ring-group* **fst** *ip-address*

Use the **source-bridge remote-peer fst** global configuration command to specify a Fast Sequenced Transport (FST) encapsulation connection. Use the **no** form of this command to disable the previous assignments.

ring-group Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

ip-address IP address of the remote peer with which the router will communicate.

lf *size* (Optional) Maximum size frame to be sent to this remote peer. The router negotiates all transit routes down to this size or lower. Use this argument to prevent timeouts in end hosts by reducing the amount of data they have to transmit in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

source-bridge remote-peer *ring-group* **ftcp** *ip-address*
[**lf** *size*] [**local-ack**]
no source-bridge remote-peer *ring-group* **ftcp** *ip-address*

Use the **source-bridge remote-peer ftcp** global configuration command to enable fast switching of Token Ring frames over TCP/IP. Use the **no** form of this command to remove a remote peer from the specified ring group.

ring-group Ring-group number. This ring-group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

ip-address IP address of the remote peer with which the router will communicate.

lf *size* (Optional) Maximum size frame to be sent to this remote peer. The router negotiates all transit routes down to this size or lower.

local-ack (Optional) LLC2 sessions destined for a specific remote peer are to be locally terminated and acknowledged. Local acknowledgment should be used for LLC2 sessions going to this remote peer.

source-bridge remote-peer *ring-group* **interface** *interface-name*
[*mac-address*] [**lf** *size*]
no source-bridge remote-peer *ring-group* **interface** *interface-name*

Use the **source-bridge remote-peer interface** global configuration command when specifying a point-to-point direct encapsulation connection. Use the **no** form of this command to disable previous interface assignments.

ring-group Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

interface-name Name of the router's serial interface over which to send source-route bridged traffic.

mac-address (Optional) MAC address for the interface you specify using the *interface-name* argument. This argument is required for nonserial interfaces. You can obtain the value of this MAC address by using the **show interface** command, and then scanning the display for the interface specified by *interface-name.*

lf *size* — (Optional) Maximum size frame to be sent to this remote peer. The router negotiates all transit routes down to this size or lower. This argument is useful in preventing timeouts in end hosts by reducing the amount of data they have to transmit in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

source-bridge remote-peer *ring-group* **tcp** *ip-address* [**lf** *size*]
[**local-ack**] [**priority**]
no source-bridge remote-peer *ring-group* **tcp** *ip-address*

Use the **source-bridge remote-peer tcp** global configuration command to identify the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP. Use the **no** form of this command to remove a remote peer for the specified ring group.

ring-group — Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

ip-address — IP address of the remote peer with which the router will communicate.

lf *size* — (Optional) Maximum size frame to be sent to this remote peer. The router negotiates all transit routes down to this size or lower. Use this argument pair to prevent timeouts in end hosts by reducing the amount of data they have to transmit in a fixed interval. The valid values for this argument pair are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

local-ack — (Optional) LLC2 sessions destined for a specific remote peer are to be locally terminated and acknowledged. Local acknowledgment should be used for LLC2 sessions going to this remote peer.

priority	(Optional) Enables prioritization over a TCP network. You must specify the keyword **local-ack** earlier in the same **source-bridge remote-peer** command. The keyword **priority** is a prerequisite for features such as SNA class of service and SNA LU address prioritization over a TCP network.

source-bridge remote-peer-keepalive *seconds*
no source-bridge remote-peer-keepalive

Use the **source-bridge remote-peer-keepalive** interface configuration command to enable remote-peer keepalives, which are used to verify that a remote peer is reachable. Use the **no** form of this command to disable the keepalive mechanism.

seconds	Keepalive interval in seconds. The valid range is 10 through 300. The default is 30 seconds.

[**no**] **source-bridge ring-group** *ring-group*

Use the **source-bridge ring-group** global configuration command to define or remove a ring group from the router configuration. Use the **no** form of this command to cancel previous assignments.

ring-group	Ring group number. The valid range is 1 through 4095.

[**no**] **source-bridge route-cache**

Use the **source-bridge route-cache** interface configuration command to enable fast switching. Use the **no** form of this command to disable fast switching.

[**no**] **source-bridge route-cache cbus**

Use the **source-bridge route-cache cbus** interface configuration command to enable autonomous switching. Use the **no** form of this command to disable autonomous switching.

[**no**] **source-bridge route-cache sse**

Use the **source-bridge route-cache sse** interface configuration command to enable Cisco's silicon switching engine (SSE) switching function. Use the **no** form of this command to disable SSE switching.

[**no**] **source-bridge sap-80d5** *dsap*

Use the **source-bridge sap-80d5** global configuration command to allow non-IBM hosts (attached to a router with 80d5 processing enabled) to use the standard Token Ring to Ethernet LLC2 translation instead of the nonstandard Token Ring to Ethernet 80d5 translation. This command allows you to set the translation on a per-DSAP basis. Use the **no** form of this command to disable this feature.

dsap	Destination service access point (DSAP).

[**no**] **source-bridge spanning** *bridge-group*

Use the **source-bridge spanning** interface configuration command to enable the automatic spanning tree function for a specified group of bridged interfaces. Use the **no** form of this command to disable the previous assignment.

bridge-group	Number in the range 1 through 9 that you choose to refer to a particular group of bridged interfaces. This must be the same bridge-group number as assigned in the **bridge protocol ibm** command.

[**no**] **source-bridge spanning** *bridge-group* **path-cost** *path-cost*

Use the **source-bridge spanning path-cost** interface configuration command to assign a path cost for a specified interface. Use the **no** form of this command to disable the previous assignment.

bridge-group — Number in the range 1 through 9 that you choose to refer to a particular group of bridged interfaces. This must be the same bridge-group number as assigned in the **bridge protocol ibm** command.

path-cost — Path cost for the interface. The valid range is 0 through 65535.

[**no**] **source-bridge tcp-queue-max** *number*

Use the **source-bridge tcp-queue-max** global configuration command to modify the size of the backup queue for remote source-route bridging. This backup queue determines the number of packets that can wait for transmission to a remote ring before packets start being thrown away. Use the **no** form of this command to return to the default value.

number — Number of packets to hold in any single outgoing TCP queue to a remote router. The default is 100 packets.

source-bridge transparent *ring-group pseudo-ring bridge-number tb-group* [*oui*]
no source-bridge transparent *ring-group pseudo-ring bridge-number tb-group*

Use the **source-bridge transparent** global configuration command to establish bridging between transparent bridging and source-route bridging. Use the **no** form of this command to disable a previously established link between a source-bridge ring group and a transparent bridge group.

ring-group — Virtual ring group created by the **source-bridge ring-group** command. This is the source-bridge virtual ring to associate with the transparent bridge group. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

pseudo-ring — Ring number used to represent the transparent bridging domain to the source-route bridged domain. This number must be a unique number, not used by any other ring in your source-route bridged network.

bridge-number — Bridge number of the bridge that leads to the transparent bridging domain.

tb-group — Number of the transparent bridge group that you want to tie into your source-route bridged domain.

oui — (Optional) Organizational unique identifier. Possible values include: **90-compatible**, **standard**, and **cisco**.

STUN Commands

This chapter describes the function and displays the syntax of each STUN command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

encapsulation stun

Use the **encapsulation stun** interface configuration command to enable STUN encapsulation on a specified serial interface.

locaddr-priority-list *list-number address-number queue-keyword*
no locaddr-priority-list

Use the **locaddr-priority-list** interface configuration command to establish queuing priorities based upon the address of the logical unit (LU). Use the **no** form of this command to cancel all previous assignments.

list-number	Arbitrary integer between 1 and 10 that identifies the LU address priority list.
address-number	Value of the LOCADDR= parameter on the LU macro, which is a 1-byte address of the LU in hexadecimal.
queue-keyword	Priority queue type: **high**, **medium**, **normal**, or **low**.

[**no**] priority-group *list-number*

Use the **priority-group** interface configuration command to assign a priority group to an interface. Use the **no** form of this command to remove assignments.

list-number	Priority list number assigned to the interface.

[**no**] **priority-list** *list-number* **protocol ip** *queue-keyword* **tcp** *tcp-port-number*

Use the **priority-list protocol ip tcp** global configuration command to establish STUN queuing priorities based on the TCP port. Use the **no** form of this command to revert to normal priorities.

list-number Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.

queue-keyword Priority queue type: **high**, **medium**, **normal**, or **low**.

tcp-port-number STUN port and priority settings are as follows: high (**1994**), medium (**1990**), normal (**1991**), and low (**1992**).

[**no**] **priority-list** *list-number* **stun** *queue-keyword* **address** *group-number address-number*

Use the **priority-list stun address** global configuration command to establish STUN queuing priorities based on the address of the serial link. Use the **no** form of this command to revert to normal priorities.

list-number Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.

queue-keyword Priority queue type: **high**, **medium**, **normal**, or **low**.

group-number Group number that is used in the **stun group** command.

address-number Address of the serial link. For an SDLC link, the format is a 1-byte hex value (for example, C1). For a non-SDLC link, the address format can be specified by the **stun schema** command.

sdlc address FF ack-mode

Use the **sdlc address FF ack-mode** interface configuration command to configure the IBM reserved address FF as a valid local (not broadcast) address.

[**no**] sdlc virtual-multidrop

Use the **sdlc virtual-multidrop** interface configuration command to allow SDLC broadcast address FF to be replicated for each of the STUN peers, so each of the end stations receive the broadcast frame. Use the **no** form of this command to disable the SDLC broadcast feature.

show stun

Use the **show stun** privileged EXEC command to display the current status of STUN connections.

show stun sdlc

Use the **show stun sdlc** EXEC command to display the status of the STUN interfaces using SDLC encapsulation and whether proxy polling is enabled for that interface.

[**no**] stun group *group-number*

Use the **stun group** interface configuration command to place each STUN-enabled interface on a router in a previously defined STUN group. Use the **no** form of this command to remove an interface from a group.

group-number	Integer in the range 1 through 255.

stun keepalive-count *count*
no stun keepalive-count

Use the **stun keepalive-count** global configuration command to define the number of times to attempt a peer connection before declaring the peer connection to be down. Use the **no** form of this command to cancel the previous definition.

count	Number of connection attempts. The range is between 2 and 10 retries.

[**no**] **stun peer-name** *ip-address*

Use the **stun peer-name** global configuration command to enable STUN on IP addresses. Use the **no** form of this command to disable STUN on an IP address.

ip-address	IP address by which this STUN peer is known to other STUN peers.

stun protocol-group *group-number* {**basic** | **sdlc** | **schema**} [**sdlc-tg**]
no stun protocol-group

Use the **stun protocol-group** global configuration command to create a protocol group. Use the **no** form of this command to remove an interface from the group.

group-number	Integer in the range 1 through 255.
basic	Indicates a non-SDLC protocol.
sdlc	Indicates an SDLC group.
schema	Indicates a custom protocol.
sdlc-tg	(Optional) Used in conjunction with the sdlc keyword. Identifies the group as part of an SNA transmission group.

stun remote-peer-keepalive *seconds*
no stun remote-peer-keepalive

Use the **stun remote-peer-keepalive** global configuration command to enable detection of the loss of a peer.

seconds	Keepalive interval, in seconds. The range is 1 to 300 seconds. The default is 30 seconds.

stun route address *address-number* **interface serial** *interface-number* [**direct**]
no stun route address *address-number* **interface serial** *interface-number*

Use the **stun route address interface serial** interface configuration command to forward all HDLC traffic of a serial interface. Use the **no** form of this command to disable this method of HDLC encapsulation.

address-number	Address of the serial interface.
interface-number	Number assigned to the serial interface.
direct	(Optional) Forwards all HDLC traffic on a direct STUN link.

[**no**] **stun route address** *address-number* **tcp** *ip-address* [**local-ack**] [**priority**]

Use the **stun route address tcp** interface configuration command to specify TCP encapsulation and optionally establish SDLC local acknowledgment (SDLC Transport) for STUN. Use the **no** form of this command to disable this method of TCP encapsulation.

address-number	Number that conforms to TCP addressing conventions.

ip-address	IP address by which this STUN peer is known to other STUN peers that are using the TCP as the STUN encapsulation.
local-ack	(Optional) Enables local acknowledgment for STUN.
priority	(Optional) Establishes the four levels used in priority queuing: low, medium, normal, and high.

stun route all interface serial *interface-number* [**direct**]

Use the **stun route all interface serial** interface configuration command to encapsulate and forward all STUN traffic using HDLC encapsulation on a serial interface.

interface-number	Number assigned to the serial interface.
direct	(Optional) Indicates that the specified interface is also a direct STUN link, rather than a serial connection to another peer.

stun route all tcp *ip-address*

Use the **stun route all tcp** interface configuration command to use TCP encapsulation and forward all STUN traffic on an interface regardless of what address is contained in the serial frame.

ip-address	IP address by which this remote STUN peer is known to other STUN peers. Use the address that identifies the remote STUN peer that is connected to the far serial link.

[**no**] **stun schema** *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*

Use the **stun schema** global configuration command to define a protocol other than SDLC for use with STUN. Use the **no** form of this command to disable the new protocol.

name	Name that defines your protocol. It can be up to 20 characters long.
offset *constant-offset*	Constant offset (in bytes) for the address to be found in the frame.
length *address-length*	Length (in bytes) in one of the following address formats: decimal (4 bytes) hexadecimal (8 bytes) octal (4 bytes)
format *format-keyword*	Format to be used to specify and display addresses for routes on interfaces that use this STUN protocol. The allowable format keywords are: **decimal** (0 through 9) **hexadecimal** (0 through F) **octal** (0 through 7)

stun sdlc-role primary

Use the **stun sdlc-role primary** interface configuration command to assign the router the role of SDLC primary node. Primary nodes poll secondary nodes in a predetermined order.

stun sdlc-role secondary

Use the **stun sdlc-role secondary** interface configuration command to assign the router the role of SDLC secondary node. Secondary nodes respond to polls sent by the SDLC primary by transmitting any outgoing data they might have.

LLC2 and SDLC Commands

This chapter describes the function and displays the syntax of each LLC2 and SDLC command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

encapsulation sdlc

Use the **encapsulation sdlc** interface configuration command to configure the router as the primary SDLC station if you plan to configure either DLSw+ or Frame Relay access support.

encapsulation sdlc-primary

Use the **encapsulation sdlc-primary** interface configuration command to configure the router as the primary SDLC station when you plan to configure SDLLC media translation.

encapsulation sdlc-secondary

Use the **encapsulation sdlc-secondary** interface configuration command to configure the router as a secondary SDLC station when you plan to configure SDLLC media translation.

llc2 ack-delay-time *milliseconds*

Use the **llc2 ack-delay-time** interface configuration command to set the amount of time the router waits for an acknowledgment before sending the next set of information frames.

milliseconds Number of milliseconds the router allows incoming information frames to stay unacknowledged. The minimum is 1; the maximum is 60000. The default is 3200 milliseconds.

llc2 ack-max *packet-count*

Use the **llc2 ack-max** interface configuration command to control the maximum amount of information frames the router can receive before it must send an acknowledgment.

packet-count Maximum number of packets the router will receive before sending an acknowledgment. The minimum is 1 packet. The maximum is 127 packets. The default is 3 packets.

llc2 idle-time *milliseconds*

Use the **llc2 idle-time** interface configuration command to control the frequency of polls during periods of idle time (no traffic).

milliseconds Number of milliseconds that can pass with no traffic before the LLC2 station sends a Receiver Ready frame. The minimum is 1 millisecond; the maximum is 60000 milliseconds. The default is 10000 milliseconds.

llc2 local-window *packet-count*

Use the **llc2 local-window** interface configuration command to control the maximum number of information frames the router sends before it waits for an acknowledgment.

packet-count Maximum number of packets that can be sent before the router must wait for an acknowledgment. The minimum is 1 packet; the maximum is 127 packets. The default is 7 packets.

llc2 n2 *retry-count*

Use the **llc2 n2** interface configuration command to control the amount of times the router retries sending unacknowledged frames or repolls remote busy stations.

retry-count Number of times the router retries operations. The minimum is 1; the maximum is 255. The default is 8 retries.

llc2 t1-time *milliseconds*

Use the **llc2 t1-time** interface configuration command to control the amount of time the router will wait before resending unacknowledged information frames.

milliseconds Number of milliseconds the router waits before resending unacknowledged information frames. The minimum is 1 millisecond; the maximum is 60000 milliseconds. The default is 1000 milliseconds.

llc2 tbusy-time *milliseconds*

Use the **llc2 tbusy-time** interface configuration command to control the amount of time the router waits until repolling a busy remote station.

milliseconds Number of milliseconds the router waits before repolling a busy remote station. The minimum is 1 millisecond; the maximum is 60000 milliseconds. The default is 9600 milliseconds.

llc2 tpf-time *milliseconds*

Use the **llc2 tpf-time** interface configuration command to set the amount of time the router waits for a final response to a poll frame before resending the poll frame.

milliseconds Number of milliseconds the router waits for a final response to a poll frame before resending the poll frame. The minimum is 1; the maximum is 60000. The default is 1000 milliseconds.

llc2 trej-time *milliseconds*

Use the **llc2 trej-time** interface configuration command to control the amount of time a router waits for a correct frame after sending a reject (REJ) command to the remote LLC2 station.

milliseconds Number of milliseconds the router waits for a resend of a rejected frame before sending a reject command to the remote station. The minimum is 1 millisecond; the maximum is 60000 milliseconds. The default is 3200 milliseconds.

llc2 xid-neg-val-time *milliseconds*

Use the **llc2 xid-neg-val-tim** interface configuration command to control the frequency of exchange of identification (XID) transmissions by the router.

milliseconds Number of milliseconds after which the router sends XID frames to other LLC2-speaking stations. The minimum is 0 milliseconds; the maximum is 60000 milliseconds. The default is 0 milliseconds.

llc2 xid-retry-time *milliseconds*

Use the **llc2 xid-retry-time** interface configuration command to set the amount of time the router waits for a reply to exchange of identification (XID) frames before dropping the session.

milliseconds Number of milliseconds the router waits for a reply to XID frame before dropping a session. The minimum is 1 millisecond; the maximum is 60000 milliseconds. The default is 60000 milliseconds.

sdlc address *hexbyte* [**echo**]
no sdlc address *hexbyte*

Use the **sdlc address** interface configuration command to assign a set of secondary stations attached to the serial link. Use the **no** form of this command to remove an assigned secondary station.

hexbyte Hexadecimal number (base 16) indicating the address of the serial link.

echo (Optional) Treats nonecho and echo SDLC addresses as the same address.

sdlc address ff ack-mode

Use the **sdlc address ff ack-mode** interface configuration command to configure the IBM reserved address FF as a valid local address.

sdlc cts-delay *unit*

Use the **sdlc cts-delay** interface configuration command to adjust the delay between the detection of request to send (RTS) and the assertion of clear to send (CTS) on an interface that is in half-duplex mode and that has been configured for DCE.

unit	The delay in microseconds. The valid range is 1 to 64000. Each unit is approximately 5 microseconds. The default is 3 units (approximately 15 microseconds).

[**no**] **sdlc dlsw** *sdlc-address sdlc-address*

Use the **sdlc dlsw** interface configuration command to attach sdlc addresses to DLSw+. Use the no form of the command to cancel the configuration.

sdlc-address	SDLC address in hex. The valid range is 1 through FE.

sdlc dte-timeout *unit*

Use the **sdlc dte-timeout** interface configuration command to adjust the amount of time a data terminal equipment (DTE) interface waits for the DCE to assert a CTS (clear to send) before dropping an RTS (request to send).

unit	Timeout wait interval in microseconds. The valid range is 10 to 64000. Each unit is approximately 5 microseconds. The default is 10 units (approximately 50 microseconds).

[**no**] **sdlc frmr-disable**

Use the **sdlc frmr-disable** interface configuration command to indicate that secondary stations on a particular serial link do not support Frame Rejects (FRMRs) or error indications. Use the **no** form of this command to specify that the secondary station does support FRMRs.

[**no**] **sdlc hdx**

Use the **sdlc hdx** interface configuration command to configure an interface for half-duplex mode. Use the **no** form of this command to reset the interface for full-duplex mode.

sdlc holdq *address queue-size*

Use the **sdlc holdq** interface configuration command to control the maximum number of packets that can be held in a buffer before being transmitted to a remote SDLC station.

address	SDLC address for which you are specifying a queue size.
queue-size	Router's local send window size. The minimum is 1 packet. No maximum value has been established. The default is 12 packets.

sdlc k *window-size*

Use the **sdlc k** interface configuration command to set the window size in order to control the maximum number of information frames a router receives before sending an acknowledgment.

window-size	Router's local send window size. The minimum is 1 frame; the maximum is 7 frames. The default is 7 frames.

sdlc line-speed *rate*

Use the **sdlc line-speed** interface configuration command to enable adaptive SDLC T1.

rate Clockrate in bits per second.

sdlc n1 *bit-count*

Use the **sdlc n1** interface configuration command to control the maximum size of an incoming frame.

bit-count Number indicating bit size. Frames that exceed this size are rejected. The minimum is 1 bit. The maximum is 12000 bits. The default is 12000 bits.

sdlc n2 *retry-count*

Use the **sdlc n2** interface configuration command to determine the number of times that a router resends a frame before terminating the SDLC session.

retry-count Number of retry attempts. When this number is exceeded, the SDLC station terminates its session with the other station. The minimum is 1. The maximum is 255. The default is 20 retries.

[**no**] **sdlc partner** *mac-address sdlc-address*

Use the **sdlc partner** command to specify the destination address with which an LLC session is established for the SDLC station. Use the **no** form of this command to cancel the configuration.

mac-address The 48-bit MAC address of the Token Ring host

sdlc-address SDLC address of the serial device that will communicate with the Token Ring host. The valid range is 1 through FE.

[**no**] **sdlc poll-limit-value** *count*

Use the **sdlc poll-limit-value** interface configuration command to control how many times a single secondary station can be polled for input before the next station must be polled. Use the **no** form of this command to retrieve the default value.

count	Number of times the router can poll one secondary station before proceeding to the next station. The minimum is 1; the maximum is 10. The default is 1 time.

[**no**] **sdlc poll-pause-timer** *milliseconds*

Use the **sdlc poll-pause-timer** interface configuration command to control how long the router pauses between sending each poll frame to secondary stations on a single serial interface. Use the **no** form of this command to retrieve the default value.

milliseconds	Number of milliseconds that the router waits before sending the poll frame to a single serial interface. The minimum is 100; the maximum is 10000. The default is 100 milliseconds.

sdlc poll-wait-timeout *milliseconds*

Use the **sdlc poll-wait-timeout** interface configuration command when the router has been configured for local acknowledgment and some form of SDLC communication (SDLLC or STUN, for example), to specify the interval the router will wait for polls from a primary node before timing out that connection.

milliseconds	Number of milliseconds the router will wait for a poll from the primary station before timing out the connection to the primary station. The minimum is 10; the maximum is 64000. The default is 10000 milliseconds.

sdlc qllc-prtnr *virtual-mac-address sdlc-address*

To establish correspondence between an SDLC and QLLC connection, use the **sdlc qllc-prtnr** interface configuration command.

virtual-mac-address	The virtual MAC address in the form H.H.H.
sdlc-address	SDLC address in hexadecimal. The valid range is 1 through FE.

[**no**] **sdlc role** {**none** \| **primary** \| **secondary** \| **prim-xid-poll**}

Use the **sdlc role** interface configuration command to establish the router to be either a primary or secondary SDLC Station. Use the **no** form of this command to cancel the designation.

none	Establishes the router as either a primary or secondary station, depending on the end stations.
primary	Establishes the router as a primary station.
secondary	Establishes the router as a secondary station.
prim-xid-poll	Establishes the router as a primary station when the end station is configured as a secondary NT2.1.

sdlc rts timeout *unit*

Use the **sdlc rts timeout** interface configuration command to adjust the amount of time the interface waits for the DCE to assert clear to send (CTS) before dropping a request to send (RTS). Use this command on an interface that is in half-duplex mode and that has been configured for DCE.

unit	The amount of time in microseconds. The valid range is 10 to 64000. Each unit is approximately 5 microseconds. The default is 10 units (approximately 50 microseconds).

[**no**] **sdlc sdlc-largest-frame** *address size*

Use the **sdlc sdlc-largest-frame** interface configuration command to indicate the largest information frame (I-frame) size that can be sent or received by the designated SDLC station. Use the **no** form of this command to return to the default value.

address	Address of the SDLC station that will communicate with the router.
size	Largest frame size that can be sent or received.

sdlc simultaneous {**full-datamode** \| **half-datamode**}

To enable an interface configured as a primary SDLC station to operate in two-way simultaneous mode, use the **sdlc simultaneous** interface configuration command.

full-datamode	Enables the primary station to send data to and receive data from the polled secondary station.
half-datamode	Prohibits the primary station from sending data to the polled secondary station.

sdlc slow-poll *seconds*
no sdlc slow-poll

Use the **sdlc slow-poll** interface configuration command to enable the slow-poll capability of the router as a primary SDLC station. Use the **no** form of this command to disable slow-poll capability.

seconds	Amount of time in seconds; the default is 10 seconds.

sdlc t1 *milliseconds*

Use the **sdlc t1** interface configuration command to control the amount of time the router waits for an acknowledgment to a frame or sequence of frames.

milliseconds	Number of milliseconds that the router waits. The minimum is 1; the maximum is 64000. The default is 3000 milliseconds.

[**no**] **sdlc vmac** *mac-address*

Use the **sdlc vmac** interface configuration command to configure a MAC address for the serial interface. Use the **no** form of this command to disable the configuration.

mac-address	The 48-bit MAC address of the Token Ring host

[**no**] **sdlc xid** *address xid*

Use the **sdlc xid** interface configuration command to specify an eXchanged ID (XID) value appropriate for the designated SDLC station associated with this serial interface. Use the **no** form of this command to disable XID processing for this address.

address	Address of the SDLC station associated with this interface.
xid	XID the router will use to respond to XID requests the router receives. This value must be 4 bytes (8 digits) in length and is specified with hexadecimal digits.

show interfaces

Use the **show interfaces** privileged EXEC command to display the SDLC information for a given SDLC interface.

show llc2

Use the **show llc2** privileged EXEC command to display the LLC2 connections active in the router.

IBM Network Media Translation Commands

This chapter describes the function and displays the syntax of each SDLLC and QLLC command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **qllc largest-packet** *virtual-mac-addr max-size*

Use the **qllc largest-packet** interface configuration command to indicate the maximum size of the SNA packet that can be sent or received on an X.25 interface configured for QLLC conversion. Use the **no** form of this command to restore the default largest packet size.

virtual-mac-addr	Virtual MAC address associated with the remote X.25 device, as defined using the **x25 map** or **x25 pvc** commands. This address is written as a dotted triple of four-digit hexadecimal numbers.
max-size	Maximum size, in bytes, of the SNA packet that can be sent or received on the X.25 interface configured for QLLC conversion. This value agrees with the value configured in the remote SNA device. The valid range is 0 through 1024.

[**no**] **qllc partner** *virtual-mac-addr mac-addr*

Use the **qllc partner** interface configuration command to enable a router configured for QLLC conversion to open a connection to the local Token Ring device on behalf of the remote X.25 device when an incoming call is received. Use the **no** form of this command to disable this capability.

virtual-mac-addr	Virtual MAC address associated with the remote X.25 device, as defined using the **x25 map** or **x25 pvc** command. This address is written as a dotted triple of four-digit hexadecimal numbers.
mac-addr	48-bit MAC address of the Token Ring host that will communicate with the remote X.25 device.

[**no**] **qllc sap** *virtual-mac-addr ssap dsap*

Use the **qllc sap** interface configuration command to associate a SAP value other than the default SAP value with a serial interface configured for X.25 communication and QLLC conversion. The **no** form of this command returns this SAP value to its default state.

virtual-mac-addr	Virtual MAC address associated with the remote X.25 device, as defined using the **x25 map** or **x25 pvc** command.
ssap	Source SAP value. It can be a decimal number in the range 2 through 254.
dsap	Destination SAP value. It can be a decimal number in the range 2 through 254.

[**no**] **qllc srb** *virtual-mac-addr srn trn*

Use the **qllc srb** interface configuration command to enable the use of QLLC conversion on a serial interface configured for X.25 communication. The **no** form of this command disables QLLC conversion on the interface.

virtual-mac-addr Virtual MAC address associated with the remote X.25 device, as defined using the **x25 map** or **x25 pvc** command. It can be 1 to 15 digits long.

srn Source ring number. This value defines a virtual ring for all of the remote X.25 devices attached to the QLLC interface. Any number of QLLC conversion connections using the same X.25 serial interface can share a common source ring. However, this source ring must be a unique hexadecimal ring number within the source-bridged network.

trn Target ring number. It must be a virtual ring group that has been defined with the **source-bridge ring-group** command. If the router has only one Token Ring interface and is bridging from the remote X.25 devices to this interface, then *trn* is the number of the ring on that Token Ring interface. If the router has several Token Ring interfaces and interconnects them by means of the **source-bridge ring-group** command, then *trn* is the number of that virtual ring group, as assigned using the **source-bridge ring-group** global configuration command.

[**no**] **qllc xid** *virtual-mac-addr xid*

Use the **qllc xid** interface configuration command to associate an XID value with the remote X.25 device that communicates through the router using QLLC conversion. The **no** form of this command disables XID processing for this address.

virtual-mac-addr	Virtual MAC address associated with the remote X.25 device, as defined using the **x25 map** or **x25 pvc** command.
xid	Combined XID IDBLK and XID IDNUM you are associating with the X.25 device at this X.121 address. This hexadecimal value must be four bytes (eight digits) in length.

[**no**] **sdllc partner** *mac-address sdlc-address*

Use the **sdllc partner** interface configuration command to enable device-initiated connections for SDLLC. This command must be specified for the serial interface that links to the serial line device. Use the **no** form of this command to cancel the original instruction.

mac-address	48-bit MAC address of the Token Ring host.
sdlc-address	SDLC address of the serial device that will communicate with the Token Ring host.

[**no**] **sdllc ring-largest-frame** *value*

Use the **sdllc ring-largest-frame** interface configuration command to indicate the largest I-frame size that can be sent to or received from the LLC2 primary station. Use the **no** form of this command to return to the default.

value	Frame size in bytes. The default is 516 bytes.

[**no**] **sdllc sap** *sdlc-address ssap dsap*

Use the **sdllc sap** interface configuration command to associate a service access point (SAP) value other than the default SAP value with a serial interface configured for SDLLC. Use the **no** form of this command to return this SAP value to 4, the default value.

sdlc-address	Virtual MAC address associated with the remote SDLC device.
ssap	Source SAP value. It must be in the range 1 through 254.
dsap	Destination SAP value. It must be in the range 1 through 254.

[**no**] **sdllc sdlc-largest-frame** *address value*

Use the **sdllc sdlc-largest-frame** interface configuration command to indicate the largest information frame (I-frame) size that can be sent or received by the designated SDLC station. Use the **no** form of this command to return to 265, the default value.

address	Address of the SDLC station that will communicate with the Token Ring host.
value	Largest frame size that can be sent or received by this SDLC station.

[**no**] **sdllc traddr** *xxxx.xxxx.xx00 lr bn tr*

Use the **sdllc traddr** interface configuration command to enable the use of SDLLC Media Translation on a serial interface. The address specified is a MAC address to be assigned to the serial station. Use the **no** form of this command to disable SDLLC media translation on the interface.

xxxx.xxxx.xx00	MAC address to be assigned to the serial interface.
lr	SDLLC virtual ring number.
bn	SDLLC bridge number.
tr	SDLLC target ring number.

[**no**] **sdllc xid** *address xxxxxxxx*

Use the **sdllc xid** interface configuration command to specify an exchanged ID (XID) value appropriate for the designated SDLC station associated with this serial interface. Use the **no** form of this command to disable XID processing for this address.

address	Address of the SDLC station associated with this interface.
xxxxxxxx	XID the router will use to respond to XID requests the router receives on the Token Ring (LLC2) side of the connection. This value must be 4 bytes (8 digits) long and is specified with hexadecimal digits.

show interfaces

Use the **show interfaces** privileged EXEC command to display the SDLC information for a given SDLC interface.

show qllc

Use the **show qllc** EXEC command to display the current state of any QLLC connections.

show sdllc local-ack

Use the **show sdllc local-ack** privileged EXEC command to display the current state of any current local acknowledgment connections and any configured passthrough rings.

[**no**] **source-bridge fst-peername** *local-interface-address*

Use the **source-bridge fst-peername** global configuration command to set up a Fast-Sequenced Transport (FST) peer name. Use the **no** form of this command to disable the IP address assignment.

local-interface-address	IP address to assign to the local router.

[**no**] **source-bridge qllc-local-ack**

Use the **source-bridge qllc-local-ack** global configuration command to enable or disable QLLC local acknowledgment for all of the router's QLLC conversion connection. The **no** form of this command disables this capability.

source-bridge remote-peer *ring-group* **fst** *ip-address* [**lf** *size*]
  [**version** *number*]
no source-bridge remote-peer *ring-group* **fst** *ip-address*

Use the **source-bridge remote-peer fst** global configuration command to specify a Fast-Sequenced Transport (FST) encapsulation connection. Use the **no** form of this command to disable the previous assignments.

ring-group	Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.
ip-address	IP address of the remote peer with which the router will communicate.
lf *size*	(Optional) Maximum size frame to be sent to this remote peer. The router negotiates all transit routes down to this size or lower. Use this argument to prevent timeouts in end hosts by reducing the amount of data they have to transmit in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.
version *number*	(Optional) Forces RSRB protocol version number for the remote peer. Because all FST peers support version 2 RSRB, the **version** keyword is always specified.

source-bridge remote-peer *ring-group* **interface** *interface-name*
[*mac-address*] [**lf** *size*]
no source-bridge remote-peer *ring-group* **interface** *interface-name*

Use the **source-bridge remote-peer interface** global configuration command when specifying a point-to-point direct encapsulation connection. Use the **no** form of this command to disable previous interface assignments.

ring-group — Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

interface-name — Name of the router's serial interface over which to send source-route bridged traffic.

mac-address — (Optional) MAC address for the interface you specify using the *interface-name* argument. This argument is required for nonserial interfaces. You can obtain the value of this MAC address by using the **show interface** command, and then scanning the display for the interface specified by *interface-name*.

lf *size* — (Optional) Maximum size frame to be sent to this remote peer. The router negotiates all transit routes down to this size or lower. This argument is useful in preventing timeouts in end hosts by reducing the amount of data they have to transmit in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

source-bridge remote-peer *ring-group* **tcp** *ip-address* [**lf** *size*]
[**local-ack**] [**priority**]
no source-bridge remote-peer *ring-group* **tcp** *ip-address*

Use the **source-bridge remote-peer tcp** global configuration command to identify the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP. Use the **no** form of this command to remove a remote peer for the specified ring group.

ring-group — Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

ip-address — IP address of the remote peer with which the router will communicate.

lf *size* — (Optional) Maximum size frame to be sent to this remote peer. The router negotiates all transit routes down to this size or lower. Use this argument to prevent timeouts in end hosts by reducing the amount of data they have to transmit in a fixed interval. The valid values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

local-ack — (Optional) LLC2 sessions destined for a specific remote peer are to be locally terminated and acknowledged. Local acknowledgment should be used for LLC2 sessions going to this remote peer.

priority — (Optional) Enables prioritization over a TCP network. You must specify the keyword **local-ack** earlier in the same **source-bridge remote-peer** command. The keyword **priority** is a prerequisite for features such as SNA class of service and SNA LU address prioritization over a TCP network.

[**no**] **source-bridge ring-group** *ring-group*

Use the **source-bridge ring-group** global configuration command to define or remove a ring group from the router configuration. Use the **no** form of this command to cancel previous assignments.

ring-group Ring group number. The valid range is 1 through 4095.

[**no**] **source-bridge sdllc-local-ack**

Use th**e source-bridge sdllc-local-ack** global configuration command to activate local acknowledgment for SDLLC sessions on a particular interface. Use the **no** form of this command to deactivate local acknowledgment for SDLLC sessions.

[**no**] **x25 map qllc** *virtual-mac-addr x121-addr*

Use the **x25 map qllc** interface configuration command to associate a virtual MAC address with the X.121 address of the remote X.25 device with which you plan to communicate using QLLC conversion. The **no** form of this command disables QLLC conversion to this X.121 address.

virtual-mac-addr Virtual MAC address you are associating with the X.25 device at this X.121 address. The router will accept explorer and data packets destined for this MAC address. It can be from 1 to 15 digits long.

x121-addr X.121 address of the remote X.25 device you are associating with this virtual MAC address. It can be from 1 to 15 digits long.

[**no**] **x25 pvc** *circuit* **qllc** *virtual-mac-addr*

Use the **x25 pvc** interface configuration command to associate a virtual MAC address with a permanent virtual circuit (PVC) for communication using QLLC conversion. The **no** form of this command removes the association.

circuit PVC you are associating with the virtual MAC address. This must be lower than any number assigned to switched virtual circuits.

virtual-mac-addr Virtual MAC address you are associating with the X.25 device at this pvc. The router will accept explorer and data packets destined for this MAC address. This virtual MAC address must match the virtual MAC address you specified using the **x25 map qllc** command.

DSPU Configuration Commands

This chapter describes the function and displays the syntax of each DSPU configuration command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **dspu activation-window**

Use the **dspu activation-window** global configuration command 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 **no** form of this command to return to the default window size.

window-size	Number of outstanding unacknowledged activation RUs.

[**no**] **dspu default-pu** [**window** *window-size*] [**maxiframe** *max-iframe*]

Use the **dspu default-pu** global configuration command 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 **no** form of this command to disable the default PU feature.

window *window-size*	(Optional) Defines the send and receive window sizes used across the link. The range is 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Defines the maximum size (in bytes) of an I-frame that can be transmitted or received across the link. The range is 64 bytes to 18,432 bytes. The default is 1472.

[**no**] **dspu enable-host** [**lsap** *local-sap*]

Use the **dspu enable-host** interface configuration command to enable a SAP for use by DSPU host connections. Use the **no** form of this command to disable the SAP.

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) The local SAP address. The default is 12.

[**no**] **dspu enable-pu** [**lsap** *local-sap*]

Use the **dspu enable-pu** interface configuration command to enable a SAP for use by DSPU downstream connections. Use the **no** form of this command to disable the SAP.

lsap	(Optional) Specifies that the local SAP will be activated as a downstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts.
local-sap	(Optional) The local SAP address. The default is 8.

[**no**] **dspu host** *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Use the **dspu host** global configuration command to define a DSPU host. Use the **no** form of this command to delete the DSPU host definition.

host-name	The specified DSPU host.

xid-snd *xid* — The 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 *rmac* — The MAC address of the remote host PU.

rsap *remote-sap* — (Optional) Specifies the SAP address of the remote host PU. The default is 4.

lsap *local-sap* — (Optional) Specifies the local SAP address used by the DSPU to establish connection with the remote host.

window *window-size* — (Optional) Specifies the send and receive window sizes used for the host link. The range is 1 to 127.

maxiframe *max-iframe* — (Optional) Specifies the 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) Specifies the 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) Specifies the 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.

focalpoint — (Optional) Specifies that the host link will be used for the focal point support.

[**no**] **dspu lu** *lu-start* [*lu-end*] [**pool** *pool-name*] [**host** *host-name* *host-lu-start*] [**pu** *pu-name*]

Use the **dspu lu** global configuration command to define a range of LUs on a downstream PU. Use the **no** form of this command to remove the definition.

lu-start	Specifies the starting LU address in the range of LUs to be assigned from a pool or dedicated to a host.
lu-end	(Optional) Specifies the ending LU address in the range of LUs to be assigned from a pool or dedicated to a host.
pool *pool-name*	(Optional) Specifies that each LU in the range of LUs will be assigned from the specified pool.
host *host-name* *host-lu-start*	(Optional) 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*.
pu *pu-name*	(Optional) Specifies the downstream PU for which this range of LUs is being defined.

[**no**] **dspu pool** *pool-name* **host** *host-name* **lu** *lu-start* [*lu-end*] [**inactivity-timeout** *inactivity-minutes*]

Use the **dspu pool lu** global configuration command to define a range of host LUs in an LU pool. Use the **no** form of this command to remove the definition.

pool-name	Specifies the name identifier of the pool.
host *host-name*	Specifies the name of the host that owns the range of host LUs in the pool.
lu *lu-start*	Specifies the starting LU address in the range of host LUs in the pool.

lu-end (Optional) Specifies the ending address (inclusive) of the range of host LUs in the pool. If no ending address is specified, only one LU (identified by *lu-start*) will be defined in the pool.

inactivity-timeout *inactivity-minutes* (Optional) Specifies the 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.

[**no**] **dspu pu** *pu-name* [**rmac** *remote-mac*] [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Use the **dspu pu** global configuration command to define an explicit downstream PU. Use the **no** form of this command to remove the definition.

pu-name Name of the downstream PU.

rmac *remote-mac* (Optional) Specifies the MAC address of the downstream PU.

rsap *remote-sap* (Optional) Specifies the SAP address of the downstream PU. The default is 4.

lsap *local-sap* (Optional) Specifies the 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.

window *window-size* (Optional) Specifies the send and receive sizes used for the downstream PU link. The range is 1 to 127. The default is 7.

maxiframe *max-iframe* (Optional) Specifies the maximum I-frame that can be transmitted or received across the link. The range is 64 to 18,432. The default is 1472.

retries *retry-count* Specifies the 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) Specifies the delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is 1 to 600 seconds. The default is 30.

[**no**] **dspu rsrb** *local-virtual-ring bridge-number target-virtual-ring virtual-macaddr*

Use the **dspu rsrb** global configuration command to define the local virtual ring, the virtual bridge, the target virtual ring, and the virtual MAC address that the DSPU feature will simulate at the RSRB. Use the **no** form of this command to cancel the definition.

local-virtual-ring The DSPU local virtual ring number

bridge-number The bridge number connecting the DSPU local virtual ring and the RSRB target virtual ring. Currently, the bridge number must always be configured with a value of 1.

target-virtual-ring The 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 The DSPU virtual MAC address.

[**no**] **dspu rsrb enable-host** [**lsap** *local-sap*]

Use the **dspu rsrb enable-host** global configuration command to enable an RSRB SAP for use by DSPU host connections. Use the **no** form of this command to disable the RSRB SAP.

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.

[**no**] **dspu rsrb enable-pu** [**lsap** *local-sap*]

Use the **dspu rsrb enable-pu** global configuration command to enable an RSRB SAP for use by DSPU downstream connections. Use the **no** form of this command to disable the SAP.

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.

[**no**] **dspu rsrb start** {*host-name* | *pu-name*}

Use the **dspu rsrb start** global configuration command 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 **no** form of this command to cancel the definition.

host-name	The name of a host defined in a **dspu host** command.
pu-name	The name of a PU defined in a **dspu pu** command.

[**no**] **dspu start** {*host-name* | *pu-name*}

Use the **dspu start** interface configuration command to specify that an attempt will be made to connect to the remote resource defined by host name or pu name. Use the **no** form of this command to cancel the definition.

host-name	The name of a host defined in a **dspu host** command.
pu-name	The name of a PU defined in a **dspu pu** command.

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

Use the **show dspu** privileged EXEC command to display the status of the DSPU feature.

pool *pool-name*	(Optional) Specifies the name of a pool of LUs (as defined by the **dspu pool** command).
pu	(Optional) Specifies the name of defined PU (as defined by either the **dspu pu** or the **dspu host** command).
pu-name	The name of a PU defined in a **dspu pu** command.
host-name	The name of a host defined in a **dspu host** command.
all	(Optional) Show a detailed status.

SNA Frame Relay Access Support Commands

This chapter describes the function and displays the syntax of each SNA Frame Relay access support command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **fras map llc** *mac-address lan-lsap lan-rsap* **serial** *port*
frame-relay *dlci fr-lsap fr-rsap* [**PFID2** | **AFID2** | **FID4**]

Use the **fras map llc** interface configuration command to associate an LLC connection with a Frame Relay connection. Use the **no** form of this command to cancel the association.

mac-address — The MAC address of the downstream SNA device. It is a 48-bit dotted-triple address.

lan-lsap — The local SAP address of the downstream SNA device in hexadecimal. For SNA, the address must be multiples of 4.

lan-rsap — The destination SAP address from the perspective of the downstream SNA device in hexadecimal. For SNA, the address must be multiples of 4.

serial *port* — The serial interface on which Frame Relay is configured.

frame-relay *dlci* — The Frame Relay data link connection identifier.

fr-lsap — The local SAP address of the logical link connection on the CFRAD.

fr-rsap — The destination SAP address on the host.

PFID2 — (Optional) The FID2 SNA transmission header for SNA peripheral traffic.

AFID2 — (Optional) The FID2 transmission header for APPN traffic.

FID4	(Optional) The transmission header used on SNA subarea flows.

[**no**] **fras map sdlc** *sdlc-address* **serial** *port* **frame-relay** *dlci* *fr-lsap fr-rsap* [**PFID2** | **AFID2** | **FID4**]

Use the **fras map sdlc** interface configuration command to associate an SDLC link with a Frame Relay DLCI. Use the **no** form of this command to cancel the association.

sdlc-address	The SDLC address of the downstream SNA device in hexadecimal.
serial *port*	The serial interface on which Frame Relay is configured.
frame-relay *dlci*	The Frame Relay data link connection identifier.
fr-lsap	The local SAP address of the logical link connection on the CFRAD.
fr-rsap	The destination SAP address on the host.
PFID	(Optional) The FID2 SNA transmission header for SNA peripheral traffic.
AFID2	(Optional) The FID2 transmission header for APPN traffic.
FID4	(Optional) The transmission header used on SNA subarea flows.

frame-relay map llc2 *dlci*

Use the **frame-relay map llc2** interface configuration command to map LLC2 traffic to a DLCI.

dlci	The Frame Relay data link connection identifier.

frame-relay map rsrb *dlci*

Use the **frame-relay map rsrb** interface configuration command to specify the DLCI number onto which the RSRB traffic is to be mapped.

dlci	The Frame Relay data link connection identifier.

[**no**] **llc2 dynwind** [**nw** *nw-number*] [**dwc** *dwc-number*]

Use the **llc2 dynwind** interface configuration command to enable dynamic window congestion management. Use the **no** form of this command to cancel the configuration.

nw *nw-number*	(Optional) Specifies a number of frames that must be received to increment the working window value by 1.
dwc *dwc-number*	(Optional) Specifies the number by which the working window value is divided when BECN occurs. Valid numbers are 1, 2, 4, 8, and 16. 1 is a special value that indicates that the working window value should be set to 1 when BECN is indicated.

show fras map

Use the **show fras map** privileged EXEC command to display the mapping and connection state of Frame Relay access support.

DLSw+ Commands

This chapter describes the function and displays the syntax of each DLSw+ configuration command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

[**no**] **dlsw bgroup-list** *group-list*

Use the **dlsw bgroup-list** global configuration command to configure a transparent bridge group list.

group-list	The transparent bridge group list number. The valid range is 1 through 255.

[**no**] **dlsw bridge-group** *group-number*

Use the **dlsw bridge-group** global configuration command to link DLSw+ to the bridge group of the Ethernet LANs. Use the **no** form of this command to disable the link.

group-number	The transparent bridge group to which DLSw+ will be attached. The valid range is 1 through 63.

dlsw disable

Use the **dlsw disable** global configuration command to disable and reenable DLSw+ without altering the configuration.

[**no**] **dlsw duplicate-path-bias** [**load-balance**]

Use the **dlsw duplicate-path-bias** global configuration command to specify how DLSw+ handles duplicate paths to the same MAC address or NetBIOS name. Use the **no** form of the command to return to the default (fault-tolerance).

load-balance	(Optional) Specifies that sessions are load-balanced across duplicate paths.

[**no**] **dlsw explorerq-depth** *queue-max*

Use the **dlsw explorerq-depth** global configuration command to configure the depth of the DLSw explorer packet processing queue. Use the **no** form of this command to disable the explorer packet processing queue.

queue-max	Maximum queue size in packets. The valid range is 25 through 500 packets.

[**no**] **dlsw icannotreach saps** *sap* [*sap* ...]

Use the **dlsw icannotreach saps** global configuration command to configure a list of SAPs not locally reachable by the router. Use the **no** form of this command to remove the list.

sap sap ...	Array of SAPs.

[**no**] **dlsw icanreach** {**mac-exclusive** | **netbios-exclusive** | **mac-address** *mac-addr* [**mask** *mask*] | **netbios-name** *name*}

Use the **dlsw icanreach** global configuration command to configure a resource that is locally reachable by this router. Use the **no** form of this command to remove the resource.

mac-exclusive	Router can reach only the MAC addresses that are user configured.
netbios-exclusive	Router can reach only the NetBIOS names that are user configured.
mac-address *mac-addr*	Configure a MAC address that this router can locally reach.
mask *mask*	(Optional) MAC address mask in hexadecimal h.h.h.
netbios-name *name*	Configure a NetBIOS name that this router can locally reach. Wildcards are allowed.

[**no**] **dlsw local-peer** [**peer-id** *ip-address*] [**group** *group*] [**border**] [**cost** *cost*] [**lf** *size*] [**keepalive** *seconds*] [**passive**] [**promiscuous**]

Use the **dlsw local-peer** global configuration command to define the parameters of the DLSw+ local peer. Use the **no** form of this command to cancel the definitions.

peer-id *ip-address* — (Optional) Local peer IP address; required for FST and TCP.

group *group* — (Optional) Peer group number for this router. The valid range is 1 through 255.

border — (Optional) Enables as a border peer.

cost *cost* — (Optional) Peer cost advertised to remote peers. The valid range is 1 through 5.

lf *size* — (Optional) Largest frame size for this local peer. Valid sizes are the following:
11407-11407 byte maximum frame size
11454-11454 byte maximum frame size
1470-1470 byte maximum frame size
1500-1500 byte maximum frame size
17800-17800 byte maximum frame size
2052-2052 byte maximum frame size
4472-4472 byte maximum frame size
516-516 byte maximum frame size
8144-8144 byte maximum frame size

keepalive *seconds* — (Optional) Default remote peer keepalive interval in seconds. The valid range is 0 through 1200 seconds.

passive — (Optional) Specifies that the router will not initiate remote peer connections.

promiscuous — (Optional) Accepts connections from nonconfigured remote peers.

[**no**] **dlsw mac-addr** *mac-addr* {**rif** *rif-entry* | **ring-group** *ring* | **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*} | **group** *group*}

Use the **dlsw mac-addr** global configuration command to configure a static MAC address. Use the **no** form of this command to cancel the configuration.

macaddr	Specifies the MAC address.
rif *rif-entry*	Maps the MAC address to a specified routing information field (RIF). The RIF entry is a hexadecimal number in the form h.h...
ring-group *ring*	Maps the MAC address to a ring number or ring group number. The valid range is 1 through 4095.
remote-peer	Maps the MAC address to a specific remote peer.
interface serial *number*	Specifies the remote peer by direct serial interface.
ip-address *ip-address*	Specifies the remote peer by IP address.
group *group*	Maps the MAC address to a specified peer group. Valid numbers are in the range 1 through 255.

[**no**] **dlsw netbios-name** *netbios-name* {**rif** *rif-entry* | **ring-group** *ring* | **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*} | **group** *group*}

Use the **dlsw netbios-name** global configuration command to configure a static NetBIOS name. Use the **no** form of this command to cancel the configuration.

netbios-name	Specifies the NetBIOS name. Wildcards are allowed.
rif *rif-string*	Maps the NetBIOS name to a specified RIF.
ring-group *ring*	Maps the NetBIOS name to a ring number or ring group number.
remote-peer	Maps the NetBIOS name to a specific remote peer.

interface serial *number* — Specifies the remote peer by direct interface.

ip-address *ip-address* — Specifies the remote peer by IP address.

group *group* — Maps the NetBIOS name to a specified peer group. Valid numbers are in the range 1 through 255.

[**no**] **dlsw peer-on-demand-defaults fst** [**bytes-netbios-out**
bytes-list-name | **cost** *cost* | **host-netbios-out** *host-list-name* |
keepalive *keepalive* | **lsap-output-list** *access-list-number* |
port-list *portnumber*]

Use the **dlsw peer-on-demand-defaults fst** global configuration command to configure FST for peer-on-demand transport. Use the **no** form of this command to disable the previous assignment.

bytes-netbios-out *bytes-list-name* — Configures NetBIOS bytes output filtering for peer-on-demand peers. The *bytes-list-name* is the name of the previously defined netbios bytes access list filter.

cost *cost* — Specifies the cost to reach peer-on-demand peers. The valid range is 1 through 5. The default cost is 3.

host-netbios-out *host-list-name* — Configures NetBIOS host output filtering for peer-on-demand peers. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.

keepalive *keepalive* — Configures the peer-on-demand keepalive interval. The valid range is 0 through 1200 seconds. The default is 30 seconds.

lsap-output-list *access-list-number* — Configures LSAP output filtering for peer-on-demand peers. Valid numbers are in the range 200 through 299.

port-list *portlistnumber* — Configures a port list for peer-on-demand peers. Valid numbers are in the range 0 through 4095.

[**no**] **dlsw peer-on-demand-defaults tcp** [**bytes-netbios-out** *bytes-list-name* | **cost** *cost* | **host-netbios-out** *host-list-name* | **keepalive** *seconds* | **local-ack** | **lsap-output-list** *accesslistnumber* | **port-list** *portnumber* | **priority**]

Use the **dlsw peer-on-demand-defaults tcp** global configuration command to configure TCP for peer-on-demand transport. Use the **no** form of this command to disable the previous assignment.

bytes-netbios-out *bytes-list-name* — Configures NetBIOS bytes output filtering for peer-on-demand peers. The bytes-list-name is the name of the previously defined netbios bytes access list filter.

cost *cost* — Specifies the cost to reach peer-on-demand peers. The valid range is 1 through 5. The default cost is 3.

host-netbios-out *host-list-name* — Configures netbios host output filtering for peer-on-demand peers. Host-list-name is the name of the previously defined netbios host access list filter.

keepalive *seconds* — Configures the peer-on-demand keepalive interval. The valid range is 0 through 1200 seconds. The default is 30 seconds.

local-ack — Configures local acknowledgment for peer-on-demand sessions.

lsap-output-list *accesslistnumber* Configures local SAP (LSAP) output filtering for peer-on-demand peers. Valid numbers are in the range 200 through 299.

port-list *portlistnumber* Configures a port-list for peer-on-demand peers. Valid numbers are in the range 0 through 4095.

priority Configures prioritization for peer-on-demand peers. The default state is off.

[**no**] **dlsw port-list** *list-number* {*type number*}

Use the **dlsw port-list** global configuration command to configure a peer post list. Use the **no** form of this command to disable the previous assignment.

list-number Port list number. The valid range is 1 through 255.

type The interface type, indicated by the keyword **ethernet**, **serial**, or **tokenring**.

number The interface number.

[**no**] **dlsw remote-peer** *ring-group* **fst** *ip-address* [**cost** *cost*] [**lf** *size*] [**keepalive** *seconds*] [**lsap-output-list** *list*] [**host-netbios-out** *host-list-name*] [**bytes-netbios-out** *bytes-list-name*] [**backup-peer** *ip-address*]

Use the **dlsw remote-peer fst** global configuration command to specify a Fast-Sequenced Transport (FST) encapsulation connection for remote peer transport. Use the **no** form of this command to disable the previous assignments.

ring-group — Remote peer ring g2.57

roup list number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

fst *ip-address* — IP address of the remote peer with which the router is to communicate.

cost *cost* — (Optional) Cost to reach this remote peer. The valid range is 1 through 5.

lf *size* — (Optional) Sets the largest frame size for this remote peer. Valid sizes are the following:
11407-11407 byte maximum frame size
11454-11454 byte maximum frame size
1470-1470 byte maximum frame size
1500-1500 byte maximum frame size
17800-17800 byte maximum frame size
2052-2052 byte maximum frame size
4472-4472 byte maximum frame size
516-516 byte maximum frame size
8144-8144 byte maximum frame size

keepalive *seconds* — (Optional) Sets the keepalive interval for this remote peer. The range is 0 through 1200 seconds.

lsap-output-list *list* — (Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range 200 through 299.

host-netbios-out *host-list-name*
(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.

bytes-netbios-out *bytes-list-name*
(Optional) Configures NetBIOS bytes output filtering for this peer. The bytes-list-name is the name of the previously defined NetBIOS bytes access list filter.

backup-peer *ip-address*
(Optional) Configures as a backup to an existing TCP/FST peer.

[**no**] **dlsw remote-peer** *ring-group* **interface serial** *number* [**cost** *cost*] [**lf** *size*] [**keepalive** *seconds*] [**lsap-output-list** *list*] [**host-netbios-out** *host-list-name*] [**bytes-netbios-out** *bytes-list-name*] [**backup-peer** *ip-address*]

Use the **dlsw remote-peer interface** global configuration command when specifying a point-to-point direct encapsulation connection. Use the **no** form of this command to disable previous interface assignments.

ring-group
Remote peer ring group list number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

interface serial *number*
Specifies the remote peer by direct serial interface.

cost *cost*
(Optional) Cost to reach this remote peer. The valid range is 1 through 5.

lf *size*	(Optional) Sets the largest frame size for this remote peer. Valid sizes are the following: 11407-11407 byte maximum frame size 11454-11454 byte maximum frame size 1470-1470 byte maximum frame size 1500-1500 byte maximum frame size 17800-17800 byte maximum frame size 2052-2052 byte maximum frame size 4472-4472 byte maximum frame size 516-516 byte maximum frame size 8144-8144 byte maximum frame size
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is 0 through 1200 seconds.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range 200 through 299.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The bytes-list-name is the name of the previously defined NetBIOS bytes access list filter.

[**no**] **dlsw remote-peer** *ring-group* **tcp** *ip-address* [**priority**] [**cost** *cost*] [**lf** *size*] [**keepalive** *seconds*] [**tcp-queue-max** *size*] [**lsap-output-list** *list*] [**host-netbios-out** *host-list-name*] [**bytes-netbios-out** *bytes-list-name*] [**backup-peer** *ip-address*]

Use th**e dlsw remote-peer tcp** global configuration command to identify the IP address of a peer with which to exchange traffic using TCP. Use the **no** form of this command to remove a remote peer.

ring-group — Remote peer ring group list number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is 1 through 4095.

tcp *ip-address* — IP address of the remote peer with which the router is to communicate.

priority — Enables prioritization features for this remote peer.

cost *cost* — (Optional) The cost to reach this remote peer. The valid range is 1 through 5.

lf *size* — (Optional) Sets the largest frame size for this remote peer. Valid sizes are the following:
11407-11407 byte maximum frame size
11454-11454 byte maximum frame size
1470-1470 byte maximum frame size
1500-1500 byte maximum frame size
17800-17800 byte maximum frame size
2052-2052 byte maximum frame size
4472-4472 byte maximum frame size
516-516 byte maximum frame size
8144-8144 byte maximum frame size

keepalive *seconds* — (Optional) Sets the keepalive interval for this remote peer. The range is 0 through 1200 seconds.

tcp-queue-max *size* — Maximum output TCP queue size for this remote peer. The valid maximum TCP queue size is a number in the range 10 through 2000.

lsap-output-list *list* — (Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range 200 through 299.

host-netbios-out *host-list-name* — (Optional) Configures NetBIOS host output filtering for this peer. The host-list-name is the name of the previously defined NetBIOS host access list filter.

bytes-netbios-out *bytes-list-name* — (Optional) Configures NetBIOS bytes output filtering for this peer. The bytes-list-name is the name of the previously defined NetBIOS bytes access list filter.

backup-peer *ip-address* — (Optional) Configures a backup to an existing TCP/FST peer.

[**no**] **dlsw ring-list** *list-number* **rings** *ring-numbers*

Use the **dlsw ring-list** to configure a ring list, mapping traffic on a local interface to remote peers. Use the **no** form of this command to cancel the definition.

list-number — Ring list number. The valid range is 1 through 255.

rings — Specify one or more physical or virtual ring

ring-number — Physical or virtual ring number. The valid range is 1-4095.

[**no**] **dlsw timer** {**icannotreach-block-time** | **netbios-cache-timeout** |
netbios-explorer-timeout | **netbios-retry-interval** |
netbios-verify-interval | **sna-cache-timeout** |
sna-explorer-timeout
| **sna-retry-interval** | **sna-verify-interval**} *time*

Use the **dlsw timer** global configuration command to tune an existing configuration parameter. Use the **no** form of this command to restore the default parameters.

icannotreach-block-time *time* — Cache life of unreachable resource, during which searches for that resource are blocked. The valid range is 1 through 86400 seconds. The default is 0 (disabled).

netbios-cache-timeout *time* — Cache life of NetBIOS name location for both local and remote reachability cache. The valid range is 1 through 86400 seconds. The default is 16 minutes.

netbios-explore-timeout *time* — Length of time that this router waits for an explorer response before marking a resource unreachable (LAN and WAN). The valid range is 1 through 86400 seconds. The default is 6 seconds.

netbios-retry-interval *time* — NetBIOS explorer retry interval (LAN only). The valid range is 1 through 86400 seconds. The default is 1 second.

netbios-verify-interval *time* — Interval between the creation of a cache entry and when the entry is marked as stale. If a search request comes in for a stale cache entry, a directed verify query is sent to assure that it still exists. The valid range is 1 through 86400 seconds. The default is 4 minutes.

sna-cache-timeout *time* Length of time that an SNA MAC/SAP location cache entry exists before it is discarded (local and remote). The valid range is 1 through 86400 seconds. The default is 16 minutes.

sna-explorer-timeout *time* Length of time that this router waits for an explorer response before marking a resource unreachable (LAN and WAN). The valid range is 1 through 86400 seconds. The default is 3 minutes.

sna-retry-interval *time* Interval between SNA explorer retries (LAN). The valid range is 1 through 86400 seconds. The default is 30 seconds.

sna-verify-interval *time* Interval between the creation of a cache entry and when the entry is marked as stale. If a search request comes in for a stale cache entry, a directed verify query is sent to assure that it still exists. The valid range is 1 through 86400 seconds. The default is 4 minutes.

show dlsw capabilities [**interface** {*type number*} | **ip-address** *ip-address* | **local**]

Use the **show dlsw capabilities** privileged EXEC command to display the configuration of the peer specified or of all peers.

interface *type* (Optional) The interface type is indicated by the keyword **ethernet**, **null**, **serial**, or **tokenring**.

number	(Optional) The interface number.
ip-address *ip-address*	(Optional) Specifies a remote peer by its IP address.
local	(Optional) Specifies the local DLSw peer.

show dlsw circuits

Use the **show dlsw circuit** privileged EXEC command to display the state of all circuits involving this MAC address as a source and destination.

show dlsw fastcache

Use the **show dlsw fastcache** privileged EXEC command to display the fast cache for FST and direct-encapsulated peers.

show dlsw peers [interface {ethernet *number* | null *number* | serial *number* | tokenring *number*} | ip-address *ip-address*]

Use the **show dlsw peers** privileged EXEC command to display DLSw peer information.

interface {**Ethernet** *number* | **Null** *number* | **Serial** *number* | **TokenRing** *number*}	(Optional) Specifies a remote peer by a direct interface.
ip-address *ip-address*	(Optional) Specifies a remote peer by its IP address.

show dlsw reachability

Use the **show dlsw reachability** privileged EXEC command to display DLSw reachability information.

IBM Channel Attach Commands

This chapter describes the function and displays the syntax of each IBM Channel Attach command. For more information about defaults and usage guidelines, see the corresponding chapter of the *Router Products Command Reference* publication.

claw *path device-address ip-address host-name device-name host-app device-app*

Use the **claw** interface configuration command to establish the IBM channel attach configuration for an ESCON Channel Adapter (ECA) interface or Bus and Tag Parallel Channel Adapter (PCA) interface on the Cisco 7000 series. This command defines information that is specific to the interface hardware and the IBM channels supported on the interface.

path	A hexadecimal value in the range of 0x0000 – 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. If not specified, the control unit address and channel logical address default to 0.
device-address	A hexadecimal value in the range of 0x00 – 0xFE. 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	The IP address specified in the host TCP/IP application configuration file.
host-name	The host name specified in the device statement in the host TCP/IP application configuration file.

device-name The CLAW workstation name specified in the device statement in the host TCP/IP application configuration file.

host-app The host application name 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 application file. Otherwise, this value must match the value hard-coded in the host application.

device-app The CLAW workstation application specified in the device statement in the host TCPIP application configuration file. For the initial release of IBM channel attach support, this value will be **TCPIP**, which is a constant specified in the host application file.

channel-protocol [**s** | **s4**]

Use the **channel-protocol** interface configuration command to define a data rate of either 3 megabytes per second or 4.5 megabytes per second for the Parallel Channel Adapter (PCA) daughter card on a Cisco 7000 series router.

s (Optional) Specifies a data rate of 3 megabytes per second.

s4 (Optional) Specifies a data rate of 4.5 megabytes per second.

interface channel *slot*/*port*

Use the **interface channel** interface configuration command to enter interface configuration mode. This command is used only on the Cisco 7000 series.

slot On the Cisco 7000 series, specifies the slot number where the CIP is located.

port On the Cisco 7000 series, specifies the port number where the CIP is located.

show extended channel *slot*/*port* **statistics** [**path** [*device-address*]]

Use the **show extended channel statistics** privileged EXEC command to display information about the channel interface processor (CIP) interfaces on the Cisco 7000 series. 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.

slot On the Cisco 7000 series, specifies the slot number.

port On the Cisco 7000 series, specifies the port number.

path (Optional) This keyword is required if a value is specified for *device-address*. A hexadecimal value in the range of 0x0000 – 0xFFFF. 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) A hexadecimal value in the range of 0x00 – 0xFE. 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.

show extended channel *slot*/*port* **subchannel**

Use the **show extended channel subchannel** privileged EXEC command to display information about the channel interface processor (CIP) interfaces on the Cisco 7000 series. 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.

slot	On the Cisco 7000 series, specifies the slot number.
port	On the Cisco 7000 series, specifies the port number.

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

Use the **show interfaces channel** privileged EXEC command to display information about the channel interface processor (CIP) interfaces on the Cisco 7000 series. 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.

slot	(Optional) On the Cisco 7000 series, specifies the slot number.
port	(Optional) On the Cisco 7000 series, specifies the port number.

INDEX