Cisco IOS Bridging Command Reference

November 2011

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

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

Cisco IOS Bridging Command Reference

CONTENTS

Bridging Commands

access-expression

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

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

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

Syntax Description

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

Defaults

No access expression is defined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

An access expression term specifies a type of access list, followed by its name or number. The result of the term is either true or false, depending on whether the access list specified in the term permits or denies the frame. Table 1 describes the terms that can be used.

Table 1 Access Expression Terms

Access Expression Term	Definition
lsap(2nn)	Subnetwork Access Protocol access list to be evaluated for this frame (Cisco 200 series).
type(2nn)	Subnetwork Access Protocol (SNAP) type access list to be evaluated for this frame (Cisco 200 series).
smac(7nn)	Access list to match the source MAC address of the frame (Cisco 700 series).

Table 1 Access Expression Terms (continued)

Access Expression Term	Definition
dmac(7nn)	Access list to match the destination MAC address of the frame (Cisco 700 series).
netbios-host(name)	NetBIOS-host access list to be applied on NetBIOS frames traversing the interface.
netbios-bytes(name)	NetBIOS-bytes access list to be applied on NetBIOS frames traversing the interface.

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

Table 2 Boolean Operators for Access Expression Terms

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

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

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

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

Related Commands

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

access-list

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

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

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

Syntax Description

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

Defaults

No access list is configured.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

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

Usage Guidelines

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

Examples

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

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

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

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

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

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

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

Related Commands

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

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

access-list (extended-ibm)

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

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

Syntax Description

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

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

Defaults

No extended access lists are established.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

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

```
Router# show interfaces crb

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

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

Table 3 describes significant fields shown in the display.

Table 3 show interfaces crb Field Descriptions

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

Related Commands

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

access-list (standard-ibm)

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

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

no access-list *access-list-number*

Syntax Description

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

Defaults

No MAC address access lists are established.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

access-list (type-code-ibm)

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

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

no access-list *access-list-number*

Syntax Description

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

Defaults

No type-code access lists are built.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Access lists are evaluated according to the following algorithm:

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

Packets are treated according to the following algorithm:

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

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

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

Examples

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

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

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

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

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

Related Commands

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

bridge acquire

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

bridge *bridge-group* **acquire**

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

Syntax Description

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

Defaults

Enabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

```
no bridge 1 acquire
```

Related Commands

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

bridge address

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

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

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

Syntax Description

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

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

Related Commands

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

bridge bitswap-layer3-addresses

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

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

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

Syntax Description

bridge-group	Bridge group number.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
no ip routing
!
interface ethernet 0
 bridge-group 1
!
```

```
interface token-ring 0
 bridge-group 1
!
!
bridge 1 protocol ieee
bridge 1 bitswap-layer3-addresses
```

bridge bridge

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

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

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

Syntax Description

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

Defaults

Bridge every protocol.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
no bridge 1 bridge ip
```

Related Commands

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

bridge circuit-group pause

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

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

Syntax Description

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

Defaults

The default forward delay interval is 0.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

bridge circuit-group source-based

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

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

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

Syntax Description

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

Defaults

No bridge-group interface is assigned.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge cmf

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

bridge cmf

no bridge cmf

Syntax Description

This command has no arguments or keywords.

Defaults

CMF is disabled.

Command Modes

Global configuration

Command History

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

Examples

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

```
bridge cmf
```

Related Commands

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

bridge crb

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

bridge crb

no bridge crb

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
bridge crb
```

Related Commands

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

bridge domain

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

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

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

Syntax Description

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

Defaults

Single bridge domain. The default domain number is 0.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

```
bridge 1 domain 3
```

Related Commands

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

bridge forward-time

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

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

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

Syntax Description

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

Defaults

30-second delay

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

bridge hello-time

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

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

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

Syntax Description

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

Defaults

1 second

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge irb

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

bridge irb

no bridge irb

Syntax Description

This command has no arguments or keywords.

Defaults

Integrated routing and bridging (IRB) is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following shows how to enable integrated routing and bridging:

```
bridge irb
```

Related Commands

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

bridge lat-service-filtering

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

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

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

Syntax Description

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

Defaults

LAT service filtering is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge max-age

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

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

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

Syntax Description

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

Defaults

15 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge multicast-source

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

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

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

Syntax Description

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

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

```
bridge 2 multicast-source
```

Related Commands

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

bridge priority

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

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

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
bridge 1 priority 100
```

Related Commands

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

bridge protocol

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

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

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

Syntax Description

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

Defaults

No Spanning Tree Protocol is defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
bridge 1 protocol dec
```

Related Commands

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

bridge protocol ibm

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

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

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

Syntax Description

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

Defaults

No bridge group is defined.

Command Modes

Global configuration

Command History

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

Examples

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

```
bridge 1 protocol ibm
```

Related Commands

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

bridge route

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

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

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

Syntax Description

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

Defaults

No default bridge group or protocol is specified.

Command Modes

Global configuration

Command History

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

Examples

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

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

Related Commands

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

bridge subscriber-policy

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

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

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

Syntax Description

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

Defaults

Table 4 shows the default values that are applied if no forward or filter decisions have been specified for the subscriber policy:

Table 4 Packet Default Values

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge-group

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

bridge-group *bridge-group*

no bridge-group *bridge-group*

Syntax Description

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

Defaults

No bridge group interface is assigned.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
bridge-group cbus-bridging	Enables autonomous bridging on a ciscoBus2 controller.
bridge-group circuit-group	Assigns each network interface to a bridge group.

Command	Description
bridge-group input-pattern-list	Associates an extended access list with a particular interface in a particular bridge group.
bridge-group output-pattern-list	Associates an extended access list with a particular interface.
bridge-group spanning-disabled	Disables the spanning tree on a given interface.

bridge-group aging-time

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

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

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

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
seconds	Aging time, in the range from 10 to 1000000 seconds. The default is 300 seconds.

Defaults

300 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

If hosts on a bridged network are likely to move, decrease the aging time to enable the bridge to adapt quickly to the change. If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time and thus reduce the possibility of flooding when the hosts send again.

Examples

The following example sets the aging time to 200 seconds:

```
bridge-group 1 aging-time 200
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

bridge-group cbus-bridging

To enable autonomous bridging on a ciscoBus2 controller, use the **bridge-group cbus-bridging** command in interface configuration mode. To disable autonomous bridging, use the **no** form of this command.

bridge-group *bridge-group* **cbus-bridging**

no bridge-group *bridge-group* **cbus-bridging**

Syntax Description

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

Defaults

Autonomous bridging is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Normally, bridging takes place on the processor card at interrupt level. When autonomous bridging is enabled, bridging takes place entirely on the ciscoBus2 controller, substantially improving performance.

You can enable autonomous bridging on Ethernet, FDDI (FCIT) and High-Speed Serial Interface (HSSI) interfaces that reside on a ciscoBus2 controller. Autonomous bridging is not supported on Token Ring interfaces, regardless of the type of bus in use.

To enable autonomous bridging on an interface, first define that interface as part of a bridge group. When a bridge group includes both autonomously and normally bridged interfaces, packets are autonomously bridged in some cases, but bridged normally in others. For example, when packets are forwarded between two autonomously bridged interfaces, those packets are autonomously bridged. But when packets are forwarded between an autonomously bridged interface and one that is not, the packet must be normally bridged. When a packet is flooded, the packet is autonomously bridged on autonomously bridged interfaces, but must be normally bridged on any others.

Note In order to maximize performance when using a ciscoBus2 controller, use the **bridge-group cbus-bridging** command to enable autonomous bridging on any Ethernet, FDDI, or HSSI interface.

Note You can filter by MAC-level address on an interface only when autonomous bridging is enabled on that interface; autonomous bridging disables all other filtering and priority queueing.

Examples

In the following example, autonomous bridging is enabled on Ethernet interface 0:

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

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

bridge-group circuit-group

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

bridge-group *bridge-group* **circuit-group** *circuit-group*

no bridge-group *bridge-group* **circuit-group** *circuit-group*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
circuit-group	Circuit group number. The range is from 1 to 9.

Defaults

No bridge group interface is assigned.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Circuit groups are primarily intended for use with High-Speed Serial Interface (HSSI)-encapsulated serial interfaces. They are not supported for packet-switched networks such as X.25 or Frame Relay. Circuit groups are best applied to groups of serial lines of equal bandwidth, but can accommodate mixed bandwidths.

Note You must configure bridging before you configure a circuit group on an interface.

Examples

In the following example, Ethernet interface 0 is assigned to circuit group 1 of bridge group 1:

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

Related Commands

Command	Description
bridge circuit-group pause	Configures the interval during which transmission is suspended in a circuit group after circuit group changes take place.
bridge circuit-group source-based	Uses just the source MAC address for selecting the output interface.

bridge-group input-address-list

To assign an access list to a particular interface, use the **bridge-group input-address-list** command in interface configuration mode. To remove an access list from an interface, use the **no** form of this command.

bridge-group *bridge-group* **input-address-list** *access-list-number*

no bridge-group *bridge-group* **input-address-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the **access-list** command. It must be in the range from 700 to 799.

Defaults

No access list is assigned.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use an access list to filter packets received on a particular interface, based on the MAC source addresses (of the packets).

Examples

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

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

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge address	Filters frames with a particular MAC-layer station source or destination address.
bridge-group output-address-list	Assigns an access list to a particular interface for filtering the MAC destination addresses of packets that would ordinarily be forwarded out that interface.

bridge-group input-lat-service-deny

To specify the group codes by which to deny access upon input, use the **bridge-group input-lat-service-deny** command in interface configuration mode. To remove this access condition, use the **no** form of this command.

bridge-group *bridge-group* **input-lat-service-deny** *group-list*

no bridge-group *bridge-group* **input-lat-service-deny** *group-list*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
group-list	List of local-area transport (LAT) service groups. Single numbers and ranges are permitted. Ranges are specified with a dash between the first and last group numbers in the range. Specify a zero (0) to disable the LAT group code for the bridge group.

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This command prevents the system from bridging any LAT service advertisement that has any of the specified groups set.

Examples

The following example causes any advertisements with groups 6, 8, and 14 through 20 to be dropped:

```
interface ethernet 0
 bridge-group 1 input-lat-service-deny 6 8 14-20
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-lat-service-permit	Specifies the group codes by which to permit access upon input.
bridge-group output-lat-service-deny	Specifies the group codes by which to deny access upon output.

bridge-group input-lat-service-permit

To specify the group codes by which to permit access upon input, use the **bridge-group input-lat-service-permit** command in interface configuration mode. To remove this access condition, use the **no** form of this command.

bridge-group *bridge-group* **input-lat-service-permit** *group-list*

no bridge-group *bridge-group* **input-lat-service-permit** *group-list*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
group-list	local-area transport (LAT) service groups. Single numbers and ranges are permitted. Specify a zero (0) to disable the LAT group code for the bridge group.

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This command causes the system to bridge only those service advertisements that match at least one group in the group list specified by the *group-list* argument.

If a message specifies group codes in both the deny and permit list, the message is not bridged.

Examples

The following example bridges any advertisements from groups 1, 5, and 12 through 14:

```
interface ethernet 1
 bridge-group 1 input-lat-service-permit 1 5 12-14
```

Related Commands

Command	Description
bridge-group input-lat-service-deny	Specifies the group codes by which to deny access upon input.
bridge-group output-lat-service-permit	Specifies the group codes by which to permit access upon output.

bridge-group input-lsap-list

To filter IEEE 802.2-encapsulated packets on input, use the **bridge-group input-lsap-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **input-lsap-list** *access-list-number*

no bridge-group *bridge-group* **input-lsap-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This access list is applied to all IEEE 802.2 frames received on that interface prior to the bridge-learning process. Subnetwork Access Protocol (SNAP) frames must also pass any applicable Ethernet type-code access list.

Examples

The following example specifies access list 203 on Ethernet interface 1:

```
interface ethernet 1
 bridge-group 3 input-lsap-list 203
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group output-lsap-list	Filters IEEE 802-encapsulated packets on output.

bridge-group input-pattern-list

To associate an extended access list with a particular interface in a particular bridge group, use the **bridge-group input-pattern-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **input-pattern-list** *access-list-number*

no bridge-group *bridge-group* **input-pattern-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned using the extended **access-list** command. Specify a zero (0) to disable the application of the access list on the interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

The following command applies access list 1101 to bridge group 3 using the filter defined in group 1:

```
interface ethernet 0
bridge-group 3 input-pattern-list 1101
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group output-pattern-list	Associates an extended access list with a particular interface.

bridge-group input-type-list

To filter Ethernet- and Subnetwork Access Protocol (SNAP)-encapsulated packets on input, use the **bridge-group input-type-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **input-type-list** *access-list-number*

no bridge-group *bridge-group* **input-type-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

For SNAP-encapsulated frames, the access list is applied against the 2-byte Type field given after the destination service access point (DSAP)/source service access point (SSAP)/Organizationally Unique Identifier (OUI) fields in the frame.

This access list is applied to all Ethernet and SNAP frames received on that interface prior to the bridge learning process. SNAP frames must also pass any applicable IEEE 802 DSAP/SSAP access lists.

Examples

The following example shows how to configure a Token Ring interface with an access list that allows only the local-area transport (LAT) protocol to be bridged:

```
interface tokenring 0
 ip address 172.16.0.0 255.255.255.0
 bridge-group 1
 bridge-group 1 input-type-list 201
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group output-type-list	Filters Ethernet- and SNAP-encapsulated packets on output.

bridge-group lat-compression

To reduce the amount of bandwidth that local-area transport (LAT) traffic consumes on the serial interface by specifying a LAT-specific form of compression, use the **bridge-group lat-compression** command in interface configuration mode. To disable LAT compression on the bridge group, use the **no** form of this command.

bridge-group *bridge-group* **lat-compression**

no bridge-group *bridge-group* **lat-compression**

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Compression is applied to LAT frames being sent out the router through the interface in question.

LAT compression can be specified only for serial interfaces. For the most common LAT operations (user keystrokes and acknowledgment packets), LAT compression reduces LAT's bandwidth requirements by nearly a factor of two.

Examples

The following example compresses LAT frames on the bridge assigned to group 1:

```
bridge-group 1 lat-compression
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

bridge-group output-address-list

To assign an access list to a particular interface for filtering the MAC destination addresses of packets that would ordinarily be forwarded out that interface, use the **bridge-group output-address-list** command in interface configuration mode. To remove an access list from an interface, use the **no** form of this command.

bridge-group *bridge-group* **output-address-list** *access-list-number*

no bridge-group *bridge-group* **output-address-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command.

Defaults

No access list is assigned.

Command Modes

Interface configuration

Command History

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

Examples

The following example assigns access list 703 to Ethernet interface 3:

```
interface ethernet 3
 bridge-group 5 output-address-list 703
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge address	Filters frames with a particular MAC-layer station source or destination address.
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-address-list	Assigns an access list to a particular interface.

bridge-group output-lat-service-deny

To specify the group codes by which to deny access upon output, use the **bridge-group output-lat-service-deny** command in interface configuration mode. To cancel the specified group codes, use the **no** form of this command.

bridge-group *bridge-group* **output-lat-service-deny** *group-list*

no bridge-group *bridge-group* **output-lat-service-deny** *group-list*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
group-list	List of local-area transport (LAT) groups. Single numbers and ranges are permitted.

Defaults

No group codes are assigned.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This command causes the system to not bridge onto this output interface any service advertisements that contain groups matching any of those in the group list.

Examples

The following example prevents bridging of LAT service announcements from groups 12 through 20:

```
interface ethernet 0
 bridge-group 1
 bridge-group 1 output-lat-service-deny 12-20
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.

Command	Description
bridge-group input-lat-service-deny	Specifies the group codes by which to deny access upon input.
bridge-group output-lat-service-permit	Specifies the group codes by which to permit access upon output.

bridge-group output-lat-service-permit

To specify the group codes by which to permit access upon output, use the **bridge-group output-lat-service-permit** command in interface configuration mode. To cancel specified group codes, use the **no** form of this command.

bridge-group *bridge-group* **output-lat-service-permit** *group-list*

no bridge-group *bridge-group* **output-lat-service-permit** *group-list*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
group-list	Local-area transport (LAT) service advertisements.

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled for you to use this command.

This command causes the system to bridge onto an output interface only those service advertisements that match at least one group in the specified group code list.

Note If a message matches both a deny and a permit condition, it will not be bridged.

Examples

The following example allows only LAT service announcements from groups 5, 12, and 20 on a bridge:

```
interface ethernet 0
 bridge-group 1 output-lat-service-permit 5 12 20
```

Related Commands

Command	Description
bridge-group input-lat-service-permit	Specifies the group codes by which to permit access upon input.
bridge-group output-lat-service-deny	Specifies the group codes by which to deny access upon output.

bridge-group output-lsap-list

To filter IEEE 802-encapsulated packets on output, use the **bridge-group output-lsap-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **output-lsap-list** *access-list-number*

no bridge-group *bridge-group* **output-lsap-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Subnetwork Access Protocol (SNAP) frames must also pass any applicable Ethernet type-code access list. This access list is applied just before sending out a frame to an interface.

For performance reasons, specify both input and output type code filtering on the same interface.

Access lists for Ethernet- and IEEE 802-encapsulated packets affect only bridging functions. Such access lists cannot be used to block frames with protocols that are being routed.

Packets bearing an 802.2 LSAP of 0xAAAA qualify for LSAP filtering because they are inherently in 802.3 format. However, because they also carry a Type field, they are matched against any Type filters. Therefore, if you use Link Service Access Point (LSAP) filters on an interface that may bear SNAP-encapsulated packets, you must explicitly permit 0xAAAA.

Examples

The following example specifies access list 204 on Ethernet interface 0:

```
interface ethernet 0
 bridge-group 4 output-lsap-list 204
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-lsap-list	Filters IEEE 802.2-encapsulated packets on input.

bridge-group output-pattern-list

To associate an extended access list with a particular interface, use the **bridge-group output-pattern-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **output-pattern-list** *access-list-number*

no bridge-group *bridge-group* **output-pattern-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Extended access list number you assigned using the extended **access-list** command. Specify a zero (0) to disable the application of the access list on the interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

The following example filters all packets sent by bridge group 3 using the filter defined in access list 1102:

```
interface ethernet 0
 bridge-group 3 output-pattern-list 1102
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-pattern-list	Associates an extended access list with a particular interface in a particular bridge group.

bridge-group output-type-list

To filter Ethernet- and Subnetwork Access Protocol (SNAP)-encapsulated packets on output, use the **bridge-group output-type-list** command in interface configuration mode. To disable this capability, use the **no** form of this command.

bridge-group *bridge-group* **output-type-list** *access-list-number*

no bridge-group *bridge-group* **output-type-list** *access-list-number*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
access-list-number	Access list number you assigned with the standard **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group. This access list is applied just before sending out a frame to an interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

The following example specifies access list 202 on Ethernet interface 0:

```
interface ethernet 0
 bridge-group 2 output-type-list 202
```

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
bridge-group	Assigns each network interface to a bridge group.
bridge-group input-type-list	Filters Ethernet- and SNAP-encapsulated packets on input.

bridge-group path-cost

To set a different path cost, use the **bridge-group path-cost** command in interface configuration mode. To choose the default path cost for the interface, use the **no** form of this command.

bridge-group *bridge-group* **path-cost** *cost*

no bridge-group *bridge-group* **path-cost** *cost*

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
cost	Relative cost of using the path. Path cost can range from 1 to 65535, with higher values indicating higher costs. This range applies regardless of whether the IEEE or Digital Spanning Tree Protocol has been specified.

Defaults

The default path cost is computed from the interface's bandwidth setting. The following are IEEE default path cost values. The Digital path cost default values are different.

- Ethernet—100
- 16-Mb Token Ring—62
- FDDI—10
- HSSI—647
- MCI/SCI Serial—647

Command Modes

Interface configuration

Command History

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

Usage Guidelines

By convention, the path cost is 10000/data rate of the attached LAN (IEEE), or 100000/data rate of the attached LAN (Digital), in megabits per second.

Examples

The following example changes the default path cost for Ethernet interface 0:

```
interface ethernet 0
 bridge-group 1 path-cost 250
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.

bridge-group priority

To set an interface priority, use the **bridge-group priority** command in interface configuration mode. The interface priority is used to select the designated port for this bridge-group on the connected media. One designated port on each medium is needed to compute the spanning tree.

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

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs. It must be a number in the range from 1 to 255.
number	Priority number ranging from 0 to 255 (Digital), or 0 to 64000 (IEEE). The default is 32768 if IEEE Spanning Tree Protocol is enabled on the router or 128 if Digital Spanning Tree Protocol is enabled on the router.

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The lower the number, the more likely it is that the bridge on the interface will be chosen as the root.

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

Examples

The following example increases the likelihood that the root bridge will be the one on Ethernet interface 0 in bridge group 1:

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

The following example shows the **bridge-group priority** help information for 9-bit port number size:

```
Router(config-if)# bridge-group 1 priority ?
<0-255> increments of 2 for IEEE or vlan-bridge, others 1
```

The following example shows the **bridge-group priority** help information for 10-bit port number size:

```
Router(config-if)# bridge-group 1 priority ?
<0-255> increments of 4 for IEEE or vlan-bridge, others 1
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
bridge priority	Configures the priority of an individual bridge, or the likelihood that it will be selected as the root bridge.

bridge-group spanning-disabled

To disable the spanning tree on a given interface, use the **bridge-group spanning-disabled** command in interface configuration mode. To enable the spanning tree on a given interface, use the no form of this command.

bridge-group *bridge-group* **spanning-disabled**

no bridge-group *bridge-group* **spanning-disabled**

Syntax Description

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

Defaults

Spanning tree is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

To enable transparent bridging on an interface, use the **bridge protocol** command to specify the type of Spanning Tree Protocol to be used. The **bridge-group spanning-disabled** command can be used to disable that spanning tree on that interface.

When a *loop-free* path exists between any two bridged subnetworks, you can prevent Bridge Protocol Data Unit (BPDU)s generated in one transparent bridging subnetwork from impacting nodes in the other transparent bridging subnetwork, yet still permit bridging throughout the bridged network as a whole.

For example, when transparently bridged LAN subnetworks are separated by a WAN, you can use this command to prevent BPDUs from traveling across the WAN link. You would apply this command to the serial interfaces connecting to the WAN in order to prevent BPDUs generated in one domain from impacting nodes in the remote domain. Because these BPDUs are prevented from traveling across the WAN link, using this command also has the secondary advantage of reducing traffic across the WAN link.

Note In order to disable the spanning tree, you must make sure that no parallel paths exist between transparently bridged interfaces in the network.

Examples

In the following example, the spanning tree for the serial interface 0 is disabled:

```
interface serial 0
 bridge-group 1 spanning-disabled
```

Related Commands

Command	Description
bridge-group	Assigns each network interface to a bridge group.
bridge protocol	Defines the type of Spanning Tree Protocol.

bridge-group sse

To enable the Cisco silicon switching engine (SSE) switching function, use the **bridge-group sse** command in interface configuration mode. To disable SSE switching, use the **no** form of this command.

bridge-group *bridge-group* **sse**

no bridge-group *bridge-group* **sse**

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Examples

The following shows how to enable SSE switching:

```
bridge-group 1 sse
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.

bridge-group subscriber-loop-control

To enable loop control on virtual circuits associated with a bridge group, use the **bridge-group subscriber-loop-control** command in interface configuration mode. To disable loop control, use the **no** form of this command.

bridge-group *bridge-group* **subscriber-loop-control**

no bridge-group *bridge-group* **subscriber-loop-control**

Syntax Description

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

Defaults

Loop control is disabled.

Command Modes

Interface configuration

Command History

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

Examples

The following shows how to enable loop control on virtual circuits associated with bridge group 1:

```
bridge-group 1 subscriber-loop-control
```

Related Commands

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

bridge-group subscriber-trunk

To specify that an interface is at the upstream point of traffic flow, use the **bridge-group subscriber-trunk** command in interface configuration mode. To remove the specification and reset the interface to a nontrunking port, use the **no** form of this command.

bridge-group *bridge-group* **subscriber-trunk**

no bridge-group *bridge-group* **subscriber-trunk**

Syntax Description

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

Defaults

The interface is set to a nontrunking port.

Command Modes

Interface configuration

Command History

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

Examples

The following example sets bridge group 1 as the upstream point of traffic flow:

```
bridge-group 1 subscriber-trunk
```

Related Commands

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

clear bridge

To remove any learned entries from the forwarding database and to clear the transmit and receive counts for any statically or system-configured entries, use the **clear bridge** command in privileged EXEC mode.

clear bridge *bridge-group*

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows the use of the **clear bridge** command:

```
Router# clear bridge 1
```

Related Commands

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

clear bridge multicast

To clear transparent bridging multicast state information, use the **clear bridge multicast** command in user EXEC or privileged EXEC mode.

clear bridge [*bridge-group*] **multicast** [**router-ports** | **groups** | **counts**]
[*group-address*] [*interface-unit*] [**counts**]

Syntax Description

bridge-group	(Optional) Bridge group number specified in the **bridge protocol** command.
router-ports	(Optional) Clear multicast router ports.
groups	(Optional) Clear multicast groups.
counts	(Optional) Clear RX and TX counts.
group-address	(Optional) Multicast IP address associated with a specific multicast group.
interface-unit	(Optional) Specific interface, such as Ethernet 0.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

If you do not specify arguments or keywords as part of the command, the command clears router ports, group ports, and counts for all configured bridge groups.

Use the **show bridge multicast** command to list transparent bridging multicast state information, then use specific pieces of state information in the **clear bridge multicast** command.

Examples

The following example clears router ports, group ports, and counts for bridge group 1:

```
Router# clear bridge 1 multicast
```

The following example clears the group and count information for the group identified as 235.145.145.223, interface Ethernet 0/3 for bridge group 1:

```
Router# clear bridge 1 multicast groups 235.145.145.223 Ethernet0/3 counts
```

Related Commands

Command	Description
bridge cmf	Enables CMF for all configured bridge groups.
show bridge multicast	Displays transparent bridging multicast state information.

clear dlsw history

To clear all currently inactive circuits from the Data-Link Switching Plus (DLSw+) circuit history, use the **clear dlsw history** command in privileged EXEC mode.

clear dlsw history

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example clears all inactive circuits from the DLSW+ circuit history:

```
clear dlsw history
```

clear dlsw local-circuit

To cause all locally switched Data-Link Switching Plus (DLSw+) circuits to be closed, use the **clear dlsw local-circuit** command in privileged EXEC mode.

clear dlsw local-circuit [*circuit-id*]

Syntax Description

circuit-id	(Optional) Circuit ID for a specific remote circuit. The valid range is 0 to 4294967295.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

A user can specify a circuit ID of a specific circuit to clear rather than clearing all local-switched circuits.

Caution This command also drops the associated Logical Link Control, type 2 (LLC2) session. The command should be used with caution and under the advice of a Cisco engineer.

Examples

The following example closes the locally switched DLSw+ circuit with ID number 100:

```
clear dlsw local-circuit 100
```

clear dlsw transparent

To clear Data-Link Switching Plus (DLSw+) transparent local MAC entries, use the **clear dlsw transparent** command in privileged EXEC mode.

clear dlsw transparent

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command is designed to be used in networks that employ DLSw+ Ethernet redundancy without transparent mappings.

Examples

The following example clears DLSw+ transparent local MAC entries:

```
clear dlsw transparent
```

clear drip counters

To clear duplicate ring protocol (DRiP) counters from the Route Switch Module (RSM) interfaces, use the **clear drip counters** command in privileged EXEC mode.

clear drip counters

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **clear drip counters** command if you want to check whether the router is receiving any packets. The counters will start at 0. If the counters are incrementing, DRiP is active on the router.

Examples

The following example clears DRiP counters:

```
Router# clear drip counters
```

Related Commands

Command	Description
interface vlan	Configures a Token Ring or Ethernet interface on the RSM.
show drip	Displays the status of the DRiP database.

clear netbios-cache

To clear the entries of all dynamically learned NetBIOS names, use the **clear netbios-cache** command in privileged EXEC mode.

clear netbios-cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The Cisco IOS software automatically learns NetBIOS names. This command clears those entries. This command will not remove statically defined name cache entries.

Examples

The following example clears all dynamically learned NetBIOS names:

```
Router# clear netbios-cache
```

Related Commands

Command	Description
netbios enable-name-cache	Enables NetBIOS name caching.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.
show netbios-cache	Displays a list of NetBIOS cache entries.

clear rif-cache

To clear the entire Routing Information Field (RIF) cache, use the **clear rif-cache** command in privileged EXEC mode.

clear rif-cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Some entries in the RIF cache are dynamically added and others are static.

Examples

The following example clears the entire RIF cache:

```
Router# clear rif-cache
```

Related Commands

Command	Description
rif	Enters static source-route information into the RIF cache.
rif timeout	Determines the number of minutes an inactive RIF entry is kept. RIF information is maintained in a cache whose entries are aged.
show rif	Displays the current contents of the RIF cache.

clear source-bridge

To clear the source-bridge statistical counters, use the **clear source-bridge** command in privileged EXEC mode.

clear source-bridge

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Examples

The following example clears the source-bridge statistical counters:

```
Router# clear source-bridge
```

Related Commands

Command	Description
clear bridge	Removes any learned entries from the forwarding database and clears the transmit and receive counts for any statically or system-configured entries.

clear sse

To reinitialize the Silicon Switch Processor (SSP) on the Cisco 7000 series routers with RSP7000, use the **clear sse** command in privileged EXEC mode.

clear sse

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The silicon switching engine (SSE) is on the SSP board in the Cisco 7000 series routers with RSP7000.

Examples

The following example reinitializes the SSP:

```
Router# clear sse
```

clear vlan statistics

To remove virtual LAN statistics from any statically or system-configured entries, use the **clear vlan statistics** command in privileged EXEC mode.

clear vlan statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Examples

The following example clears VLAN statistics:

```
Router# clear vlan statistics
```

Related Commands

Command	Description
show vlan counters	Displays the software-cached counter values.

dlsw multicast

To enable a DLSw router to participate in a multicast group, use the **dlsw multicast** command in global configuration mode. To remove the router from the multicast group, use the **no** form of this command.

dlsw multicast [*multicast-ip-address*]

no dlsw multicast [*multicast-ip-address*]

Syntax Description

multicast-ip-address	(Optional) The IP address used by the multicast group. The default is 224.0.10.0.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

In order for routers to be able to receive multicast traffic through DLSw, they must be properly configured to receive multicasts. The appropriate multicast configuration will depend on the specific topologies used.

The **dlsw multicast** command is implemented together with the DLSw version 2 support (RFC2166). It allows anybody-to-anybody communication without configuring a full mesh of the DLSw peers.

Examples

The following example configures a router to be part of the multicast group using 224.0.11.0 as the multicast address:

```
dlsw local-peer peer-id 172.18.62.11 promiscuous
dlsw multicast 224.0.11.0
```

encapsulation tr-isl trbrf-vlan

To enable Token Ring Inter-Switch Link (TRISL), a Cisco protocol for interconnecting multiple routers and switches and maintaining Token Ring VLAN information as traffic goes between switches, use the **encapsulation tr-isl trbrf-vlan** command in subinterface configuration mode. To disable the TRISL configuration, use the **no** form of this command.

encapsulation tr-isl trbrf-vlan *vlanid* **bridge-num** *bridge-number*

no encapsulation tr-isl trbrf-vlan *vlanid* **bridge-num** *bridge-number*

Syntax Description

vlanid	Number identifying the VLAN.
bridge-num *bridge-number*	Keyword and bridge number assigned to the ISL trunk. Values are from 01 to 15.

Defaults

No default behavior or values

Command Modes

Subinterface configuration

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables TRISL on a Fast Ethernet subinterface:

```
interface Fast Ethernet4/0.2
 encapsulation tr-isl trbrf-vlan 999 bridge-num 14
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
clear vlan statistics	Removes virtual LAN statistics from any statically or system configured entries.
multiring	Enables collection and use of RIF information.
multiring trcrf-vlan	Creates a pseudo ring to terminate the RIF for source-routed traffic and assigns it to a VLAN.
show drip	Displays the status of the DRiP database.
show vlans	Displays virtual LAN subinterfaces.
source-bridge trcrf-vlan	Attaches a TrCRF VLAN to the virtual ring of the router.

ethernet-transit-oui

To choose the Organizational Unique Identifier (OUI) code to be used in the encapsulation of Ethernet Type II frames across Token Ring backbone networks, use the **ethernet-transit-oui** command in subinterface configuration mode. To return the default OUI code, use the **no** form of this command.

ethernet-transit-oui [**90-compatible** | **standard** | **cisco**]

no ethernet-transit-oui

Syntax Description

90-compatible	(Optional) Default OUI form.
standard	(Optional) Standard OUI form.
cisco	(Optional) Cisco's OUI form.

Defaults

The default OUI form is 90-compatible.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Before using this command, you must have completely configured your router using multiport source bridging and transparent bridging. 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.

Table 5 shows the actual OUI codes used, when they are used, and how they compare to Software Release 9.0-equivalent commands.

Table 5 Bridge OUI Codes

Keyword	OUI Used	When Used/Benefits	Software Release 9.0 Command Equivalent
90-compatible	0000F8	By default, when talking to other Cisco routers. Provides the most flexibility.	**no bridge old-oui**

Table 5 Bridge OUI Codes (continued)

Keyword	OUI Used	When Used/Benefits	Software Release 9.0 Command Equivalent
cisco	00000C	Provided for compatibility with future equipment.	None
standard	000000	When talking to IBM 8209 bridges and other vendor equipment. Does not provide for as much flexibility as the other two choices.	**bridge old-oui**

Specify the **90-compatible** keyword when talking to our routers. This keyword provides the most flexibility. When **90-compatible** is specified or the default is used, Token Ring frames with an OUI of 0x0000F8 are translated into Ethernet Type II frames and Token Ring frames with the OUI of 0x000000 are translated into Subnetwork Access Protocol (SNAP)-encapsulated frames. Specify the **standard** keyword when talking to IBM 8209 bridges and other vendor equipment. This OUI does not provide for as much flexibility as the other two choices. The **cisco** keyword oui is provided for compatibility with future equipment.

Do not use the **standard** keyword unless you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity. Only use the **standard** keyword only when you are transferring data between IBM 8209 Ethernet/Token Ring bridges and routers running the source-route translational bridging (SR/TLB) software (to create a Token Ring backbone to connect Ethernets).

Use of the **standard** keyword causes the OUI code in Token Ring frames to always be 0x000000. In the context of the **standard** keyword, an OUI of 0x000000 identifies the frame as an Ethernet Type II frame. (Compare with 90-compatible, where 0x000000 OUI means SNAP-encapsulated frames.)

If you use the **90-compatible** keyword, the router, acting as an SR/TLB, can distinguish immediately on Token Ring interfaces between frames that started on an Ethernet Type II frame and those that started on an Ethernet as a SNAP-encapsulated frame. The distinction is possible because the router uses the 0x0000F8 OUI when converting Ethernet Type II frames into Token Ring SNAP frames, and leaves the OUI as 0x000000 for Ethernet SNAP frames going to a Token Ring. This distinction in OUIs leads to efficiencies in the design and execution of the SR/TLB product; no tables need to be kept to know which Ethernet hosts use SNAP encapsulation and which hosts use Ethernet Type II.

The IBM 8209 bridges, however, by using the 0x000000 OUI for all the frames entering the Token Ring, must take extra measures to perform the translation. For every station on each Ethernet, the 8209 bridges attempt to remember the frame format used by each station, and assume that once a station sends out a frame using Ethernet Type II or 802.3, it will always continue to do so. It must do this because in using 0x000000 as an OUI, there is no way to distinguish between SNAP and Type II frame types. Because the SR/TLB router does not need to keep this database, when 8209 compatibility is enabled with the **standard** keyword, the SR/TLB chooses to translate all Token Ring SNAP frames into Ethernet Type II frames as described earlier in this discussion. Because every nonroutable protocol on Ethernet uses either non-SNAP 802.3 (which traverses fully across a mixed IBM 8209/ router Token Ring backbone) or Ethernet Type II, this results in correct inter connectivity for virtually all applications.

Do not use the **standard** keyword OUI if you want SR/TLB to output Ethernet SNAP frames. Using either the **90-compatible** or **cisco** keyword OUI does not present such a restriction, because SNAP frames and Ethernet Type II-encapsulated frames have different OUI codes on Token Ring networks.

Examples

The following example specifies standard OUI form:

```
interface tokenring 0
 ethernet-transit-oui standard
```

Related Commands

Command	Description
source-bridge transparent	Establishes bridging between transparent bridging and SRB.

frame-relay map bridge broadcast

To bridge over a Frame Relay network, use the **frame-relay map bridge broadcast** command in interface configuration mode. To delete the mapping entry, use the **no** form of this command.

frame-relay map bridge *dlci* **broadcast**

no frame-relay map bridge *dlci* **broadcast**

Syntax Description

dlci	Data Link Connection Identifier (DLCI) number. The valid range is from 16 to 1007.

Defaults

No mapping entry is established.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Bridging over a Frame Relay network is supported on networks that do and do not support a multicast facility.

The following example allows bridging over a Frame Relay network:

```
frame-relay map bridge 144 broadcast
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.

interface bvi

To create the bridge-group virtual interface (BVI) that represents the specified bridge group to the routed world and links the corresponding bridge group to the other routed interfaces, use the **interface bvi** command in global configuration mode. To delete the BVI, use the **no** form of this command.

interface bvi *bridge-group*

no interface bvi *bridge-group*

Syntax Description

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

Defaults

No BVI is created.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You must enable integrated routing and bridging (IRB) before attempting to create a BVI.

When you intend to bridge and route a given protocol in the same bridge group, you must configure the network-layer attributes of the protocol on the BVI. Do not configure protocol attributes on the bridged interfaces. No bridging attributes can be configured on the BVI.

Examples

The following example creates a bridge group virtual interface and associates it with bridge group 1:

```
interface bvi 1
```

Related Commands

Command	Description
bridge irb	Enables the Cisco IOS software to route a given protocol between routed interfaces and bridge groups or to route a given protocol between bridge groups.

interface vlan

To configure a Token Ring or Ethernet interface on a Route Switch Module (RSM) or to create or access a dynamic Switch Virtual Interface (SVI), use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlanid* **type** {**trbrf** | **ethernet**}

no interface vlan *vlanid*

Syntax Description

vlanid	Unique VLAN ID number (1 to 4094) used to create or access a VLAN.
type trbrf	Configures a Token Ring interface on the RSM.
type ethernet	Configures an Ethernet interface on the RSM.

Defaults

Configuring on an RSM

RSM interfaces are not configured.

Creating a Dynamic Switch Virtual Interface

Fast EtherChannel is not specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3(5)T	This command was introduced.
12.2(14)SX	Support for this command was added on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to create Layer 2 VLANs when you create an SVI.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring on an RSM

Valid Token Ring VLAN ID numbers are 2 through 1000.

Routing or bridging to a Token Ring VLAN (TrBRF) on the RSM is done by creating a logical interface to a TrBRF VLAN on the RSM with the **interface vlan** command. The TrBRF VLAN must be defined on the Supervisor module prior to creating the TrBRF interface on the RSM.

Creating a Dynamic Switch Virtual Interface

SVIs are created the first time that you enter the **interface vlan** *vlanid* command for a particular VLAN. The *vlanid* value corresponds to the VLAN tag that is associated with the data frames on an Inter-Switch Link (ISL), the 802.1Q-encapsulated trunk, or the VLAN ID that is configured for an access port. A message displays whenever you create a new VLAN interface, so that you can check if you entered the correct VLAN number.

If you delete an SVI by entering the **no interface vlan** *vlanid* command, the associated initial domain part (IDP) pair is forced into an administrative down state and is marked as deleted. The deleted interface will not be visible in the **show interface** command.

You can reinstate a deleted SVI by entering the **interface vlan** *vlanid* command for the deleted interface. The interface comes back up, but much of the previous configuration is gone.

VLANs 1006 to 1014 are internal VLANs on the Cisco 7600 series router and cannot be used for creating new VLANs.

Examples

Configuring on an RSM

The following example show how to configure an RSM Token Ring interface with VLAN 998:

```
Router(config)# interface vlan 998 type trbrf
 ip address 10.5.5.1 255.255.255.0
```

Creating a Dynamic Switch Virtual Interface

The following example shows the output when you enter the **interface vlan** *vlanid* command for a new VLAN number:

```
Router(config)# interface vlan 23
% Creating new VLAN interface.
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
show drip	Displays the status of the DRiP database.

lnm alternate

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm alternate** command is not available in Cisco IOS 12.3T software.

To specify the threshold reporting link number, use the **lnm alternate** command in interface configuration mode. In order for a LAN Reporting Manager (LRM) to change parameters, it must be attached to the reporting link with the lowest reporting link number, and that reporting link number must be lower than this threshold reporting link number. To restore the default of 0, use the **no** form of this command.

lnm alternate *number*

no lnm alternate

Syntax Description

number	Threshold reporting link number. It must be in the range from 0 to 3.

Defaults

The default threshold reporting link number is 0.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

LAN Network Manager (LNM) employs the concepts of reporting links and reporting link numbers. A reporting link is simply a connection (or potential connection) between an LRM and a bridge. A reporting link number is a unique number used to identify a reporting link. An IBM bridge allows four simultaneous reporting links numbered 0 to 3. Only the LRM attached to the lowest number connection is allowed to change any parameters, and then only when that connection number falls below a certain configurable number. In the default configuration, the LRM connected through link 0 is the only LRM allowed to change parameters.

Note Setting the threshold reporting link number on one interface in a source-route bridge will cause it to appear on the other interface of the bridge, because the command applies to the bridge itself and not to either of the interfaces.

Examples

The following example permits LRMs connected through links 0 and 1 to change parameters:

```
! provide appropriate global configuration command if not currently in your config.
!
! permit 0 and 1
lnm alternate 1
```

The following example permits all LRMs to change parameters in the Cisco IOS software:

```
! provide appropriate global configuration command if not currently in your config.
!
! permit 0, 1, 2, and 3
lnm alternate 3
```

Related Commands

Command	Description
lnm password	Sets the password for the reporting link.

lnm crs

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm crs** command is not available in Cisco IOS 12.3T software.

To monitor the current logical configuration of a Token Ring, use the **lnm crs** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm crs

no lnm crs

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Configuration Report Server service tracks the current logical configuration of a Token Ring and reports any changes to LAN Network Manager (LNM). It also reports on various other activities such as the change of the Active Monitor on a Token Ring.

For more information about the Active Monitor, refer to the *IBM Token Ring Architecture Reference Manual* or the IEEE 802.5 specification.

Examples

The following example disables monitoring of the current logical configuration of a Token Ring:

```
interface tokenring 0
 no lnm crs
```

Related Commands

Command	Description
lnm rem	Monitors errors reported by any station on the ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm disabled

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm disable** command is not available in Cisco IOS 12.3T software.

To disable LAN Network Manager (LNM) functionality, use the **lnm disabled** command in global configuration mode. To restore LNM functionality, use the **no** form of this command.

lnm disabled

no lnm disabled

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 1.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Under some circumstances, you can disable all LNM server functions on the router without having to determine whether to disable a specific server, such as the ring parameter server or the ring error monitor on a given interface.

This command can be used to terminate all LNM server input and reporting links. In normal circumstances, this command should not be necessary because it is a superset of the functions normally performed on individual interfaces by the **no lnm rem** and **no lnm rps** commands.

Examples

The following example disables LNM functionality:

```
lnm disabled
```

Related Commands

Command	Description
lnm pathtrace-disabled	Disables pathtrace reporting to LNM stations.
lnm rem	Monitors errors reported by any station on the ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm express-buffer

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm express-buffer** command is not available in Cisco IOS 12.3T software.

To enable the LAN Network Manager (LNM) Ring Parameter Server (RPS) express buffer function, use the **lnm express-buffer** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm express-buffer

no lnm express-buffer

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The RPS express buffer function allows the router to set the express buffer bit to ensure priority service for frames required for ring station initiation. When this function is enabled, the router sets the express buffer bit in its initialize ring station response, which allows Token Ring devices to insert into the ring during bursty conditions.

Examples

The following example enables the LNM RPS express buffer function:

```
lnm express-buffer
```

lnm loss-threshold

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm loss-threshold** command is not available in Cisco IOS 12.3T software.

To set the threshold at which the Cisco IOS software sends a message informing all attached LAN Network Manager (LNM)s that it is dropping frames, use the **lnm loss-threshold** command in interface configuration mode. To return to the default value, use the **no** form of this command.

lnm loss-threshold *number*

no lnm loss-threshold

Syntax Description

number	Single number expressing the percentage loss rate in hundredths of a percent. The valid range is from 0 to 9999. The default is

Defaults

10 (0.10 percent)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The software sends a message to all attached LNMs whenever it begins to drop frames. The point at which this report is generated (threshold) is a percentage of the number of frames dropped compared with the number of frames forwarded.

When setting this value, remember that 9999 would mean 100 percent of your frames could be dropped before the message is sent. A value of 1000 would mean 10 percent of the frames could be dropped before sending the message. A value of 100 would mean 1 percent of the frames could be dropped before the message is sent.

Examples

In the following example, the loss threshold is set to 0.02 percent:

```
interface tokenring 0
 lnm loss-threshold 2
```

lnm password

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm password** command is not available in Cisco IOS 12.3T software.

To set the password for the reporting link, use the **lnm password** command in interface configuration mode. To return the password to its default value of 00000000, use the **no** form of this command.

lnm password *number string*

no lnm password *number*

Syntax Description

number	Number of the reporting link to which to apply the password. This value must be in the range from 0 to 3.
string	Password you enter at the keyboard. In order to maintain compatibility with LAN Network Manager (LNM), the parameter *string* should be a six- to eight-character string of the type listed in the "Usage Guidelines" section.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

LNM employs the concepts of reporting links and reporting link numbers. A reporting link is simply a connection (or potential connection) between a LAN Reporting Manager (LRM) and a bridge. A reporting link number is a unique number used to identify a reporting link. An IBM bridge allows four simultaneous reporting links numbered 0 to 3. Only the LRM attached to the lowest number connection is allowed to change any parameters, and then only when that connection number falls below a certain configurable number. In the default configuration, the LRM connected through link 0 is the only LRM allowed to change parameters.

Each reporting link has its own password. Passwords are used not only to prevent unauthorized access from an LRM to a bridge, but also to control access to the different reporting links. This is important because of the different abilities associated with the various reporting links.

Characters allowable in the *string* are the following:

- Letters
- Numbers
- Special characters @, #, $, or %

Passwords are displayed only through use of the privileged EXEC **show running-config** command.

Note Two parameters in an IBM bridge have no corresponding parameter in the Cisco IOS software. This means that any attempt to modify these parameters from LNM will fail and display an error message. The LNM names of these two parameters are *route active status* and *single route broadcast mode*.

Examples

In the following example, the password1 is assigned to reporting link 2:

```
! provide appropriate global configuration command if not currently in your config.
!
lnm password 2 password1
```

Related Commands

Command	Description
lnm alternate	Specifies the threshold reporting link number.

lnm pathtrace-disabled

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm pathtrace-dsiabled** command is not available in Cisco IOS 12.3T software.

To disable pathtrace reporting to LAN Network Manager (LNM) stations, use the **lnm pathtrace-disabled** command in global configuration mode. To restore pathtrace reporting functionality, use the **no** form of this command.

lnm pathtrace-disabled [**all** | **origin**]

no lnm pathtrace-disabled

Syntax Description

all	(Optional) Disable pathtrace reporting to the LNM and originating stations.
origin	(Optional) Disable pathtrace reporting to originating stations only.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Under some circumstances, such as when new hardware has been introduced into the network and is causing problems, the automatic report pathtrace function can be disabled. The new hardware may be setting bit-fields B1 or B2 (or both) of the routing control field in the routing information field embedded in a source-route bridged frame. This condition may cause the network to be flooded by report pathtrace frames if the condition is persistent. The **lnm pathtrace-disabled** command, along with its options, allows you to alleviate network congestion that may be occurring by disabling all or part of the automatic report pathtrace function within LNM.

Examples

The following example disables all pathtrace reporting:

```
lnm pathtrace-disabled
```

Related Commands

Command	Description
lnm disabled	Disables LNM functionality.

lnm rem

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm rem** command is not available in Cisco IOS 12.3T software.

To monitor errors reported by any station on the ring, use the **lnm rem** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm rem

no lnm rem

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Ring Error Monitor (REM) service monitors errors reported by any station on the ring. It also monitors whether the ring is in a functional state or in a failure state.

Examples

The following example shows the use of the **lnm rem** command:

```
interface tokenring 0
 lnm rem
```

Related Commands

Command	Description
lnm crs	Monitors the current logical configuration of a Token Ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm rps

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm rps** command is not available in Cisco IOS 12.3T software.

To ensure that all stations on a ring are using a consistent set of reporting parameters, use the **lnm rps** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm rps

no lnm rps

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Ring Parameter Server (RPS) service ensures that all stations on a ring are using a consistent set of reporting parameters and are reporting to LAN Network Manager (LNM) when any new station joins a Token Ring.

Examples

The following example shows the use of the **lnm rps** command:

```
interface tokenring 0
 lnm rps
```

Related Commands

Command	Description
lnm crs	Monitors the current logical configuration of a Token Ring.
lnm rem	Monitors errors reported by any station on the ring.

lnm snmp-only

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm snmp-only** command is not available in Cisco IOS 12.3T software.

To prevent any LAN Network Manager (LNM) stations from modifying parameters in the Cisco IOS software, use the **lnm snmp-only** command in global configuration mode. To allow modifications, use the **no** form of this command.

lnm snmp-only

no lnm snmp-only

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring a router for LNM support is very simple. It happens automatically as a part of configuring the router to act as a source-route bridge. Several commands are available to modify the behavior of the LNM support, but none of them are necessary for it to function.

Because there is now more than one way to remotely change parameters in the Cisco IOS software, this command was developed to prevent them from detrimentally interacting with each other.

This command does not affect the ability of LNM to monitor events, only to modify parameters in the Cisco IOS software.

Examples

The following command prevents any LNM stations from modifying parameters in the software:

```
lnm snmp-only
```

lnm softerr

Note Effective with Cisco IOS Release 12.3(4)T, the **lnm softerr** command is not available in Cisco IOS 12.3T software.

To set the time interval in which the Cisco IOS software will accumulate error messages before sending them, use the **lnm softerr** command in interface configuration mode. To return to the default value, use the **no** form of this command.

lnm softerr *ten-milliseconds*

no lnm softerr

Syntax Description

ten-milliseconds	Time interval in tens of milliseconds between error messages. The valid range is from 0 to 65535.

Defaults

200 ms (2 seconds)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All stations on a Token Ring notify the ring error monitor (REM) when they detect errors on the ring. To prevent an excessive number of messages, error reports are not sent immediately, but are accumulated for a short period of time and then reported. A station learns this value from a router (configured as a source-route bridge) when it first enters the ring.

Examples

The following example changes the error-reporting frequency to once every 5 seconds:

```
lnm softerr 500
```

Related Commands

Command	Description
lnm rem	Monitors errors reported by any station on the ring.

mac-address

To modify the default MAC address of an interface to some user-defined address, use the **mac-address** command in interface configuration mode. To return to the default MAC address on the interface, use the **no** form of this command.

mac-address *ieee-address*

no mac-address *ieee-address*

Syntax Description

ieee-address	48-bit IEEE MAC address written as a dotted triple of four-digit hexadecimal numbers.

Defaults

The interface uses a default MAC address that is derived from the base address stored in the electrically erasable programmable read-only memory (EEPROM).

Command Modes

Interface configuration

Usage Guidelines

Be sure that no other interface on the network is using the MAC address that you assign.

There is a known defect in earlier forms of this command when the Texas Instruments Token Ring MAC firmware is used. This implementation is used by Proteon, Apollo, and IBM RTs. A host using a MAC address whose first two bytes are zeros (such as a Cisco router) will not properly communicate with hosts using that form of this command of TI firmware.

There are two solutions. The first involves installing a static Routing Information Field (RIF) entry for every faulty node with which the router communicates. If there are many such nodes on the ring, this may not be practical. The second solution involves setting the MAC address of the Cisco Token Ring to a value that works around the problem.

This command forces the use of a different MAC address on the specified interface, thereby avoiding the Texas Instrument MAC firmware problem. It is up to the network administrator to ensure that no other host on the network is using that MAC address.

Examples

The following example sets the MAC layer address, where *xx.xxxx* is an appropriate second half of the MAC address to use:

```
interface tokenring 0
 mac-address 5000.5axx.xxxx
```

The following example changes the default MAC address on the interface to 1111.2222.3333:

```
Router# configure terminal
Router(config)# interface fastethernet 2/1/1
Router(config-if)# mac-address 1111.2222.3333
```

Related Commands

Command	Description
show interfaces fastethernet	Displays information about the Fast Ethernet interfaces.
show interfaces gigabitethernet	Displays information about the Gigabit Ethernet interfaces.

multiring

To enable collection and use of Routing Information Field (RIF) information, use the **multiring** command in interface configuration mode. To disable the use of RIF information for the protocol specified, use the **no** form of this command.

multiring {*protocol* [**all-routes** | **spanning**] | **all** | **other**}

no multiring {*protocol* [**all-routes** | **spanning**] | **all** | **other**}

Syntax Description

protocol	Specifies a protocol. The following protocols are supported: • **appletalk**—AppleTalk Phase 1 and 2 • **clns**—ISO CLNS • **decnet**—DECnet Phase IV • **ip**—IP • **ipx**—Novell IPX
all-routes	(Optional) Uses all-routes explorers.
spanning	(Optional) Uses spanning-tree explorers.
all	Enables the multiring for *all* frames.
other	Enables the multiring for *any* routed frame not included in the previous list of supported protocols.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Level 3 routers that use protocol-specific information (for example, Novell IPX or XNS headers) rather than MAC information to route datagrams also must be able to collect and use RIF information to ensure that they can send datagrams across a source-route bridge. The software default is to not collect and use RIF information for routed protocols. This allows operation with software that does not understand or properly use RIF information.

Note When you are configuring DLSw+ over FDDI, the **multiring** command supports only IP and IPX.

The **multiring** command allows for per-protocol specification of the interface's ability to append RIFs to routed protocols. When it is enabled for a protocol, the router will source packets that include information used by source-route bridges. This allows a router with Token Ring interfaces, for the protocol or protocols specified, to connect to a source-bridged Token Ring network. If a protocol is not specified for multiring, the router can route packets only to nodes directly connected to its local Token Ring.

Examples

The following example enables IP and Novell IPX bridging on a Token Ring interface. RIFs will be generated for IP frames, but not for the Novell IPX frames.

```
! commands that follow apply to interface token 0
interface tokenring 0
! enable the Token Ring interface for IP
 ip address 172.16.0.0 255.255.255.0
! generate RIFs for IP frames
 multiring ip
! enable the Token Ring interface for Novell IPX
 novell network 33
```

Related Commands

Command	Description
clear rif-cache	Clears the entire RIF cache.
rif	Enters static source-route information into the RIF cache.
rif timeout	Determines the number of minutes an inactive RIF entry is kept.
show rif	Displays the current contents of the RIF cache.
xns encapsulation	Selects the type of encapsulation used on a Token Ring interface.

multiring trcrf-vlan

To create a pseudoring on the Route Switch Module (RSM) and to terminate the Routing Information Field (RIF) when routing IP or IPX source-routed traffic on Token Ring VLAN (TrBRF) interfaces, use the **multiring trcrf-vlan** command in interface configuration mode. To disable the termination of RIFs on the RSM interface, use the **no** form of this command.

multiring trcrf-vlan *vlanid* **ring-group** *ring-number*

no multiring trcrf-vlan *vlanid* **ring-group** *ring-number*

Syntax Description

vlanid	VLAN ID number. Valid VLAN ID numbers are 2 through 1000.
ring-group *ring-number*	Specifies the pseudoring number used to terminate the RIF.

Defaults

Termination of RIFs is disabled on the RSM interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **multiring** command to collect and use RIFs for routed protocols. On an RSM, the multiring command appends RIFs for routed protocols on Token Ring VLAN interfaces. When this command is enabled for a protocol, the RSM will source packets that include information used by source-route bridges. The Token Ring VLAN interfaces on the RSM can connect to an Source-route bridging (SRB) Token Ring network for the protocols specified in the command.

Each Token Ring VLAN interface that is configured with the **multiring** command on the RSM must also be accompanied by the **multiring trcrf-vlan** command.

Use the **multiring trcrf-vlan** command to:

- Create a pseudoring on which RIFs are terminated for routed protocols.
- Assign the pseudoring to a Token Ring Concentrator Relay Function (TrCRF) VLAN.

When configuring SRB and IP or IPX routing source routing (SR) frames on an RSM's TrBRF interface, define both a virtual ring and a pseudoring for the interface using the **source-bridge** and **multiring trcrf-vlan** commands. In this case, the VLAN ID used for the TrCRF that corresponds to the virtual ring can be the same as the one used for the pseudoring number. If the VLAN IDs are different, the virtual ring and pseudoring numbers must be different.

Examples

In the following example, the **multiring trcrf-vlan** command is used to configure a pseudoring with ring number 100 on the RSM:

```
interface Ethernet 2/2
 ip address 10.4.4.1 255.255.255.0
!
interface vlan998 type trbrf
 ip address 10.5.5.1 255.255.255.0
 multiring trcrf-vlan 200 ring-group 100
 multiring all
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
interface vlan	Configures a Token Ring or Ethernet interface on the RSM.
multiring	Enables collection and use of RIF information.
rif	Enters static source-route information into the RIF cache.
show drip	Displays the status of the DRiP database.
show rif	Displays the current contents of the RIF cache.
source-bridge	Configures an interface for source-route bridging.

netbios access-list bytes

To define the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets, use the **netbios access-list bytes** command in global configuration mode. To remove an entire list or the entry specified with the *pattern* argument, use the **no** form of this command.

netbios access-list bytes *name* {**permit** | **deny**} *offset pattern*

no netbios access-list bytes *name* [**permit** | **deny**]

Syntax Description

name	Name of the access list being defined.
permit	Permits the condition.
deny	Denies the condition.
offset	Decimal number indicating the number of bytes into the packet where the byte comparison should begin. An offset of zero points to the very beginning of the NetBIOS header. Therefore, the NetBIOS delimiter string (0xFFEF), for example, begins at offset 2.
pattern	Hexadecimal string of digits representing a byte pattern. The *pattern* argument must conform to certain conventions described in the “Usage Guidelines” section.

Defaults

No offset or pattern is defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For offset pattern matching, the byte pattern must be an even number of hexadecimal digits in length.

The byte pattern must be no more than 16 bytes (32 hexadecimal digits) in length.

As with all access lists, the NetBIOS access lists are scanned in order.

You can specify a wildcard character in the byte string indicating that the value of that byte does not matter in the comparison. This is done by specifying two asterisks (**) in place of digits for that byte. For example, the following command would match 0xabaacd, 0xab00cd, and so on:

```
netbios access-list bytes marketing permit 3 0xab**cd
```

Examples

The following example shows how to configure for offset pattern matching:

```
netbios access-list bytes marketing permit 3 0xabcd
```

In the following example, the byte pattern would not be accepted because it must be an even number of hexadecimal digits:

```
netbios access-list bytes marketing permit 3 0xabc
```

In the following example, the byte pattern would not be permitted because the byte pattern is longer than 16 bytes in length:

```
netbios access-list bytes marketing permit 3 00112233445566778899aabbccddeeff00
```

The following example would match 0xabaacd, 0xab00cd, and so on:

```
netbios access-list bytes marketing permit 3 0xab**cd
```

The following example deletes the entire marketing NetBIOS access list named marketing:

```
no netbios access-list bytes marketing
```

The following example removes a single entry from the list:

```
no netbios access-list bytes marketing deny 3 0xab**cd
```

In the following example, the first line serves to deny all packets with a byte pattern starting in offset 3 of 0xab. However, this denial would also include the pattern 0xabcd because the entry permitting the pattern 0xabcd comes after the first entry:

```
netbios access-list bytes marketing deny 3 0xab
netbios access-list bytes marketing permit 3 0xabcd
```

Related Commands

Command	Description
netbios input-access-filter bytes	Defines a byte access list filter on incoming messages. T
netbios output-access-filter bytes	Defines a byte access list filter on outgoing messages.

netbios access-list host

To assign the name of the access list to a station or set of stations on the network, use the **netbios access-list host** command in global configuration mode. To remove either an entire list or just a single entry from a list, depending upon the value given for *pattern* argument, use the **no** form of this command.

netbios access-list host *name* {**permit** | **deny**} *pattern*

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

Syntax Description

name	Name of the access list being defined.
permit	Permits the condition.
deny	Denies the condition.
pattern	A set of characters. The characters can be the name of the station, or a combination of characters and pattern-matching symbols that establish a pattern for a set of NetBIOS station names. This combination can be especially useful when stations have names with the same characters, such as a prefix. Table 6 in the "Usage Guidelines" section explains the pattern-matching symbols that can be used.

Defaults

No access list is assigned.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The NetBIOS station access list contains the station name to match, along with a permit or deny condition.

Table 6 explains the pattern-matching characters that can be used.

Table 6 Station Name Pattern-Matching Characters

Character	Description
*	Used at the end of a string to match any character or string of characters.
?	Matches any single character. If this wildcard is used as the first letter of the name, you must precede it with a Cntl-V key sequence. Otherwise it will be interpreted by the router as a request for help.

Examples

The following example specifies a full station name to match:

```
netbios access-list host marketing permit ABCD
```

The following example specifies a prefix where the pattern matches any name beginning with the characters DEFG:

```
!The string DEFG itself is included in this condition.
netbios access-list host marketing deny DEFG*
```

The following example permits any station name with the letter W as the first character and the letter Y as the third character in the name. The second and fourth character in the name can be any character. This example would allow stations named WXYZ and WAYB; however, stations named WY and WXY would not be allowed because the question mark (?) must match specific characters in the name:

```
netbios access-list host marketing permit W?Y?
```

The following example illustrates how to combine wildcard characters. In this example the marketing list denies any name beginning with AC that is not at least three characters in length (the question mark [?] would match any third character). The string ACBD and ACB would match, but the string AC would not:

```
netbios access-list host marketing deny AC?
```

In the following example, a single entry in the marketing NetBIOS access list is removed:

```
no netbios access-list host marketing deny AC?*
```

In the following example, the entire marketing NetBIOS access list is removed:

```
no netbios access-list host marketing
```

Related Commands

Command	Description
netbios input-access-filter host	Defines a station access list filter on incoming messages.
netbios output-access-filter host	Defines a station access list filter on outgoing messages.

netbios enable-name-cache

To enable NetBIOS name caching, use the **netbios enable-name-cache** command in interface configuration mode. To disable the name-cache behavior, use the **no** form of this command.

netbios enable-name-cache

no netbios enable-name-cache

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command enables the NetBIOS name cache on the specified interface. By default the name cache is disabled for the interface. Proxy explorers must be enabled on any interface that is using the NetBIOS name cache.

Examples

The following example enables NetBIOS name caching for Token Ring interface 0:

```
interface tokenring 0
 source-bridge proxy-explorer
 netbios enable-name-cache
```

Related Commands

Command	Description
clear netbios-cache	Clears the entries of all dynamically learned NetBIOS names.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.
show netbios-cache	Displays a list of NetBIOS cache entries.

netbios input-access-filter bytes

To define a byte access list filter on incoming messages, use the **netbios input-access-filter bytes** command in interface configuration mode. To remove the entire access list, use the **no** form of this command with the appropriate name.

netbios input-access-filter bytes *name*

no netbios input-access-filter bytes *name*

Syntax Description

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list bytes** global configuration commands.

Defaults

No access list is defined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The actual access filter byte offsets and patterns used are defined in one or more **netbios-access-list bytes** commands.

Examples

The following example applies a previously defined filter named *marketing* to packets coming into Token Ring interface 1:

```
interface tokenring 1
 netbios input-access-filter bytes marketing
```

Related Commands

Command	Description
netbios access-list bytes	Defines the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets.

netbios input-access-filter host

To define a station access list filter on incoming messages, use the **netbios input-access-filter host** command in interface configuration mode. To remove the entire access list, use the **no** form of this command with the appropriate argument.

netbios input-access-filter host *name*

no netbios input-access-filter host *name*

Syntax Description

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list host** global configuration commands.

Defaults

No access list is defined.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The access lists of station names are defined in **netbios access-list host** commands.

Examples

The following example filters packets coming into Token Ring interface 1 using the NetBIOS access list named *marketing*:

```
interface tokenring 1
 netbios access-list host marketing permit W?Y?
 netbios input-access-filter host marketing
```

Related Commands

Command	Description
netbios access-list host	Assigns the name of the access list to a station or set of stations on the network.
netbios output-access-filter host	Defines a station access list filter on outgoing messages.

netbios name-cache

To define a static NetBIOS name cache entry, tying the server with the name *netbios-name* to the *mac-address*, and specifying that the server is accessible either locally through the *interface-name* specified, or remotely, through the **ring-group** *group-number* specified, use the **netbios name-cache** command in global configuration mode. To remove the entry, use the **no** form of this command.

netbios name-cache *mac-address netbios-name* {*interface-name interface-number* | **ring-group** *group-number*}

no netbios name-cache *mac-address netbios-name*

Syntax Description

mac-address	The MAC address.
netbios-name	Server name linked to the MAC address.
interface-name	Name of the interface by which the server is accessible locally.
interface-umber	Number of the interface by which the server is accessible locally.
ring-group	Specifies that the link is accessible remotely.
group-number	Number of the ring group by which the server is accessible remotely. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.

Defaults

No entry is defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

To specify an entry in the static name cache, first specify a Routing Information Field (RIF) that leads to the server's MAC address. The Cisco IOS software displays an error message if it cannot find a static RIF entry for the server when the NetBIOS name-cache entry is attempted or if the server's type conflicts with that given for the static RIF entry.

Note The names are case sensitive; therefore "Cc" is not the same as "cC."

Examples

The following example indicates the syntax usage of this command if the NetBIOS server is accessed locally:

```
source-bridge ring-group 2
 rif 0220.3333.4444 00c8.042.0060 tokenring 0
 netbios name-cache 0220.3333.4444 DEF tokenring 0
```

The following example indicates the syntax usage of this command if the NetBIOS server is accessed remotely:

```
source-bridge ring-group 2
 rif 0110.2222.3333 0630.021.0030 ring group 2
 netbios name-cache 0110.2222.3333 DEF ring-group 2
```

Related Commands

Command	Description
show netbios-cache	Displays a list of NetBIOS cache entries.

netbios name-cache name-len

To specify how many characters of the NetBIOS type name the name cache will validate, use the **netbios name-cache name-len** command in global configuration mode.

netbios name-cache name-len *length*

no netbios name-cache name-len *length*

Syntax Description

length	Length of the NetBIOS type name. The range is from 8 to 16 characters.

Defaults

15 characters

Command Modes

Global configuration

Command History

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

Examples

The following example specifies that the name cache will validate 16 characters of the NetBIOS type name:

```
netbios name-cache name-len 16
```

Related Commands

Command	Description
netbios enable-name-cache	Enables NetBIOS name caching.
netbios name-cache	Defines a static NetBIOS name cache entry.
netbios name-cache proxy-datagram	Enables the Cisco IOS software to act as a proxy and send NetBIOS datagram type frames.
netbios name-cache query-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame.
netbios name-cache recognized-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.

netbios name-cache proxy-datagram

To enable the Cisco IOS software to act as a proxy and send NetBIOS datagram type frames, use the **netbios name-cache proxy-datagram** command in global configuration mode. To return to the default value, use the **no** form of this command.

netbios name-cache proxy-datagram *seconds*

no netbios name-cache proxy-datagram *seconds*

Syntax Description

seconds	Time interval, in seconds, that the software forwards a route broadcast datagram type packet. The valid range is any number greater than 0.

Defaults

There is no default time interval.

Command Modes

Global configuration

Command History

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

Examples

The following example specifies that the software will forward a NetBIOS datagram type frame in 20-second intervals:

```
netbios name-cache proxy-datagram 20
```

Related Commands

Command	Description
netbios enable-name-cache	Enables NetBIOS name caching.
netbios name-cache	Defines a static NetBIOS name cache entry, tying the server with the name netbios-name to the mac-address, and specifying that the server is accessible either locally through the interface-name specified, or remotely through the ring-group group-number specified.
netbios name-cache query-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame.

Command	Description
netbios name-cache recognized-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.

netbios name-cache query-timeout

To specify the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame, use the **netbios name-cache query-timeout** command in global configuration mode. To restore the default of 6 seconds, use the **no** form of this command.

netbios name-cache query-timeout *seconds*

no netbios name-cache query-timeout

Syntax Description

seconds	Dead time period in seconds. Default is 6 seconds.

Defaults

6 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

During the dead time, the Cisco IOS software drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process.

Examples

The following example sets the timeout to 15 seconds:

```
netbios name-cache query-timeout 15
```

Related Commands

Command	Description
netbios name-cache recognized-timeout	Specifies the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame.

netbios name-cache recognized-timeout

To specify the "dead" time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame, use the **netbios name-cache recognized-timeout** command in global configuration mode. To restore the default of 6 seconds, use the **no** form of this command.

netbios name-cache recognized-timeout *seconds*

no netbios name-cache recognized-timeout

Syntax Description

seconds	Dead time period in seconds. Default is 6 seconds.

Defaults

6 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

During the dead time, the Cisco IOS software drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is effective only at the time of the login negotiation process.

Examples

The following example sets the timeout to 15 seconds:

```
netbios name-cache recognized-timeout 15
```

Related Commands

Command	Description
netbios name-cache query-timeout	Specifies the "dead" time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame.

netbios name-cache timeout

To enable NetBIOS name caching and to set the time that entries can remain in the NetBIOS name cache, use the **netbios name-cache timeout** command in global configuration mode. To restore the default of 15 minutes, use the **no** form of this command.

netbios name-cache timeout *minutes*

no netbios name-cache timeout *minutes*

Syntax Description

minutes	Time, in minutes, that entries can remain in the NetBIOS name cache. Default is 15 minutes.

Defaults

15 minutes

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command allows you to establish NetBIOS name caching. NetBIOS name-caching does not apply to static entries. Once the time expires, the entry will be deleted from the cache.

Examples

The following example sets the timeout to 10 minutes:

```
interface tokenring 0
 netbios name-cache timeout 10
```

Related Commands

Command	Description
show netbios-cache	Displays a list of NetBIOS cache entries.

netbios output-access-filter bytes

To define a byte access list filter on outgoing messages, use the **netbios output-access-filter bytes** command in interface configuration mode. To remove the entire access list, use the **no** form of this command.

netbios output-access-filter bytes *name*

no netbios output-access-filter bytes *name*

Syntax Description

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list bytes** global configuration commands.

Defaults

No access list is defined.

Command Modes

Interface configuration

Command History

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

Examples

The following example filters packets leaving Token Ring interface 1 using the NetBIOS access list named engineering:

```
interface tokenring 1
 netbios access-list bytes engineering permit 3 0xabcd
 netbios output-access-filter bytes engineering
```

Related Commands

Command	Description
netbios access-list bytes	Defines the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets.
netbios input-access-filter bytes	Defines a byte access list filter on incoming messages.

netbios output-access-filter host

To define a station access list filter on outgoing messages, use the **netbios output-access-filter host** command in interface configuration mode. To remove the entire access list, use the **no** form of this command.

netbios output-access-filter host *name*

no netbios output-access-filter host *name*

Syntax Description

name	Name of a NetBIOS access filter previously defined with one or more of the **netbios access-list host** global configuration commands.

Defaults

No access list filter is defined.

Command Modes

Interface configuration

Command History

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

Examples

The following example filters packets leaving Token Ring interface 1 using the NetBIOS access list named *engineering*:

```
interface tokenring 1
 netbios access-list host engineering permit W?Y?
 netbios output-access-filter host engineering
```

Related Commands

Command	Description
netbios access-list host	Assigns the name of the access list to a station or set of stations on the network.
netbios input-access-filter host	Defines a station access list filter on incoming messages.

rif

To enter static source-route information into the Routing Information Field (RIF) cache, use the **rif** command in global configuration mode. To remove an entry from the cache, use the **no** form of this command.

rif *mac-address rif-string* {*interface-name* | **ring-group** *ring*}

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

Syntax Description

mac-address	12-digit hexadecimal string written as a dotted triple of four-digit hexadecimal numbers; for example, 0010.0a00.20a6.
rif-string	Series of 4-digit hexadecimal numbers separated by a period (.). This RIF string is inserted into the packets sent to the specified MAC address.
interface-name	Interface name (for example, tokenring 0) that indicates the origin of the RIF.
ring-group	Specifies the origin of the RIF is a ring group.
ring	Ring group number that indicates the origin of the RIF. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095.

Usage Guidelines

If a Token Ring host does not support the use of IEEE 802.2 TEST or XID datagrams as explorer packets, you may need to add static information to the RIF cache of the router.

Command Default

No static source-route information is entered.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You must specify either an interface name or a ring group number to indicate the origin of the RIF. You specify an interface name (for example, tokenring 0) with the *interface-name* argument, and you specify a ring group number with the **ring-group** *ring* keyword and argument. The ring group number must match the number you specified with the **source-bridge ring-group** command. Ring groups are explained in the "Configuring Source-Route Bridging" chapter of the *Bridging and IBM Networking Configuration Guide*.

Using the command **rif** *mac-address* without any other arguments puts an entry into the RIF cache indicating that packets for this MAC address should not have RIF information.

Do not configure a static RIF with any of the *all rings* type codes. Doing so causes traffic for the configured host to appear on more than one ring and leads to unnecessary congestion.

Note Input to the **source-bridge** interface configuration command is in decimal format. RIF displays and input are in hexadecimal format, and IBM source-route bridges use hexadecimal for input. It is essential that bridge and ring numbers are consistent for proper network operation. This means you must explicitly declare the numbers to be hexadecimal by preceding the number with 0x, or you must convert IBM hexadecimal numbers to a decimal equivalent when entering them. For example, IBM hexadecimal bridge number 10 would be entered as hexadecimal number 0x10 or decimal number 16 in the configuration commands. In the displays, these commands always will be in decimal.

Examples

The following example configuration sets up a static RIF:

```
! insert entry with MAC address 1000.5A12.3456 and RIF of
! 0630.0081.0090 into RIF cache
rif 1000.5A12.3456 0630.0081.0090 tokenring 0
```

Related Commands

Command	Description
multiring	Enables collection and use of RIF information.
source-bridge ring-group	Defines or removes a ring group from the configuration.

rif timeout

To determine the number of minutes an inactive Routing Information Field (RIF) entry is kept, use the **rif timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

rif timeout *minutes*

no rif timeout

Syntax Description

minutes	Number of minutes an inactive RIF entry is kept. The value must be greater than 0. Default is 15 minutes.

Defaults

15 minutes

Command Modes

Global configuration

Command History

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

Usage Guidelines

A RIF entry is cached based on the MAC address and the interface.

RIF information is maintained in a cache whose entries are aged. A RIF entry can be aged out even if there is active traffic, but the traffic is fast or autonomously switched. Until a RIF entry is removed from the cache, no new information is accepted for that RIF entry.

A RIF entry is refreshed only if a RIF field of an incoming frame is identical to the RIF information of the RIF entry in the cache.

Examples

The following example changes the timeout period to 5 minutes:

```
rif timeout 5
```

Related Commands

Command	Description
clear rif-cache	Clears the entire RIF cache.
rif validate-enable	Enables RIF validation for entries learned on an interface (Token Ring or FDDI).
show rif	Displays the current contents of the RIF cache.

rif validate-age

To define the validation time when the Cisco IOS software is acting as a proxy for NetBIOS NAME_QUERY packet or for explorer frames, use the **rif validate-age** command in global configuration mode.

rif validate-age *seconds*

no rif validate-age *seconds*

Syntax Description

seconds	Interval, in seconds, at which a proxy is sent. The valid range is any number greater than 0. Default is 2 seconds.

Defaults

2 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

If the timer expires before the response is received, the Routing Information Field (RIF) entry or the NetBIOS cache entry is marked as invalid and is flushed from the cache table when another explorer or NAME_QUERY packet is received.

Examples

The following example specifies the interval at which a proxy is sent to be 3 seconds:

```
rif validate-age 3
```

Related Commands

Command	Description
rif	Enters static source-route information into the RIF cache.
rif timeout	Determines the number of minutes an inactive RIF entry is kept.

rif validate-enable

To enable Routing Information Field (RIF) validation for entries learned on an interface (Token Ring or Fiber Distributed Data Interface [FDDI]), use the **rif validate-enable** command in global configuration mode. To disable the specification, use the **no** form of this command.

rif validate-enable

no rif validate-enable

Syntax Description

This command has no arguments or keywords.

Defaults

RIF validation is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

A RIF validation algorithm is used for the following cases:

- To decrease convergence time to a new source-route path when an intermediate bridge goes down.
- To keep a valid RIF entry in a RIF cache even if a RIF entry is not refreshed either because traffic is fast or autonomously switched, or because there is no traffic.

A directed IEEE TEST command is sent to the destination MAC address. If a response received in the time specified by the **rif validate-age** command, the entry is refreshed and is considered valid. Otherwise, the entry is removed from the cache. To prevent sending too many TEST commands, any entry that has been refreshed in fewer than 70 seconds is considered valid.

Validation is triggered as follows:

- When a RIF entry is found in the cache.
- When a RIF field of an incoming frame and the RIF information of the RIF entry is not identical. If, as the result of validation, the entry is removed from the cache, the RIF field of the next incoming frame with the same MAC address is cached.
- When the RIF entry is not refreshed for the time specified in the **rif timeout** command.

Note If the RIF entry has been in the RIF cache for 6 hours, and has not been refreshed for the time specified in the **rif timeout** command, the entry is removed unconditionally from the cache.

Note The **rif validate-enable** commands have no effect on remote entries learned over RSRB.

Examples

The following example enables RIF validation:

```
rif validate-enable
```

Related Commands

Command	Description
rif timeout	Determines the number of minutes an inactive RIF entry is kept.
rif validate-age	Defines the validation time when the Cisco IOS software is acting as a proxy for NetBIOS NAME_QUERY packet or for explorer frames.
rif validate-enable-age	Enables RIF validation for stations on a source-route bridge network that do not respond to an IEEE TEST command.
rif validate-enable-route-cache	Enables synchronization of the RIF cache with the protocol route cache.

rif validate-enable-age

To enable Routing Information Field (RIF) validation for stations on a source-route bridge network that do not respond to an IEEE TEST command, use the **rif validate-enable-age** command in global configuration mode. To disable the specification, use the **no** form of this command.

rif validate-enable-age

no rif validate-enable-age

Syntax Description

This command has no arguments or keywords.

Defaults

RIF validation is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You must first issue the **rif validate-enable** command.

When this command is enabled, a RIF entry is not removed from the cache even if it becomes invalid. If the entry is refreshed, it becomes valid again.

If a RIF field of an incoming frame and the RIF information of the invalid RIF entry are not identical, the old RIF information is replaced by the new information.

Note The **rif validate-enable** commands have no effect on remote entries learned over remote source-route bridging (RSRB).

Examples

The following example enables RIF validation:

```
rif validate-enable-age
```

Related Commands

Command	Description
rif validate-enable	Enables RIF validation for entries learned on an interface (Token Ring or FDDI).

rif validate-enable-route-cache

To enable synchronization of the Routing Information Field (RIF) cache with the protocol route cache, use the **rif validate-enable-route-cache** command in global configuration mode. To disable the specification, use the **no** form of this command.

rif validate-enable-route-cache

no rif validate-enable-route-cache

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

When a RIF entry is removed from the RIF cache, or the RIF information in the RIF entry is changed, the protocol route caches are synchronized with the RIF cache.

Note The **rif validate-enable** commands have no effect on remote entries learned over remote source-route bridging (RSRB).

Examples

The following example synchronizes the RIF cache with the protocol route cache:

```
rif validate-enable-route-cache
```

Related Commands

Command	Description
rif validate-enable	Enables RIF validation for entries learned on an interface (Token Ring or FDDI).

show access-expression

To display the defined input and output access list expressions, use the **show access-expression** command in privileged EXEC mode.

show access-expression [**begin** | **include** | **exclude**]

Syntax Description

begin	(Optional) Begin with the access list expression that matches.
include	(Optional) Include access list expressions that match.
exclude	(Optional) Exclude access list expressions that match.

Defaults

Displays all input and output access list expressions.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show access-expression** command:

```
Router# show access-expression
Router# interface TokenRing0/0:
        Input:(dmac(701) | ~lsap(202))
```

See the **access-expression** command for a description of the access expressions.

Related Commands

Command	Description
access-expression	Defines an access expression.

show bridge

To display classes of entries in the bridge forwarding database, use the **show bridge** command in privileged EXEC mode.

show bridge [*bridge-group*] [*interface*] [*address* [*mask*]] [**verbose**]

Syntax Description

bridge-group	(Optional) Number that specifies a particular spanning tree.
interface	(Optional) Specific interface, such as Ethernet 0.
address	(Optional) 48-bit canonical (Ethernet ordered) MAC address. This may be entered with an optional mask of bits to be ignored in the address, which is specified with the *mask* argument.
mask	(Optional) Bits to be ignored in the address. You must specify the *address* argument if you want to specify a mask.
verbose	(Optional) Displays additional detail, including any Frame Relay data-link connection identifier (DLCI) associated with a station address.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **verbose** keyword first appeared in Cisco IOS Release 11.0.

The following are possible variations of the **show bridge** command:

```
show bridge ethernet 0
show bridge 0000.0c00.0000 0000.00FF.FFFF
show bridge 0000.0c00.0e1a
show bridge
show bridge verbose
```

In the sample output, the first command would display all entries for hosts reachable via Ethernet interface 0, the second command would display all entries with the vendor code of 0000.0c00.0000, and the third command would display the entry for address 0000.0c00.0e1a. In the fourth command, all entries in the forwarding database would be displayed. The fifth command provides additional detail. In all five lines, the bridge group number has been omitted.

Examples

The following is sample output from the **show bridge** command. The second display is output from the **show bridge** command with the **verbose** argument.

```
Router# show bridge

Total of 300 station blocks, 280 free
Codes: P - permanent, S - self

Bridge Group 32:Bridge Group 32:

    Address       Action   Interface       Age   RX count   TX count
0180.c200.0000   receive       -            S          0          0
ffff.ffff.ffff   receive       -            S          0          0
0900.2b01.0001   receive       -            S          0          0
0300.0c00.0001   receive       -            S          0          0
0000.0c05.1000   forward   Ethernet0/1      4          1          0
0000.0c04.4b5b   receive       -            S          0          0
0000.0c04.4b5e   receive       -            S          0          0
0000.0c04.4b5d   receive       -            S          0          0
0000.0c04.4b5c   receive       -            S          0          0
0000.0c05.4a62   forward   Ethernet0/1      4          1          0
aa00.0400.2108   forward   Ethernet0/1      0         42          0
0000.0c12.b888   forward   Ethernet0/2      4          1          0
0000.0c12.b886   forward   Ethernet0/1      4          1          0
aa00.0400.4d09   forward   Ethernet0/1      4          1          0
0000.0c06.fb9a   forward   Ethernet0/1      4          1          0
0000.0c04.b039   forward   Ethernet0/1      4          1          0

Router# show bridge verbose

Total of 300 station blocks, 287 free
Codes: P - permanent, S - self

BG Hash      Address      Action Interface     DLCI   Age RX count   TX count
32 00/0   0180.c200.0000 receive      -           -     S           0          0
32 00/1   ffff.ffff.ffff receive      -           -     S           0          0
32 01/0   0900.2b01.0001 receive      -           -     S           0          0
32 01/1   0300.0c00.0001 receive      -           -     S           0          0
32 10/0   0000.0c04.4b5b receive      -           -     S           0          0
32 15/0   0000.0c04.4b5e receive      -           -     S           0          0
32 16/0   0000.0c04.4b5d receive      -           -     S           0          0
32 17/0   0000.0c04.4b5c receive      -           -     S           0          0
32 29/0   aa00.0400.2108 forward  Ethernet0/1     -     0          48          0
32 30/0   0000.0c12.b888 forward  Ethernet0/2     -     0           1          0
32 A4/0   0800.2002.ff5b forward  Ethernet0/1     -     0           6          0
32 E2/0   aa00.0400.e90b forward  Ethernet0/1     -     0          65          0
32 F2/0   0000.0c04.b042 forward  Ethernet0/2     -     3           2          0
```

Table 7 describes the significant fields shown in the display.

Table 7 show bridge Field Descriptions

Field	Description
Total of 300 station blocks	Total number of forwarding database elements in the system. The memory to hold bridge entries is allocated in blocks of memory sufficient to hold 300 individual entries. When the number of free entries falls below 25, another block of memory sufficient to hold another 300 entries is allocated. Therefore, the size of the bridge forwarding database is limited to the amount of free memory in the router.
295 free	Number in the free list of forwarding database elements in the system. The total number of forwarding elements is expanded dynamically, as needed.
BG	Bridging group to which the address belongs.
Hash	Hash key/relative position in the keyed list.
Address	Canonical (Ethernet ordered) MAC address.
Action	Action to be taken when that address is looked up; choices are to discard or forward the datagram.
Interface	Interface, if any, on which that address was seen.
Age	Number of minutes since a frame was received from or sent to that address. The letter “P” indicates a permanent entry. The letter “S” indicates the system as recorded by the router. On the modular systems, this is typically the broadcast address and the router’s own hardware address; on the IGS, this field will also include certain multicast addresses.
RX count	Number of frames received from that address.
TX count	Number of frames forwarded to that address.

show bridge circuit-group

To display the interfaces configured in each circuit group and show whether they are currently participating in load distribution, use the **show bridge circuit-group** command in user EXEC or privileged EXEC mode.

show bridge [*bridge-group*] **circuit-group** [*circuit-group*] [*src-mac-address*] [*dst-mac-address*]

Syntax Description

bridge-group	(Optional) Number that specifies a particular bridge group.
circuit-group	(Optional) Number that specifies a particular circuit group.
src-mac-address	(Optional) 48-bit canonical (Ethernet ordered) source MAC address.
dst-mac-address	(Optional) 48-bit canonical (Ethernet ordered) destination MAC address.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

The following is sample output from various **show bridge circuit-group** command strings:

```
Router# show bridge circuit-group

Bridge group 1 Circuit group 1:
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding
Bridge group 1 Circuit group 2:
    Interface Serial2 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 1

Bridge group 1 Circuit group 1:
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 2

Bridge group 1 Circuit group 2:
    Interface Serial2 : inserted, learning, forwarding

Router# show bridge 1 circuit-group 1 0000.6502.23EA 0000.1234.4567

Output circuit group interface is Serial3
```

```
Router# show bridge 1 circuit-group 1 0000.6502.23EA

%Destination MAC address required

Router# show bridge 1 circuit-group 1

Bridge group 1 Circuit group 1:
    Transmission pause interval is 250ms
    Output interface selection is source-based
    Interface Serial0 : inserted, learning, forwarding
    Interface Serial3 : inserted, learning, forwarding
    Interface Serial2 is unavailable

Router# show bridge 1 circuit-group 1 0000.6502.23EA 0000.1234.4567

%Please enter source MAC address only
```

Table 8 describes the significant fields shown in the display.

Table 8 show bridge circuit-group Field Descriptions

Field	Description
inserted	Indicates whether this interface is included or not included in circuit-group operation. If the interface is administratively down, or if line protocol is not up, the interface is not included in the circuit-group operation.
learning	Indicates whether this interface is in Spanning Tree Protocol (IEEE or Digital) learning or not learning state.
forwarding	Indicates whether this port is in Spanning Tree Protocol (IEEE or Digital) forwarding or not forwarding state.

show bridge group

To display the status of each bridge group, use the **show bridge group** command in privileged EXEC mode.

show bridge group [**verbose**]

Syntax Description

verbose	(Optional) Displays detailed information.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show bridge group** command:

```
Router# show bridge group

Bridge Group 1 is running the DEC compatible Spanning Tree Protocol

   Port 7 (ATM0.1 LANE Ethernet) of bridge group 1 is down
   Port 4 (TokenRing0) of bridge group 1 is forwarding
```

“Forwarding” and “down” indicate the port state as determined by the spanning-tree algorithm or via configuration.

The following examples are for bridge group 30 and bridge group 40 of a PA-12E/2FE port adapter in slot 3:

```
Router# show bridge group

Bridge Group 30 is running the IEEE compatible Spanning Tree Protocol
   Port 19 (Fast Ethernet3/0) of bridge group 30 is forwarding
   Port 20 (Fast Ethernet3/1) of bridge group 30 is forwarding
   Port 21 (Ethernet3/2) of bridge group 30 is forwarding
   Port 22 (Ethernet3/3) of bridge group 30 is forwarding
   Port 23 (Ethernet3/4) of bridge group 30 is forwarding
   Port 24 (Ethernet3/5) of bridge group 30 is forwarding
   Port 25 (Ethernet3/6) of bridge group 30 is forwarding

Bridge Group 40 is running the IEEE compatible Spanning Tree Protocol

   Port 26 (Ethernet3/7) of bridge group 40 is down
   Port 27 (Ethernet3/8) of bridge group 40 is down
   Port 28 (Ethernet3/9) of bridge group 40 is down
   Port 29 (Ethernet3/10) of bridge group 40 is down
Port 30 (Ethernet3/11) of bridge group 40 is down
Port 31 (Ethernet3/12) of bridge group 40 is down
Port 32 (Ethernet3/13) of bridge group 40 is down
```

show bridge multicast

To display transparent bridging multicast state information, use the **show bridge multicast** command in user EXEC or privileged EXEC mode.

show bridge [*bridge-group*] **multicast** [**router-ports** | **groups**] [*group-address*]

Syntax Description

bridge-group	(Optional) Bridge group number specified in the **bridge protocol** command.
router-ports	(Optional) Display information for multicast router ports.
groups	(Optional) Display information for multicast groups.
group-address	(Optional) Multicast IP address associated with a specific multicast group.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

The following is sample output from the **show bridge multicast** command:

```
Router# show bridge multicast

 Multicast router ports for bridge group 1:

  2 multicast router ports
   Fddi2/0         R
   Ethernet0/4     R

 Multicast groups for bridge group 1:

  235.145.145.223            RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0

  235.5.5.5                  RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0

  235.4.4.4                  RX count     TX count
   Fddi2/0         R                0            2
   Ethernet0/4     R                0            3
   Ethernet0/3     G                1            0
```

Table 9 describes the significant fields shown in the display.

Table 9 show bridge multicast Field Descriptions

Field	Description
Multicast router ports for…	List of the multicast router ports by bridge group. Within the bridge group cluster, the display lists the number of multicast router ports and then lists the ports by interface.
Multicast groups for…	List of the multicast groups by bridge group. Within each multicast group, identified by a unique address, the display lists each port by interface name and indicates whether that port is a group member (“G”), a multicast router port (“R”), or both. The receive (RX) and transmit (TX) counts show the number of multicast packets that have been constrained to the multicast group by the bridge.

show bridge vlan

To display virtual LAN subinterfaces, use the **show bridge vlan** command in privileged EXEC mode.

show bridge vlan

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show bridge vlan** command:

```
Router# show bridge vlan

Bridge Group: 50

Virtual LAN Trunking Interface(s):  vLAN Protocol:     vLAN ID:  State

Fddi2/0.1000                        IEEE 802.10        1000      forwarding
Fast Ethernet4/0.500                 Inter Switch Link  500       listening

Virtual LAN Native Interface(s):    State

Ethernet0/1                         forwarding
Serial1/1                           down
```

Table 10 describes the fields shown in the display.

Table 10 show bridge vlan Field Descriptions

Field	Description
Bridge Group	Bridge group to which these interfaces belong.
Virtual LAN Trunking Interface(s)	VLAN interface.
vLAN Protocol)	IEEE 802.10 or Cisco Inter-Switch Link (ISL) encapsulation.
vLAN ID	VLAN identifier that maintains VLAN identities between switches.

Table 10 show bridge vlan Field Descriptions (continued)

Field	Description
State	Spanning-tree port state of the interface.
Virtual LAN Native Interface(s):	Interfaces whose transparently bridged traffic will be propagated only to other LAN segments within the same virtual LAN.

show controllers token (IBM)

To display information about memory management, error counters, and the board itself, use the **show controllers token** command in privileged EXEC mode.

show controllers token

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Depending on the board being used, the output from the **show controllers token** command can vary. The **show controllers token** command also displays proprietary information. Thus, the information that the **show controllers token** command displays is of primary use to Cisco Systems technical personnel. Information that is useful to users can be obtained with the **show interfaces tokenring** command, described later.

Examples

The following is sample output from the **show controllers token** command of a CSC-IR or CSC-2R card:

```
Router# show controllers token

TR Unit 0 is board 0 - ring 0

 state 3, dev blk: 0x1D2EBC, mailbox: 0x2100010, sca: 0x2010000
   current address: 0000.3080.6f40, burned in address: 0000.3080.6f40
   current TX ptr: 0xBA8, current RX ptr: 0x800

   Last Ring Status: none

 Stats: soft:0/0, hard:0/0, sig loss:0/0
        tx beacon: 0/0, wire fault 0/0, recovery: 0/0
        only station: 0/0, remote removal: 0/0
   Bridge: local 3330, bnum 1, target 3583
     max_hops 7, target idb: 0x0, not local
   Interface failures: 0 -- Bkgnd Ints: 0
   TX shorts 0, TX giants 0

   Monitor state: (active)
     flags 0xC0, state 0x0, test 0x0, code 0x0, reason 0x0
 f/w ver: 1.0, chip f/w: '000000.ME31100', [bridge capable]
```

```
     SMT form of this command s: 1.01 kernel, 4.02 fastmac
     ring mode: F00, internal enables: SRB REM RPS CRS/NetMgr
     internal functional: 0000011A (0000011A), group: 00000000 (00000000)
     if_state: 1, ints: 0/0, ghosts: 0/0, bad_states: 0/0
     t2m fifo purges: 0/0
     t2m fifo current: 0, t2m fifo max: 0/0, proto_errs: 0/0
     ring: 3330, bridge num: 1, target: 3583, max hops: 7

Packet counts:
       receive total: 298/6197, small: 298/6197, large 0/0
               runts: 0/0, giants: 0/0
               local: 298/6197, bridged: 0/0, promis: 0/0
             bad rif: 0/0, multiframe: 0/0
       ring num mismatch 0/0, spanning violations 0
       transmit total: 1/25, small: 1/25, large 0/0
                runts: 0/0, giants: 0/0, errors 0/0
bad fs: 0/0, bad ac: 0
congested: 0/0, not present: 0/0
     Unexpected interrupts: 0/0, last unexp. int: 0

     Internal controller counts:
    line errors:  0/0, internal errors: 0/0
    burst errors: 0/0, ari/fci errors:  0/0
    abort errors: 0/0, lost frame: 0/0
    copy errors:  0/0, rcvr congestion: 0/0
    token errors: 0/0, frequency errors: 0/0
    dma bus errors: -/-, dma parity errors: -/-
     Internal controller smt state:
    Adapter MAC:     0000.3080.6f40, Physical drop:     00000000
    NAUN Address:    0000.a6e0.11a6, NAUN drop:         00000000
    Last source:     0000.a6e0.11a6, Last poll:         0000.3080.6f40
    Last MVID:       0006,           Last attn code:    0006
    Txmit priority:  0006,           Auth Class:        7FFF
    Monitor Error:   0000,           Interface Errors:  FFFF
    Correlator:      0000,           Soft Error Timer:  00C8
    Local Ring:      0000,           Ring Status:       0000
    Beacon rcv type: 0000,           Beacon txmit type: 0000
    Beacon type:     0000,           Beacon NAUN:       0000.a6e0.11a6
```

Table 11, Part 1 describes the fields shown in the first line of sample output.

Table 11, Part 1 show controllers token Field Descriptions

Field	Description
TR Unit 0	Unit number assigned to the Token Ring interface associated with this output.
is board 0	Board number assigned to the Token Ring controller board associated with this interface.
ring 0	Number of the Token Ring associated with this board.

In the following line, state 3 indicates the state of the board. The rest of this output line displays memory mapping that is of primary use to Cisco engineers.

```
state 3, dev blk: 0x1D2EBC, mailbox: 0x2100010, sca: 0x2010000
```

The following line also appears in **show interface token** output as the address and burned-in address (bia), respectively:

```
current address: 0000.3080.6f40, burned in address: 0000.3080.6f40
```

The following line displays buffer management pointers that change by board:

```
current TX ptr: 0xBA8, current RX ptr: 0x800
```

The following line indicates the ring status from the controller chipset. This information is used by LAN Network Manager:

```
Last Ring Status: none
```

The following line displays Token Ring statistics. See the Token Ring specification for more information:

```
Stats: soft:0/0, hard:0/0, sig loss:0/0
        tx beacon: 0/0, wire fault 0/0, recovery: 0/0
        only station: 0/0, remote removal: 0/0
```

The following line indicates that Token Ring communication has been enabled on the interface. If this line of output appears, the message "Source Route Bridge capable" should appear in the **show interfaces tokenring** display.

```
Bridge: local 3330, bnum 1, target 3583
```

Table 11, Part 2 describes the fields shown in the following line of sample output:

```
max_hops 7, target idb: 0x0, not local
```

Table 11, Part 2 show controllers token Field Descriptions

Field	Description
max_hops 7	Maximum number of bridges.
target idb: 0x0	Destination interface definition.
not local	Interface has been defined as a remote bridge.

The following line is specific to the hardware:

```
Interface failures: 0 -- Bkgnd Ints: 0
```

In the following line, transmit (TX) shorts are the number of packets the interface sends that are discarded because they are smaller than the medium's minimum packet size. TX giants are the number of packets the interface sends that are discarded because they exceed the medium's maximum packet size.

```
TX shorts 0, TX giants 0
```

The following line indicates the state of the controller. Possible values are active, failure, inactive, and reset.

```
Monitor state: (active)
```

The following line displays detailed information relating to the monitor state shown in the previous line of output. This information relates to the firmware on the controller. This information is relevant to Cisco engineers only if the monitor state is something other than active.

```
flags 0xC0, state 0x0, test 0x0, code 0x0, reason 0x0
```

Table 11, Part 3 describes the fields in the following line of output:

```
f/w ver: 1.0 expr 0, chip f/w: '000000.ME31100', [bridge capable]
```

Table 11, Part 3 show controllers token Field Descriptions

Field	Description
f/w ver: 1.0	Version of Cisco firmware on the board.
chip f/w: '000000.ME31100'	Firmware on the chipset.
[bridge capable]	Interface has not been configured for bridging, but it has that capability.

The following line displays the version numbers for the kernel and the accelerator microcode of the Madge firmware on the board; this firmware is the Logical Link Control (LLC) interface to the chipset:

```
SMT form of this command s: 1.01 kernel, 4.02 fastmac
```

The following line displays LAN Network Manager information that relates to ring status:

```
ring mode: F00, internal enables: SRB REM RPS CRS/NetMgr
```

The following line corresponds to the functional address and the group address shown in **show interfaces tokenring** output:

```
internal functional: 0000011A (0000011A), group: 00000000 (00000000)
```

The following line displays interface board state information that is proprietary:

```
if_state: 1, ints: 0/0, ghosts: 0/0, bad_states: 0/0
```

The following lines display information that is proprietary. Our engineers use this information for debugging purposes:

```
t2m fifo purges: 0/0
t2m fifo current: 0, t2m fifo max: 0/0, proto_errs: 0/0
```

Each of the fields in the following line maps to a field in the **show source bridge** display, as follows: ring maps to srn; bridge num maps to bn; target maps to trn; and max hops maps to max:

```
ring: 3330, bridge num: 1, target: 3583, max hops: 7
```

In the following lines of output, the number preceding the slash (/) indicates the count since the value was last displayed; the number following the slash (/) indicates the count since the system was last booted:

```
Packet counts:
       receive total: 298/6197, small: 298/6197, large 0/0
```

In the following line, the number preceding the slash (/) indicates the count since the value was last displayed; the number following the slash (/) indicates the count since the system was last booted. The runts and giants values that appear here correspond to the runts and giants values that appear in **show interfaces tokenring** output:

```
runts: 0/0, giants: 0/0
```

The following lines are receiver-specific information that Cisco engineers can use for debugging purposes:

```
local: 298/6197, bridged: 0/0, promis: 0/0
bad rif: 0/0, multiframe: 0/0
ring num mismatch 0/0, spanning violations 0
transmit total: 1/25, small: 1/25, large 0/0
runts: 0/0, giants: 0/0, errors 0/0
```

The following lines include very specific statistics that are not relevant in most cases, but exist for historical purposes. In particular, the internal errors, burst errors, ari/fci, abort errors, copy errors, frequency errors, dma bus errors, and dma parity errors fields are not relevant.

```
Internal controller counts:
 line errors: 0/0, internal errors: 0/0
 burst errors: 0/0, ari/fci errors: 0/0
 abort errors: 0/0, lost frame: 0/0
 copy errors: 0/0, rcvr congestion: 0/0
 token errors: 0/0, frequency errors: 0/0
 dma bus errors: -/-, dma parity errors: -/-
```

The following lines are low-level Token Ring interface statistics relating to the state and status of the Token Ring with respect to all other Token Rings on the line:

```
Internal controller smt state:
 Adapter MAC:     0000.3080.6f40, Physical drop:     00000000
 NAUN Address:    0000.a6e0.11a6, NAUN drop:         00000000
 Last source:     0000.a6e0.11a6, Last poll:         0000.3080.6f40
 Last MVID:       0006,           Last attn code:    0006
 Txmit priority:  0006,           Auth Class:        7FFF
 Monitor Error:   0000,           Interface Errors:  FFFF
 Correlator:      0000,           Soft Error Timer:  00C8
 Local Ring:      0000,           Ring Status:       0000
 Beacon rcv type: 0000,           Beacon txmit type: 0000
```

show drip

To display the status of the duplicate ring protocol (DRiP) database for a router or Route Switch Module (RSM), use the **show drip** command in privileged EXEC mode.

show drip

Syntax Descriptions

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show drip** command:

```
Router# show drip

DRIP Database for Mgmt Domain Fast Ethernet4/0
--------------------------------------------------
Mac Address 0010-A6AE-B440
Vlan     100    Status    30 : l-active, l-config,

Mac Address 0010-2F72-C800
Vlan      20    Status    0C : r-active, r-config,
Vlan    1003    Status    0C : r-active, r-config,

Statistics:
Advertisements received           126
Advertisements processed          1
Advertisements transmitted        131
Last revision transmitted         0x84
Last changed revision transmitted  0x2
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
interface vlan	Configures a Token Ring or Ethernet interface on the RSM.
show vlans	Displays virtual LAN subinterfaces.

show interfaces crb

To display the configuration for each interface that has been configured for routing or bridging, use the **show interfaces crb** command in privileged EXEC mode.

show interfaces crb

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show interfaces crb** command:

```
Router# show interfaces crb

Ethernet0/0

Routed protocols on Ethernet0/0:
appletalk decnet ip novell

Ethernet0/1

Routed protocols on Ethernet0/1:
appletalk  decnet  ip  novell

Ethernet0/2

Routed protocols on Ethernet0/2:
appletalk  ip

Bridged protocols on Ethernet0/2:
clns  decnet  vines  apollo
novell  xns

Software MAC address filter on Ethernet0/2
Hash Len   Address         Matches   Act   Type
0x00: 0    ffff.ffff.ffff  0         RCV   Physical broadcast
0x00: 1    ffff.ffff.ffff  0         RCV   Appletalk zone
0x2A: 0    0900.2b01.0001  0         RCV   DEC spanning tree
0x49: 0    0000.0c36.7a45  0         RCV   Interface MAC address
0xc0: 0    0100.0ccc.cccc  20        RCV   CDP
0xc2: 0    0180.c200.0000  0         RCV   IEEE spanning tree
0xF8: 0    0900.07ff.ffff  0         RCV   Appletalk broadcast
```

```
Ethernet0/3

Routed protocols on Ethernet0/3:
appletalk  ip

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

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

Table 12 describes the significant fields shown in the display.

Table 12 show interfaces crb Field Descriptions

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

show interfaces irb

To display the configuration for each interface that has been configured for integrated routing or bridging, use the **show interfaces irb** command in privileged EXEC mode.

show interfaces {**ethernet** | **fastethernet**} [*interface* | *slot*/*port*] **irb**

Syntax Description

ethernet	Specify Ethernet interface.
fastethernet	Specify Fast Ethernet interface.
interface	(Optional) Specific interface, such as Ethernet 0.
slot/*port*	(Optional) Specific slot and port, such as Fast Ethernet 3/0.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show interfaces irb** command:

```
Router# show interfaces ethernet 2 irb

Ethernet 2

Routed protocols on Ethernet 2:
appletalk ip

Bridged protocols on Ethernet 2:
appletalk   clns   decnet   vines
apollo      ipx    xns

Software MAC address filter on Ethernet 2
Hash Len  Address         Matches  Act   Type
0x00: 0   ffff.ffff.ffff  4886     RCV   Physical broadcast
0x1F: 0   0060.3e2b.a221  7521     RCV   Appletalk zone
0x1F: 1   0060.3e2b.a221  0        RCV   Bridge-group Virtual Interface
0x2A: 0   0900.2b01.0001  0        RCV   DEC spanning tree
0x05: 0   0900.0700.00a2  0        RCV   Appletalk zone
0xC2: 0   0180.c200.0000  0        RCV   IEEE spanning tree
0xF8: 0   0900.07ff.ffff  2110     RCV   Appletalk broadcast
```

The following example shows that IP is configured for the first PA-12E/2FE interface of the port adapter in slot 3:

```
Router# show interfaces fastethernet 3/0 irb

Fast Ethernet3/0
```

```
Routed protocols on Fast Ethernet3/0:
 ip

Bridged protocols on Fast Ethernet3/0:
 appletalk  clns       decnet     ip
 vines      apollo     ipx        xns

Software MAC address filter on Ethernet3/0
 Hash Len    Address      Matches  Act      Type
 0x00:  0 ffff.ffff.ffff         0 RCV Physical broadcast
 0x2A:  0 0900.2b01.0001         0 RCV DEC spanning tree
 0xC2:  0 0180.c200.0000         0 RCV IEEE spanning tree
 0xC7:  0 00e0.f7a4.5130         0 RCV Interface MAC address
 0xC7:  1 00e0.f7a4.5130         0 RCV Bridge-group Virtual Interface
```

Table 13 describes the significant fields shown in the displays.

Table 13 show interfaces irb Field Descriptions

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

show interfaces tokenring (IBM)

To display information about the Token Ring interface and the state of source-route bridging (SRB), use the **show interfaces tokenring** command in privileged EXEC mode.

show interfaces tokenring [*number*]

Syntax Description

number	(Optional) Interface number. If you do not provide a value, the command will display statistics for all Token Ring interfaces.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show interfaces tokenring** command:

```
Router# show interfaces tokenring

TokenRing 0 is up, line protocol is up
Hardware is 16/4 Token Ring, address is 5500.2000.dc27 (bia 0000.3000.072b)
   Internet address is  10.136.230.203, subnet mask is 255.255.255.0
   MTU 8136 bytes, BW 16000 Kb, DLY 630 usec, rely 255/255, load 1/255
   Encapsulation SNAP, loopback not set, keepalive set (10 sec)
   ARP type: SNAP, ARP Timeout 4:00:00
   Ring speed: 16 Mbps
   Single ring node, Source Route Bridge capable
   Group Address: 0x00000000, Functional Address: 0x60840000
   Last input 0:00:01, output 0:00:01, output hang never
   Output queue 0/40, 0 drops; input queue 0/75, 0 drops
   Five minute input rate 0 bits/sec, 0 packets/sec
   Five minute output rate 0 bits/sec, 0 packets/sec
   16339 packets input, 1496515 bytes, 0 no buffer
        Received 9895 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     32648 packets output, 9738303 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets, 0 restarts
     5 transitions
```

Table 14 describes the significant fields shown in the display.

Table 14 show interfaces tokenring Field Descriptions

Field	Description
Token Ring is up	Interface is currently active and inserted into ring (up) or inactive and not inserted (down).
Token Ring is Reset	Hardware error has occurred. This is not in the sample output; it is informational only.
Token Ring is Initializing	Hardware is up, in the process of inserting the ring. This is not in the sample output; it is informational only.
Token Ring is Administratively Down	Hardware has been taken down by an administrator. This is not in the sample output; it is informational only. "Disabled" indicates the Cisco IOS software has received over 5000 errors in a keepalive interval, which is 10 seconds by default.
line protocol is up	Indicates whether the software processes that handle the line protocol believe the interface is usable (that is, whether keepalives are successful).
Hardware	Specifies the hardware type. "Hardware is ciscoBus Token Ring" indicates that the board is a CSC-C2CTR board. "Hardware is 16/4 Token Ring" indicates that the board is a CSC-1R, CSC-2R, or a CSC-R16M board. Also shows the address of the interface.
Internet address	Lists the Internet address followed by the subnet mask.
MTU	Maximum transmission unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether loopback is set.
keepalive	Indicates whether keepalives are set.
ARP type	Type of Address Resolution Protocol assigned.
Ring speed	Speed of Token Ring—4 or 16 Mbps.
Single ring node	Indicates whether a node is enabled to collect and use source RIF for routable Token Ring protocols.
Group Address	Interface's group address, if any. The group address is a multicast address; any number of interfaces on the ring may share the same group address. Each interface may have at most one group address.
Functional Address	Bit-significant group address. Each "on" bit represents a function performed by the station.

Table 14 show interfaces tokenring Field Descriptions (continued)

Field	Description
Last input	Number of hours, minutes, and seconds since the last packet was received by an interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because the data took too long to send. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Output queue, drops input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
Five minute input rate, Five minute output rate	Average number of bits and packets sent per second in the last 5 minutes.
packets input	Total number of error-free packets received by the system.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium’s minimum packet size.
giants	Number of packets that are discarded because they exceed the medium’s maximum packet size.
CRC	Cyclic redundancy check (CRC) generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or problems sending data on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station sending bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver’s ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
packets output	Total number of messages sent by the system.
bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
underruns	Number of times that the far-end sender has been running faster than the near-end router’s receiver can handle. This may never be reported on some interfaces.

Table 14 show interfaces tokenring Field Descriptions (continued)

Field	Description
output errors	Sum of all errors that prevented the final sending of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Because a Token Ring cannot have collisions, this statistic is nonzero only if an unusual event occurred when frames were being queued or dequeued by the system software.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Should always be zero for Token Ring interfaces.
transitions	Number of times the ring made a transition from up to down, or vice versa. A large number of transitions indicates a problem with the ring or the interface.

show lnm bridge

Note Effective with Cisco IOS Release 12.3(4)T, the **show lnm bridge** command is not available in Cisco IOS 12.3T software.

To display all currently configured bridges and all parameters that are related to the bridge as a whole, not to one of its interfaces, use the **show lnm bridge** command in privileged EXEC mode.

show lnm bridge

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show lnm bridge** command:

```
Router# show lnm bridge

Bridge 001-2-003, Ports 0000.3000.abc4, 0000.0028.abcd
Active Links: 0000.0000.0000 0000.0000.0000 0000.0000.0000 0000.0000.0000
Notification: 0 min, Threshold 00.10%
```

Table 15 describes the significant fields shown in the display.

Table 15 show lnm bridge Field Descriptions

Field	Description
Bridge 001-2-003	Ring and bridge numbers of this bridge.
Ports 0000.3000.abc4....	MAC addresses of the two interfaces of this bridge.
Active Links:	Any LAN Network Manager (LNM) stations that are connected to this bridge. An entry preceded by an asterisk is the controlling LNM.
Notification: 0 min	Current counter notification interval in minutes.
Threshold 00.10%	Current loss threshold (in percent) that will trigger a message to the LNM.

show lnm config

Note Effective with Cisco IOS Release 12.3(4)T, the **show lnm config** command is not available in Cisco IOS 12.3T software.

To display the logical configuration of all bridges configured in a router, use the **show lnm config** command in privileged EXEC mode. This information is needed to configure an LAN Network Manager (LNM) Management Station to communicate with a router. This is especially important when the router is configured as a multiport bridge, thus employing the concept of a virtual ring.

show lnm config

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show lnm config** command for a simple two-port bridge:

```
Router# show lnm config

Bridge(s) currently configured:

           From     ring 001, address 0000.3000.abc4
           Across bridge 002
           To       ring 003, address 0000.0028.abcd
```

The following is sample output from the **show lnm config** command for a multiport bridge:

```
Router# show lnm config

Bridge(s) currently configured:

           From     ring 001, address 0000.0028.abc4
           Across bridge 001
           To       ring 008, address 4000.0028.abcd

           From     ring 002, address 0000.3000.abc4
           Across bridge 002
           To       ring 008, address 4000.3000.abcd
```

```
From     ring 003, address 0000.3000.5735
Across bridge 003
To       ring 008, address 4000.3000.5735
```

Table 16 describes the significant fields shown in the display.

Table 16 show lnm config Field Descriptions

Field	Description
From ring 001	Ring number of the first interface in the two-port bridge.
address 0000.3000.abc4	MAC address of the first interface in the two-port bridge.
Across bridge 002	Bridge number assigned to this bridge.
To ring 003	Ring number of the second interface in the two-port bridge.
address 0000.0028.abcd	MAC address of the second interface in the two-port bridge.

show lnm interface

Note Effective with Cisco IOS Release 12.3(4)T, the **show lnm interface** command is not available in Cisco IOS 12.3T software.

To display all LAN Network Manager (LNM)-related information about a specific interface or all interfaces, use the **show lnm interface** command in privileged EXEC mode.

show lnm interface [*type number*]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.

Defaults

The *type* argument is not specified, information about all interface types is displayed.
If *number* is not specified, information about all interface numbers is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is for all types of interfaces, including Token Ring interfaces. If you want information specific to Token Ring, use the **show lnm ring** command.

Examples

The following is sample output from the **show lnm interface** command:

```
Router# show lnm interface

 nonisolating error counts
interface  ring   Active Monitor  SET   dec   lost   cong.  fc    freq.token
TokenRing1 0001*  1000.5a98.23a0  00200 00001 00000  00000  00000 0000000002

Notification flags: FE00, Ring Intensive: FFFF, Auto Intensive: FFFF
Active Servers: LRM LBS REM RPS CRS
Last NNIN:   never, from 0000.0000.0000.
Last Claim:  never, from 0000.0000.0000.
Last Purge:  never, from 0000.0000.0000.
Last Beacon: never, 'none' from 0000.0000.0000.
Last MonErr: never, 'none' from 0000.0000.0000.

                 isolating error counts
station         int ring   loc.    weight line   inter  burst  ac    abort
1000.5a98.23a0  T1  0001   0000    00 - N00000   00000  00000  00000 00000
1000.5a98.239e  T1  0001   0000    00 - N00000   00000  00000  00000 00000
1000.5a6f.bc15  T1  0001   0000    00 - N00000   00000  00000  00000 00000
0000.3000.abc4  T1  0001   0000    00 - N00000   00000  00000  00000 00000
1000.5a98.239f  T1  0001   0000    00 - N00000   00000  00000  00000 00000
```

Table 17 describes the significant fields shown in the display. See the **show lnm station** command for a description of the fields that follow after the “isolating error counts” line in the sample output.

Table 17 show lnm interface Field Descriptions

Field	Description
interface	Interface about which information was requested.
ring	Number assigned to that Token Ring. An asterisk following the ring number indicates that stations with nonzero error counters are present on that ring.
Active Monitor	Address of the station that is providing “Active Monitor” functions to the ring. The description of this server can be found in the *IBM Token Ring Architecture Reference Manual.*
SET	Current soft error reporting time for the ring in units of tens of milliseconds.
dec	Rate at which the various counters of nonisolating errors are being decreased. This number is in errors per 30 seconds.
lost, cong., fc, freq.token	Current values of the five nonisolating error counters specified in the 802.5 specification. These are Lost Frame errors, Receiver Congestion errors, FC errors, Frequency errors, and Token errors.
Notification flags:	Representation of which types of ring errors are being reported to LNM. The description of this number can be found in the *IBM Token Ring Architecture Reference Manual.*
Ring Intensive:	Representation of which specific ring error messages are being reported to LNM when in the “Ring Intensive” reporting mode. The description of this number can be found in the *IBM Token Ring Architecture Reference Manual.*
Auto Intensive:	Representation of which specific ring error messages are being reported to LNM when in the “Auto Intensive” reporting mode. The description of this number can be found in the *IBM Token Ring Architecture Reference Manual.*

Table 17 show lnm interface Field Descriptions (continued)

Field	Description
Active Servers:	A list of which servers are active on this Token Ring. The acronyms and their meanings are as follows: • CRS—Configuration Report Server • LRM—LAN Reporting Manager • LBS—LAN Bridge Server • REM—Ring Error Monitor • RPS—Ring Parameter Server The description of these servers can be found in the *IBM Token Ring Architecture Reference Manual*.
Last NNIN:	Time since the last "Neighbor Notification Incomplete" frame was received, and the station that sent this message.
Last Claim:	Time since the last "Claim Token" frame was received, and the station that sent this message.
Last Purge:	Time since the last "Purge Ring" frame was received, and the station that sent this message.
Last Beacon:	Time since the last "Beacon" frame was received, the type of the last beacon frame, and the station that sent this message.
Last Mon Err:	Time since the last "Report Active Monitor Error" frame was received, the type of the last monitor error frame, and the station that sent this message.

Related Commands

Command	Description
show lnm ring	Displays all LNM information about a specific Token Ring or all Token Rings.
show lnm station	Displays LNM-related information about a specific station or all known stations on all rings.

show lnm ring

Note Effective with Cisco IOS Release 12.3(4)T, the **show lnm ring** command is not available in Cisco IOS 12.3T software.

To display all LAN Network Manager (LNM) information about a specific Token Ring or all Token Rings, use the **show lnm ring** command in privileged EXEC mode.

show lnm ring [*ring-number*]

Syntax Description

ring-number	(Optional) Number of a specific Token Ring. It can be a value in the range from 1 to 4095.

Defaults

If the *ring-number* argument is not specified, information about all Token Rings is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a specific interface is requested, it also displays a list of all active stations on that interface.

The output of this command is the same as the output of the **show lnm interface** command. See the **show lnm interface** and **show lnm station** commands for sample output and a description of the fields. The same information can be obtained by using the **show lnm interface** command, but instead of specifying an interface number, you specify a ring number as an argument.

Related Commands

Command	Description
show lnm interface	Displays all LNM-related information about a specific interface or all interfaces.
show lnm station	Displays LNM-related information about a specific station or all known stations on all rings.

show lnm station

Note Effective with Cisco IOS Release 12.3(4)T, the **show lnm station** command is not available in Cisco IOS 12.3T software.

To display LAN Network Manager (LNM)-related information about a specific station or all known stations on all rings, use the **show lnm station** command in privileged EXEC mode

show lnm station [*address*]

Syntax Description

address	(Optional) Address of a specific LNM station.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.3(4)T	This command was removed.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a specific station is requested, it also displays a detailed list of that station's current MAC-level parameters.

Examples

The following is sample output from the **show lnm station** command when a particular address has been specified:

```
Router# show lnm station 1000.5a6f.bc15

                                           isolating error counts
    station      int  ring  loc.    weight   line  inter burst   ac  abort
1000.5a6f.bc15    T1  0001  0000    00 - N   00000 00000 00000 00000 00000

Unique ID:  0000.0000.0000          NAUN: 0000.3000.abc4
Functional: C000.0000.0000         Group: C000.0000.0000
Physical Location:   00000        Enabled Classes:  0000
Allowed Priority:    00000        Address Modifier: 0000
Product ID:     00000000.00000000.00000000.00000000.0000
Ucode Level:    00000000.00000000.0000
Station Status: 00000000.0000
Last transmit status: 00
```

Table 18 describes the significant fields shown in the display.

Table 18 show lnm station Field Descriptions

Field	Description
station	MAC address of the given station on the Token Ring.
int	Interface used to reach the given station.
ring	Number of the Token Ring where the given station is located.
loc.	Physical location number of the given station.
weight	Weighted accumulation of the errors of the given station, and of its nearest active upstream neighbor (NAUN). The three possible letters and their meanings are as follows:[1] • N—not in a reported error condition. • P—in a "preweight" error condition. • W—in a "preweight" error condition.
isolating error counts	Current values of the five isolating error counters specified in the 802.5 specification. These are Line errors, Internal errors, Burst errors, AC errors, and Abort errors.
Values below this point will be zero unless the LNM has previously requested this information.	
Unique ID:	Uniquely assigned value for this station.
NAUN:	MAC address of this station's "upstream" neighbor.
Functional:	MAC-level functional address currently in use by this station.
Group:	MAC-level group address currently in use by this station.
Physical Location:	Number assigned to this station as its "Physical Location" identifier.
Enabled Classes:	Functional classes that the station is allowed to send.
Allowed Priority:	Maximum access priority that the station may use when sending onto the Token Ring.
Address Modifier:	Reserved field.
Product ID:	Encoded 18-byte string used to identify what hardware and software combination is running on this station.
Ucode Level:	10-byte extended binary coded decimal interchange code (EBCDIC) string indicating the microcode level of the station.
Station Status:	Implementation-dependent vector that is not specified anywhere.
Last transmit status:	Contains the strip status of the last "Report Transmit Forward" MAC frame forwarded by this interface.

[1] The description of these error conditions can be found in the *IBM Architecture Reference Manual*.

show netbios-cache

To display a list of NetBIOS cache entries, use the **show netbios-cache** command in privileged EXEC mode.

show netbios-cache

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show netbios-cache** command:

```
Router# show netbios-cache

  HW Addr          Name            How       Idle      NetBIOS Packet Savings
1000.5a89.449a     IC6W06_B        TR1       6         0
1000.5a8b.14e5     IC_9Q07A        TR1       2         0
1000.5a25.1b12     IC9Q19_A        TR1       7         0
1000.5a25.1b12     IC9Q19_A        TR1       10        0
1000.5a8c.7bb1     BKELSA1         TR1       4         0
1000.5a8b.6c7c     ICELSB1         TR1       -         0
1000.5a31.df39     ICASC_01        TR1       -         0
1000.5ada.47af     BKELSA2         TR1       10        0
1000.5a8f.018a     ICELSC1         TR1       1         0
```

Table 19 describes the significant fields shown in the display.

Table 19 show netbios-cache Field Descriptions

Field	Description
HW Addr	MAC address mapped to the NetBIOS name in this entry.
Name	NetBIOS name mapped to the MAC address in this entry.
How	Interface through which this information was learned.
Idle	Period of time (in seconds) since this entry was last accessed. A hyphen in this column indicates it is a static entry in the NetBIOS name cache.
NetBIOS Packet Savings	Number of packets to which local replies were made (thus preventing sending of these packets over the network).

Related Commands

Command	Description
netbios name-cache	Defines a static NetBIOS name cache entry, tying the server with the name netbios-name to the mac-address, and specifying that the server is accessible either locally through the interface-name specified, or remotely through the ring-group group-number specified.
netbios name-cache timeout	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.

show pxf cpu statistics

To display parallel express forwarding (PXF) central processing unit (CPU) statistics for a configured router, use the **show pxf cpu statistics** command in privilege EXEC mode.

show pxf cpu statistics [**crtp** | **diversion** | **drop** | **ip** | **mlp** | **qos** | **spd**]

Syntax Description

crtp	(Optional) IP header compression statistics.
diversion	(Optional) Packets that need to be bridged, as well as control packets such as Spanning Tree Protocol (STP) and Virtual Router Redundancy Protocol (VRRP), that are not processed by PXF and are diverted to a route processor (RP).
drop	(Optional) Packets that are dropped by the PXF.
ip	(Optional) IP statistics.
mlp	(Optional) Multilink PPP (MLP) statistics.
qos	(Optional) Quality of Service (QoS) statistics.
spd	(Optional) Multicast Selective Packet Discard (SPD) statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.3(14)T	This command was enhanced to include counters for Integrated Routing and Bridging (IRB) functionality.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show pxf cpu statistics** command for diversion statistics:

```
Router# show pxf cpu statistics diversion

Diversion Cause Stats:
 local      = 31
 dest       = 0
 option     = 0
 protocol   = 0
 encap      = 0
 oam f5     = 149
 oam f4     = 0
 atm ilmi   = 0
 comp       = 0
 ip_sanity  = 0
 ip_bcast   = 0
 ip_dest    = 0
 fib_punt   = 0
 mtu       = 0
 arp       = 1
 rarp      = 0
 icmp      = 0
 divert    = 0
 no_group  = 0
 direct    = 0
 local_mem = 0
 p2p_prune = 0
 assert    = 0
 dat_prune = 0
 join_spt  = 0
 null_out  = 0
 igmp      = 0
 register  = 0
 no_fast   = 0
 ipc_resp  = 0
 keepalive = 0
 min_mtu   = 0
 icmp_frag = 0
 icmp_bad  = 0
 mpls_ttl  = 0
 tfib      = 0
 multicast = 0
 clns_isis = 0
 ppp_cntrl = 0
 tun_norte = 0
 tun_nofrg = 0
 ctcp_in   = 0
 vsi_sig   = 8
 mvpn_tfrg = 0
 cdp       = 0

!IRB counters

 smf_msmtch= 0
 irb_stp   = 0
 brdg_ip   = 0
 no_rt_ip  = 0
 multi_mac = 0
```

Related Commands

Command	Description
debug pxf tbridge	Displays debugging output of the PXF transparent bridging.
show pxf cpu subblock	Displays PXF CPU for a bridged subinterface.
show pxf cpu tbridge	Displays PXF CPU statistics for transparent bridging.

show pxf cpu subblock

To display parallel express forwarding (PXF) central processing unit (CPU) statistics for a bridged subinterface (encapsulation type), use the **show pxf cpu subblock** command in privileged EXEC mode.

show pxf cpu subblock *interface-name*

Syntax Description

interface-name	Name of the interface.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2	This command was introduced.
12.3(14)T	This command was enhanced to display more information for all subblocks.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show pxf cpu subblock** command, which shows the bridge-group virtual interface software MAC-address filtering (SMF) table:

```
Router# show pxf cpu subblock switch1.100

Switch1.100 is up

 ICB = C001, LinkId = 3, interface PXF, enabled
 IOS encapsulation type 33 ATM

!BVI encapsulation denoted by the type.

 ICB: Index: 49155 Min mtu: 4 Max mtu: 4486 Encapsulation Type:8
 VCCI maptable location = 0x8340A800
 VCCImap entry: vcci: 0x5   u0 : 0x64   Max mtu : 4486
             Min mtu : 0x4   vc_type_flags: 0x20
 VCCI 0x5        seg channel id 0x1A5
    icmp ipaddress 10.4.4.1          timestamp 0
    feature_data: flags 0x0000 fib_index 0x0
 col_5_cicb.flags : 0x00
```

Related Commands

Command	Description
debug pxf tbridge	Displays debugging output of the PXF transparent bridging.
show pxf cpu statistics	Displays PXF CPU statistics for a configured router.
show pxf cpu tbridge	Displays PXF CPU statistics for transparent bridging.

show pxf cpu tbridge

To display parallel express forwarding (PXF) central processing unit (CPU) statistics for transparent bridging, use the **show pxf cpu tbridge** command in privileged EXEC mode.

show pxf cpu tbridge

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show pxf cpu tbridge** command, which shows the bridge-group virtual interface software MAC-address filtering (SMF) table:

```
Router# show pxf cpu tbridge

Bridge-group Virtual Interface SMF table ========================================

SMF Entry    Mac Address     SMF MATCH     BVI Flags
     1      0000.0000.0000           0      0x0
     2      0000.0000.0000           0      0x0
     3      0000.0000.0000           0      0x0
     4      0000.0000.0000           0      0x0
     5      0000.0000.0000           0      0x0
     6      0000.0000.0000           0      0x0
     7      0000.0000.0000           0      0x0
     8      0000.0000.0000           0      0x0
     9      0000.0000.0000           0      0x0

!Entry for BVI 10.

    10      0000.0c09.6504           0      0x1

!Bridged packets.

    11      0000.0000.0000           0      0x0001
    12      0000.0000.0000           0      0x0
    13      0000.0000.0000           0      0x0
    14      0000.0000.0000           0      0x0
    15      0000.0000.0000           0      0x0
    16      0000.0000.0000           0      0x0
    17      0000.0000.0000           0      0x0

!Routed packets.
```

```
    18      0000.0000.0000          0      0x0100
    19      0000.0000.0000          0      0x0
    20      0000.0000.0000          0      0x0
.
.
```

Related Commands

Command	Description
debug pxf tbridge	Displays debugging output of the PXF transparent bridging.
show pxf cpu statistics	Displays PXF CPU statistics for a configured router.
show pxf cpu subblock	Displays PXF CPU statistics for a bridged subinterface.

show rif

To display the current contents of the Routing Information Field (RIF) cache, use the **show rif** command in privileged EXEC mode.

show rif

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show rif** command:

```
Router# show rif

Codes: * interface, - static, + remote
Hardware Addr  How   Idle (min)  Routing Information Field
5C02.0001.4322 rg5           -   0630.0053.00B0
5A00.0000.2333 TR0           3   08B0.0101.2201.0FF0
5B01.0000.4444 -             -   -
0000.1403.4800 TR1           0   -
0000.2805.4C00 TR0           *   -
0000.2807.4C00 TR1           *   -
0000.28A8.4800 TR0           0   -
0077.2201.0001 rg5          10   0830.0052.2201.0FF0
```

In the display, entries marked with an asterisk (*) are the router's interface addresses. Entries marked with a dash (-) are static entries. Entries with a number denote cached entries. If the RIF timeout is set to something other than the default of 15 minutes, the timeout is displayed at the top of the display. Table 20 describes the significant fields shown in the display.

Table 20 show rif Field Descriptions

Field	Description
Hardware Addr	Lists the MAC-level addresses.
How	Describes how the RIF has been learned. Values are ring group (rg) or interface (TR).
Idle (min)	Indicates how long, in minutes, since the last response was received directly from this node.
Routing Information Field	Lists the RIF.

Related Commands

Command	Description
multiring	Enables collection and use of RIF information.

show source-bridge

To display the current source bridge configuration and miscellaneous statistics, use the **show source-bridge** command in privileged EXEC mode.

show source-bridge [**interface**]

Syntax Description

interface	(Optional) Displays the current source bridge configuration over all interfaces and a summary of all packets sent and received over each interface, not just the number of packets forwarded through the bridge.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show source-bridge** command:

```
Router# show source-bridge

Local Interfaces:                           receive     transmit
             srn bn  trn r p s n  max hops     cnt         cnt        drops
TR0            5  1   10 *   *          7    39:1002     23:62923

Ring Group 10:
  This peer: TCP 10.136.92.92
   Maximum output TCP queue length, per peer: 100
  Peers:                 state   lv  pkts_rx  pkts_tx  expl_gn    drops TCP
   TCP  10.136.92.92     -       2       0        0         0     0    0
   TCP  10.136.93.93     open    2*     18       18         3     0    0
Rings:
   bn: 1 rn: 5    local  ma: 4000.3080.844b TokenRing0            fwd: 18
   bn: 1 rn: 2   remote  ma: 4000.3080.8473 TCP  10.136.93.93     fwd: 36

Explorers: ------- input -------             ------- output -------
       spanning  all-rings     total      spanning  all-rings     total
  TR0         0          3         3             3          5         8
```

The following is sample output from the **show source-bridge** command when Token Ring LAN emulation (LANE) is configured.

```
Router# show source-bridge
```

```
Local Interfaces:                           receive     transmit
             srn bn  trn r p s n  max hops     cnt         cnt        drops
AT2/0.1     2048  5  256 *   f    7  7  7     5073        5072          0
To3/0/0        1  1  256 *   f    7  7  7     4719        4720          0

Global RSRB Parameters:
 TCP Queue Length maximum: 100

Ring Group 256:
  No TCP peername set, TCP transport disabled
   Maximum output TCP queue length, per peer: 100
  Rings:
   bn: 5  rn: 2048 local  ma: 4000.0ca0.5b40 ATM2/0.1              fwd: 5181
   bn: 1  rn: 1    local  ma: 4000.3005.da06 TokenRing3/0/0        fwd: 5180

Explorers: ------- input -------             ------- output -------
         spanning  all-rings     total      spanning  all-rings     total
AT2/0.1         9          1        10            10          0        10
To3/0/0        10          0        10             9          1        10

  Local: fastswitched 20        flushed 0         max Bps 38400

         rings      inputs         bursts         throttles     output drops
       To3/0/0           10              0                 0                0
```

The following is sample output from the **show source-bridge** command with the **interface** keyword specified:

```
Router# show source-bridge interface

                                           v p s n r                    Packets
 Interface  St  MAC-Address    srn bn  trn r x p b c IP-Address          In   Out

 To0/0      up 0000.300a.7c06    1  1 2009 *   b   F 10.2.0.9         63836 75413
 To0/1      up 0000.300a.7c86    2  1 2009 *   b   F 10.1.0.9         75423 63835
 To0/2      up 0000.300a.7c46 1001  1 2009 *   b   F                   5845  5845
```

Table 21 describes the significant fields shown in the displays.

Table 21 show source-bridge Field Descriptions

Field	Description
Local Interfaces:	Description of local interfaces.
srn	Ring number of this Token Ring.
bn	Bridge number of this router for this ring.
trn	Group in which the interface is configured. Can be the target ring number or virtual ring group.
r	Ring group is assigned. An asterisk (*) in this field indicates that a ring group has been assigned for this interface.
p	Interface can respond with proxy explorers. An asterisk (*) in this field indicates that the interface can respond to proxy explorers.
s	Spanning-tree explorers enabled on the interface. An asterisk (*) indicates that this interface will forward spanning-tree explorers.

Table 21 show source-bridge Field Descriptions (continued)

Field	Description
n	Interface has NetBIOS name caching enabled. An asterisk (*) in this field indicates that the interface has NetBIOS name caching enabled.
max hops	Maximum number of hops.
receive cnt	Bytes received on the interface for source bridging.
transmit cnt	Bytes sent on the interface for source bridging.
drops	Number of dropped packets.
Ring Group *n*:	The number of the ring group.
This peer:	Address and address type of this peer.
Maximum output TCP queue length, per peer:	Maximum number of packets queued on this peer before the Cisco IOS software starts dropping packets.
Peers:	Addresses and address types of the ring group peers.
state	Current state of the peer, open or closed. A hyphen indicates this router.
lv	Indicates local acknowledgment.
pkts_rx	Number of packets received.
pkts_tx	Number of packets sent.
expl_gn	Explorers generated.
drops	Number of packets dropped.
TCP	Lists the current TCP backup queue length.
Rings:	Describes the ring groups. Information displayed is the bridge groups, ring groups, whether each group is local or remote, the MAC address, the network address or interface type, and the number of packets forwarded. A type shown as “locvrt” indicates a local virtual ring used by SDLLC or SR/TLB; a type shown as “remvrt” indicates a remote virtual ring used by SDLC Logical Link Control (SDLLC) or source-route translational bridging (SR/TLB).
Explorers:	This section describes the explorer packets that the Cisco IOS software has sent and received.
input	Explorers received by Cisco IOS software.
output	Explorers generated by Cisco IOS software.
TR0	Interface on which explorers were received.
spanning	Spanning-tree explorers.
all-rings	All-rings explored.
total	Summation of spanning and all-rings.
fastswitched	Number of fast-switched packets.
flushed	Number of flushed packets.
max Bps	Maximum bytes per second.
rings	Interface for the particular ring.
inputs	Number of inputs.
bursts	Number of bursts.

Table 21 show source-bridge Field Descriptions (continued)

Field	Description
throttles	Number of throttles.
output drops	Number of output drops.

show span

To display the spanning-tree topology known to the router, use the **show span** command in user EXEC or privileged EXEC mode.

show span

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

The following is sample output from the **show span** command:

```
Router# show span

Bridge Group 1 is executing the IBM compatible Spanning Tree Protocol
  Bridge Identifier has priority 32768, address 0000.0c0c.f68b
  Configured hello time 2, max age 6, forward delay 4
  Current root has priority 32768, address 0000.0c0c.f573
  Root port is 001A (TokenRing0/0), cost of root path is 16
  Topology change flag not set, detected flag not set
  Times:  hold 1, topology change 30, notification 30
          hello 2, max age 6, forward delay 4, aging 300
  Timers: hello 0, topology change 0, notification 0
Port 001A (TokenRing0/0) of bridge group 1 is forwarding. Path cost 16
   Designated root has priority 32768, address 0000.0c0c.f573
   Designated bridge has priority 32768, address 0000.0c0c.f573
   Designated port is 001B, path cost 0, peer 0
   Timers: message age 1, forward delay 0, hold 0
Port 002A (TokenRing0/1) of bridge group 1 is blocking. Path cost 16
   Designated root has priority 32768, address 0000.0c0c.f573
   Designated bridge has priority 32768, address 0000.0c0c.f573
   Designated port is 002B, path cost 0, peer 0
   Timers: message age 0, forward delay 0, hold 0
Port 064A (spanRSRB) of bridge group 1 is disabled. Path cost 250
   Designated root has priority 32768, address 0000.0c0c.f573
   Designated bridge has priority 32768, address 0000.0c0c.f68b
   Designated port is 064A, path cost 16, peer 0
   Timers: message age 0, forward delay 0, hold 0
```

A port (spanRSRB) is created with each virtual ring group. The port will be disabled until one or more peers go into open state in the ring group.

show spanning-tree

To display spanning-tree information for the specified spanning-tree instances, use the **show spanning-tree** command in privileged EXEC mode.

Cisco 2600, 3660, and 3845 Series Switches

show spanning-tree [*bridge-group*] [**active** | **backbonefast** | **blockedports** | **bridge** | **brief** | **inconsistentports** | **interface** *interface-type interface-number*| **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id*]

Cisco 6500/6000 Catalyst Series Switches and Cisco 7600 Series Routers

show spanning-tree [*bridge-group* | **active** | **backbonefast** | **bridge** [*id*] | **detail** | **inconsistentports** | **interface** *interface-type interface-number* [**portfast** [**edge**]] | **mst** [*list* | **configuration** [**digest**]] | **root** | **summary** [**totals**] | **uplinkfast** | **vlan** *vlan-id* | **port-channel** *number* | **pathcost** *method*]

Syntax Description

bridge-group	(Optional) Specifies the bridge group number. The range is 1 to 255.
active	(Optional) Displays spanning-tree information on active interfaces only.
backbonefast	(Optional) Displays spanning-tree BackboneFast status.
blockedports	(Optional) Displays blocked port information.
bridge	(Optional) Displays status and configuration of this switch.
brief	(Optional) Specifies a brief summary of interface information.
configuration [**digest**]	(Optional) Displays the multiple spanning-tree current region configuration.
inconsistentports	(Optional) Displays information about inconsistent ports.
interface *interface-type interface-number*	(Optional) Specifies the type and number of the interface. Enter each interface designator, using a space to separate it from the one before and the one after. Ranges are not supported. Valid interfaces include physical ports and virtual LANs (VLANs). See the “Usage Guidelines” for valid values.
list	(Optional) Specifies a multiple spanning-tree instance list.
mst	(Optional) Specifies multiple spanning-tree.
portfast [**edge**]	(Optional) Displays spanning-tree PortFast edge interface operational status. Beginning with Cisco IOS Release 12.2(33)SXI, the **edge** keyword is required. In earlier releases, the **edge** keyword is not used.
root	(Optional) Displays root-switch status and configuration.
summary	(Optional) Specifies a summary of port states.
totals	(Optional) Displays the total lines of the spanning-tree state section.
uplinkfast	(Optional) Displays spanning-tree UplinkFast status.
vlan *vlan-id*	(Optional) Specifies the VLAN ID. The range is 1 to 1005. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094. If the *vlan-id* value is omitted, the command applies to the spanning-tree instance for all VLANs.

id	(Optional) Identifies the spanning tree bridge.
detail	(Optional) Shows status and configuration details.
port-channel *number*	(Optional) Identifies the Ethernet channel associated with the interfaces.
pathcost *method*	(Optional) Displays the default path-cost calculation method that is used. See the "Usage Guidelines" section for the valid values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.0(5.2)WC(1)	This command was integrated into Cisco IOS Release 12.0(5.2)WC(1).
12.1(6)EA2	This command was integrated into Cisco IOS Release 12.1(6)EA2. The following keywords and arguments were added: *bridge-group*, **active**, **backbonefast**, **blockedports**, **bridge**, **inconsistentports**, **pathcost** *method*, **root**, **totals**, and **uplinkfast**.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(15)ZJ	The syntax added in Cisco IOS Release 12.1(6)EA2 was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(4)T	The platform support and syntax added in Cisco IOS Release 12.2(15)ZJ was integrated into Cisco IOS Release 12.3(4)T.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1–4094 for specified platforms.
12.2(33)SXI	This command was modified to require the **edge** keyword after **portfast**. The command output was modified to show the status of Bridge Assurance and PVST Simulation.

Usage Guidelines

The keywords and arguments that are available with the **show spanning-tree** command vary depending on the platform you are using and the network modules that are installed and operational.

Cisco 2600, 3660, and 3845 Series Switches

The valid values for **interface** *interface-type* are:

- **fastethernet**—Specifies a Fast Ethernet IEEE 802.3 interface.
- **port-channel**—Specifies an Ethernet channel of interfaces.

Cisco 6500/6000 Catalyst Switches and 7600 Series Routers

The **port-channel** *number* values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewal Services Module (FWSM) only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 2 to 13 and valid values for the port number are from 1 to 48.

When checking spanning tree-active states and you have a large number of VLANs, you can enter the **show spanning-tree summary total** command. You can display the total number of VLANs without having to scroll through the list of VLANs.

The valid values for **interface** *interface-type* are:

- **fastethernet**—Specifies a Fast Ethernet IEEE 802.3 interface.
- **port-channel**—Specifies an Ethernet channel of interfaces.
- **atm**—Specifies an Asynchronous Transfer Mode (ATM) interface.
- **gigabitethernet**—Specifies a Gigabit Ethernet IEEE 802.3z interface.
- **multilink**—Specifies a multilink-group interface.
- **serial**—Specifies a serial interface.
- **vlan**—Specifies a catalyst VLAN interface.

The valid values for keyword **pathcoast** *method* are:

- **append**—Appends the redirected output to a URL (supporting the append operation).
- **begin**—Begins with the matching line.
- **exclude**—Excludes matching lines.
- **include**—Includes matching lines.
- **redirect**—Redirects output to a URL.
- **tee**—Copies output to a URL.

When you run the **show spanning-tree** command for a VLAN or an interface the switch router will display the different port states for the VLAN or interface. The valid spanning-tree port states are listening, learning, forwarding, blocking, disabled, and loopback. See Table 22 for definitions of the port states:

Table 22 show spanning-tree vlan Command Port States

Field	Definition
LIS	Listening is when the port spanning tree initially starts to listen for BPDU packets for the root bridge.
LRN	Learning is when the port sets the proposal bit on the BPDU packets it sends out
FWD	Forwarding is when the port is sending and listening to BPDU packets and forwarding traffic.
BLK	Blocked is when the port is still sending and listening to BPDU packets but is not forwarding traffic.
DIS	Disabled is when the port is not sending or listening to BPDU packets and is not forwarding traffic.
LBK	Loopback is when the port recieves its own BPDU packet back.

Examples

Cisco 2600, 3660, and 3845 Series Switches

The following example shows that bridge group 1 is running the VLAN Bridge Spanning Tree Protocol:

```
Router# show spanning-tree 1

Bridge group 1 is executing the VLAN Bridge compatible Spanning Tree Protocol
Bridge Identifier has priority 32768, address 0000.0c37.b055
Configured hello time 2, max age 30, forward delay 20
We are the root of the spanning tree
Port Number size is 10 bits
Topology change flag not set, detected flag not set
Times: hold 1, topology change 35, notification 2
      hello 2, max age 30, forward delay 20
Timers: hello 0, topology change 0, notification 0
  bridge aging time 300

Port 8 (Ethernet1) of Bridge group 1 is forwarding
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 0000.0c37.b055
   Designated bridge has priority 32768, address 0000.0c37.b055
   Designated port is 8, path cost 0
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 184, received 0
```

The following is sample output from the **show spanning-tree summary** command:

```
Router# show spanning-tree summary

UplinkFast is disabled

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
VLAN1                23       0         0        1          24
-------------------- -------- --------- -------- ---------- ----------
              1 VLAN 23       0         0        1          24
```

Table 23 describes the significant fields shown in the display.

Table 23 show spanning-tree summary Field Descriptions

Field	Description
UplinkFast	Indicates whether the spanning-tree UplinkFast feature is enabled or disabled.
Name	Name of VLAN.
Blocking	Number of ports in the VLAN in a blocking state.
Listening	Number of ports in a listening state.
Learning	Number of ports in a learning state.
Forwarding	Number of ports in a forwarding state.
STP Active	Number of ports using the Spanning-Tree Protocol.

The following is sample output from the **show spanning-tree brief** command:

```
Router# show spanning-tree brief

VLAN1
  Spanning tree enabled protocol IEEE
  ROOT ID    Priority 32768
             Address 0030.7172.66c4
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
VLAN1
  Spanning tree enabled protocol IEEE
  ROOT ID    Priority 32768
             Address 0030.7172.66c4
Port                          Designated
Name     Port ID Prio Cost Sts  Cost  Bridge ID      Port ID
------- ------- ---- ---- ---  ----  -------------- -------
Fa0/11  128.17  128  100  BLK  38    0404.0400.0001 128.17
Fa0/12  128.18  128  100  BLK  38    0404.0400.0001 128.18
Fa0/13  128.19  128  100  BLK  38    0404.0400.0001 128.19
Fa0/14  128.20  128  100  BLK  38    0404.0400.0001 128.20
Fa0/15  128.21  128  100  BLK  38    0404.0400.0001 128.21
Fa0/16  128.22  128  100  BLK  38    0404.0400.0001 128.22
Fa0/17  128.23  128  100  BLK  38    0404.0400.0001 128.23
Fa0/18  128.24  128  100  BLK  38    0404.0400.0001 128.24
Fa0/19  128.25  128  100  BLK  38    0404.0400.0001 128.25
Fa0/20  128.26  128  100  BLK  38    0404.0400.0001 128.26
Fa0/21  128.27  128  100  BLK  38    0404.0400.0001 128.27

Port                          Designated
Name     Port ID Prio Cost Sts  Cost  Bridge ID      Port ID
------- ------- ---- ---- ---  ----  -------------- -------
Fa0/22  128.28  128  100  BLK  38    0404.0400.0001 128.28
Fa0/23  128.29  128  100  BLK  38    0404.0400.0001 128.29
Fa0/24  128.30  128  100  BLK  38    0404.0400.0001 128.30 Hello Time   2 sec  Max Age 20
sec  Forward Delay 15 sec
```

Table 24 describes the significant fields shown in the display.

Table 24 show spanning-tree brief Field Descriptions

Field	Description
VLAN1	VLAN for which spanning-tree information is shown.
Spanning tree enabled protocol	Type of spanning tree (IEEE, IBM, CISCO).
ROOT ID	Indicates the root bridge.
Priority	Priority indicator.
Address	MAC address of the port.
Hello Time	Amount of time, in seconds, that the bridge sends bridge protocol data units (BPDUs).
Max Age	Amount of time, in seconds, that a BPDU packet should be considered valid.
Forward Delay	Amount of time, in seconds, that the port spends in listening or learning mode.
Port Name	Interface type and number of the port.
Port ID	Identifier of the named port.
Prio	Priority associated with the port.

Table 24 show spanning-tree brief Field Descriptions (continued)

Field	Description
Cost	Cost associated with the port.
Sts	Status of the port.
Designated Cost	Designated cost for the path.
Designated Bridge ID	Bridge identifier of the bridge assumed to be the designated bridge for the LAN associated with the port.

The following is sample output from the **show spanning-tree vlan 1** command:

```
Router# show spanning-tree vlan 1

Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00e0.1eb2.ddc0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0010.0b3f.ac80
  Root port is 5, cost of root path is 10
  Topology change flag not set, detected flag not set, changes 1
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0

Interface Fa0/1  in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 0010.0b3f.ac80
Designated bridge has priority 32768, address 00e0.1eb2.ddc0
   Designated port is 1, path cost 10
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
```

Table 25 describes the significant fields shown in the display.

Table 25 show spanning-tree vlan Field Descriptions

Field	Description
Spanning tree	Type of spanning tree (IEEE, IBM, CISCO).
Bridge Identifier	Part of the bridge identifier and taken as the most significant part for bridge ID comparisons.
address	Bridge MAC address.
Root port	Identifier of the root port.
Topology change	Flags and timers associated with topology changes.

The following is sample output from the **show spanning-tree interface fastethernet0/3** command:

```
Router# show spanning-tree interface fastethernet0/3

Interface Fa0/3 (port 3) in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 6000, address 0090.2bba.7a40
   Designated bridge has priority 32768, address 00e0.1e9f.4abf
   Designated port is 3, path cost 410
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
```

Cisco 6500/6000 Series Catalyst Switches and 7600 Series Routers

This example shows how to display a summary of interface information:

```
Router# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    4097
             Address     0004.9b78.0800
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     0004.9b78.0800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface        Port ID                     Designated                Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID            Prio.Nbr
---------------- -------- --------- --- --------- -------------------- --------
Gi2/1            128.65           4 LIS         0  4097 0004.9b78.0800 128.65
Gi2/2            128.66           4 LIS         0  4097 0004.9b78.0800 128.66
Fa4/3            128.195         19 LIS         0  4097 0004.9b78.0800 128.195
Fa4/4            128.196         19 BLK         0  4097 0004.9b78.0800 128.195

Router#
```

Table 26 describes the fields that are shown in the example.

Table 26 show spanning-tree Command Output Fields

Field	Definition
Port ID Prio.Nbr	Port ID and priority number.
Cost	Port cost.
Sts	Status information.

This example shows how to display information about the spanning tree on active interfaces only:

```
Router# show spanning-tree active

UplinkFast is disabled
BackboneFast is disabled

 VLAN1 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0050.3e8d.6401
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 16384, address 0060.704c.7000
  Root port is 265 (FastEthernet5/9), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 18:13:54 ago
  Times:  hold 1, topology change 24, notification 2
          hello 2, max age 14, forward delay 10
  Timers: hello 0, topology change 0, notification 0

Router#
```

This example shows how to display the status of spanning-tree BackboneFast:

```
Router# show spanning-tree backbonefast

BackboneFast is enabled

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs)     : 0
Number of RLQ request PDUs received (all VLANs)   : 0
Number of RLQ response PDUs received (all VLANs)  : 0
Number of RLQ request PDUs sent (all VLANs)       : 0
Number of RLQ response PDUs sent (all VLANs)      : 0
Router#
```

This example shows how to display information about the spanning tree for this bridge only:

```
Router# show spanning-tree bridge

VLAN1
  Bridge ID  Priority    32768
             Address     0050.3e8d.6401
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
.
Router#
```

This example shows how to display detailed information about the interface:

```
Router# show spanning-tree detail

VLAN1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 4096, address 00d0.00b8.1401
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 9 last change occurred 02:41:34 ago
from FastEthernet4/21
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 1, topology change 0, notification 0, aging 300


Port 213 (FastEthernet4/21) of VLAN1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.213.
Designated root has priority 4096, address 00d0.00b8.1401
Designated bridge has priority 4096, address 00d0.00b8.1401
Designated port id is 128.213, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
BPDU: sent 4845, received 1
Router#
```

This example shows how to display information about the spanning tree for a specific interface:

```
Router# show spanning-tree interface fastethernet 5/9

Interface Fa0/10 (port 23) in Spanning tree 1 is ROOT-INCONSISTENT
Port path cost 100, Port priority 128
Designated root has priority 8192, address 0090.0c71.a400
Designated bridge has priority 32768, address 00e0.1e9f.8940
```

This example shows how to display information about the spanning tree for a specific bridge group:

```
Router# show spanning-tree 1

UplinkFast is disabled
 BackboneFast is disabled

  Bridge group 1 is executing the ieee compatible Spanning Tree protocol
   Bridge Identifier has priority 32768, address 00d0.d39c.004d
   Configured hello time 2, max age 20, forward delay 15
   Current root has priority 32768, address 00d0.d39b.fddd
   Root port is 7 (FastEthernet2/2), cost of root path is 19
   Topology change flag set, detected flag not set
   Number of topology changes 3 last change occurred 00:00:01 ago
           from FastEthernet2/2
   Times:  hold 1, topology change 35, notification 2
           hello 2, max age 20, forward delay 15
   Timers: hello 0, topology change 0, notification 0  bridge aging time 15

Port 2 (Ethernet0/1/0) of Bridge group 1 is down

    Port path cost 100, Port priority 128
    Designated root has priority 32768, address 0050.0bab.1808
    Designated bridge has priority 32768, address 0050.0bab.1808
    Designated port is 2, path cost 0
    Timers: message age 0, forward delay 0, hold 0
    BPDU: sent 0, received 0
Router#
```

This example shows how to display a summary of port states:

```
Router# show spanning-tree summary

Root bridge for: Bridge group 1, VLAN0001, VLAN0004-VLAN1005
 VLAN1013-VLAN1499, VLAN2001-VLAN4094
EtherChannel misconfiguration guard is enabled
Extended system ID is enabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
1 bridge               0        0         0        1          1
3584 vlans 3584 0 0 7168 10752


Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                  3584     0         0        7169       10753
Router#
```

This example shows how to display the total lines of the spanning-tree state section:

```
Router#  show spanning-tree summary total
Root bridge for:Bridge group 10, VLAN1, VLAN6, VLAN1000.
Extended system ID is enabled.
PortFast BPDU Guard is disabled
EtherChannel misconfiguration guard is enabled
UplinkFast is disabled
BackboneFast is disabled
```

```
Default pathcost method used is long

Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
           105 VLANs 3433     0         0        105        3538

BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) :0
Number of inferior BPDUs received (all VLANs)     :0
Number of RLQ request PDUs received (all VLANs)   :0
Number of RLQ response PDUs received (all VLANs)  :0
Number of RLQ request PDUs sent (all VLANs)       :0
Number of RLQ response PDUs sent (all VLANs)      :0
Router#
```

This example shows how to display information about the spanning tree for a specific VLAN:

```
Router# show spanning-tree vlan 200
VLAN0200
 Spanning tree enabled protocol ieee
 Root ID Priority 32768
    Address 00d0.00b8.14c8
    This bridge is the root
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Bridge ID Priority 32768
    Address 00d0.00b8.14c8
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Aging Time 300
Interface Role Sts Cost Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4 Desg FWD 200000 128.196 P2p
Fa4/5 Back BLK 200000 128.197 P2p
Router#
```

Table 27 describes the fields that are shown in the example.

Table 27 show spanning-tree vlan Command Output Fields

Field	Definition
Role	Current 802.1w role; valid values are Boun (boundary), Desg (designated), Root, Altn (alternate), and Back (backup).
Sts	Spanning-tree states; valid values are BKN* (broken)[1], BLK (blocking), DWN (down), LTN (listening), LBK (loopback), LRN (learning), and FWD (forwarding).
Cost	Port cost.

Table 27 show spanning-tree vlan Command Output Fields (continued)

Field	Definition
Prio.Nbr	Port ID that consists of the port priority and the port number.
Status	Status information; valid values are as follows: • P2p/Shr—The interface is considered as a point-to-point (resp. shared) interface by the spanning tree. • Edge—PortFast has been configured (either globally using the **default** command or directly on the interface) and no BPDU has been received. • *ROOT_Inc, *LOOP_Inc, *PVID_Inc and *TYPE_Inc—The port is in a broken state (BKN*) for an inconsistency. The port would be (respectively) Root inconsistent, Loopguard inconsistent, PVID inconsistent, or Type inconsistent. • Bound(type)—When in MST mode, identifies the boundary ports and specifies the type of the neighbor (STP, RSTP, or PVST). • Peer(STP)—When in PVRST rapid-pvst mode, identifies the port connected to a previous version of the 802.1D bridge.

[1] For information on the *, see the definition for the Status field.

This example shows how to determine if any ports are in the root-inconsistent state:

```
Router#  show spanning-tree inconsistentports

Name                 Interface            Inconsistency
-------------------- -------------------- ------------------
 VLAN1               FastEthernet3/1      Root Inconsistent

Number of inconsistent ports (segments) in the system :1
Router#
```

Related Commands

Command	Description
spanning-tree backbonefast	Enables BackboneFast on all Ethernet VLANs.
spanning-tree cost	Sets the path cost of the interface for STP calculations.
spanning-tree guard	Enables or disables the guard mode.
spanning-tree pathcost method	Sets the default path-cost calculation method.
spanning-tree portfast (interface configuration mode)	Enables PortFast mode.
spanning-tree portfast bpdufilter default	Enables BPDU filtering by default on all PortFast ports.
spanning-tree portfast bpduguard default	Enables BPDU guard by default on all PortFast ports.
spanning-tree port-priority	Sets an interface priority when two bridges vie for position as the root bridge.
spanning-tree uplinkfast	Enables UplinkFast.
spanning-tree vlan	Enables the Spanning Tree Protocol (STP) on a VLAN.

show spantree

To display spanning-tree information for a virtual LAN (VLAN) or port, use the **show spantree** command in privileged EXEC mode.

show spantree [*vlan*] [**active**]

show spantree *mod/port*

Syntax Description

vlan	(Optional) Number of the VLAN; valid values are from 1 to 1001 and from 1025 to 4094.
active	(Optional) Displays only the active ports.
mod/port	Number of the module and the port on the module. The slash mark is required.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify the VLAN number, VLAN 1 is displayed.

If you are in Multiple Instances of Spanning Tree (MISTP) mode, instance information is not displayed.

The maximum length of the channel port list is 47. The space in the Port(s) column might not be enough to display the entire list in one line. If this is the case, the port list is split into multiple lines. For example, in the following display, ports 6/5-8, 6/13, 6/15, 6/17, 6/19 are channeling:

```
.
.
.
Port(s)                  Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
6/5-8,6/13,6/15,6/17,6/1 1    not-connected 2684354   32   disabled 0

9
.
.
.
```

The Link Aggregation Control Protocol (LACP) for channels does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated).

The port is shown as “connected” if you use the **show port** command and as “not connected” if you use the **show spantree** command. This discrepancy occurs because the port is physically connected but never joined the active spanning-tree topology. To get the port to join the active spanning- tree topology, either set the duplex to full or set the channel mode to off for that port.

Examples

The following example shows how to display the active spanning tree port configuration for VLAN 1 while in Per VLAN Spanning Tree (PVST+ mode):

```
Router# (enable) show spantree 1 active

VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-60-70-4c-70-00
Designated Root Priority    16384
Designated Root Cost        19
Designated Root Port        2/3
Root Max Age   14 sec   Hello Time 2  sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-d0-00-4c-18-00
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding           19   32 disabled 0
 2/12                    1    forwarding           19   32 disabled 0
```

The following example shows how to display the active spanning-tree port configuration for VLAN 1 (while in MISTP mode):

```
Router# (enable) show spantree 1 active

VLAN 1
Spanning tree mode          MISTP
Spanning tree type          ieee
Spanning tree enabled
VLAN mapped to MISTP Instance: 1
Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 2/3                     1    forwarding       200000   32 disabled 0
 2/12                    1    forwarding       200000   32 disabled 0
```

Table 28 describes the significant fields shown in the displays.

Table 28 show spantree Field Descriptions

Field	Description
VLAN	VLAN for which the spanning-tree information is shown.
Spanning tree mode	Indicates the current mode that spanning tree is operating in: • PVST—Per VLAN Spanning Tree • MSTP—Multiple Spanning Tree Protocol
Spanning tree type	Indicates the current Spanning Tree Protocol type: • IEEE—IEEE Spanning Tree • DEC—Digital Equipment Corporation Spanning Tree
Spanning tree enabled	Indicates whether Spanning Tree Protocol is enabled or disabled.
Designated Root	MAC address of the designated spanning-tree root bridge.
Designated Root Priority	Priority of the designated root bridge.
Designated Root Cost	Total path cost to reach the root.
Designated Root Port	Port through which the root bridge can be reached. (Shown only on nonroot bridges.)
Root Max Age	Amount of time a bridge packet data unit (BPDU) packet should be considered valid.
Hello Time	Number of times the root bridge sends BPDUs.
Forward Delay	Amount of time the port spends in listening or learning mode.
Port	Port number.
Vlan	VLAN to which the port belongs.
Port-State	Spanning tree port state (disabled, inactive, not-connected, blocking, listening, learning, forwarding, bridging, or type-pvid-inconsistent).
Cost	Cost associated with the port.
Prio	Priority associated with the port.
Portfast	Status of whether the port is configured to use the PortFast feature.
Channel_id	Channel ID number.

Related Commands

Command	Description
show spantree backbonefast	Displays whether the spanning-tree BackboneFast Convergence feature is enabled.
show spantree blockedports	Displays only the blocked ports on a per-VLAN or per-instance basis.
show spantree portvlancost	Shows the path cost for the VLANs or extended-range VLANs.
show spantree statistics	Shows spanning tree statistical information
show spantree summary	Displays a summary of spanning-tree information.
show spantree uplinkfast	Shows the UplinkFast feature settings.

show subscriber-policy

To display the details of a subscriber policy, use the **show subscriber-policy** command in user EXEC or privileged EXEC mode.

show subscriber-policy *range*

Syntax Description

range	Range of subscriber policy numbers (range 1 to 100).

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

The following is sample output from the **show subscriber-policy** command:

```
Router# show subscriber-policy 1

ARP: Permit
Broadcast: Deny
Multicast: Permit
Unknown: Deny
STP: Disable
CDP: Disable
```

Related Commands

Command	Description
bridge protocol	Defines the type of Spanning Tree Protocol.
bridge subscriber-policy	Binds a bridge group with a subscriber policy.
show bridge	Displays classes of entries in the bridge forwarding database.
subscriber-policy	Defines or modifies the forward and filter decisions of the subscriber policy.

source-bridge trcrf-vlan

To attach a VLAN to the Route Switch Module (RSM)'s virtual ring when source-route bridging, use the **source-bridge trcrf-vlan** command in interface configuration mode. To disable the attachment of a VLAN to the RSM's virtual ring, use the **no** form of this command.

source-bridge trcrf-vlan *vlanid* **ring-group** *ringnum*

Syntax Description

vlanid	VLAN ID number.
ring-group *ringnum*	Pseudoring number that corresponds to the virtual ring number for the interface.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **source-bridge ring-group** command to create a virtual ring for source-route bridging (SRB) between Token Ring Bridge Relay Function (TrBRF) VLANs. Use the **source-bridge trcrf-vlan** command to assign a Token Ring Concentrator Relay Function (TrCRF) VLAN ID to the virtual ring.

In SRB and source-route translational bridging (SR/TLB), define a unique TrCRF VLAN ID that corresponds to the virtual ring on the RSM for each TrBRF. Although the VLAN ID for the TrCRF is unique for each TrBRF, the ring number will be the same.

If IP or IPX routing source routing (SR) frames is required on a TrBRF interface configured for SRB, you must also define a pseudoring for this interface with the **multiring trcrf-vlan** command. In this case, the VLAN ID used for the TrCRF that corresponds to the virtual ring can be the same as the one used for the pseudoring. If the VLAN IDs are different, the virtual ring and pseudoring numbers must be different.

Examples

The following example shows both SRB and IP routing for SR frames:

```
source-bridge ring-group 100
interface Token Ring3/1
 source-bridge 10 1 100
 source-bridge spanning
!
```

```
interface vlan999 type trbrf
 source-bridge trcrf-vlan 400 ring-group 100
 source-bridge spanning
 multiring all
 multiring trcrf-vlan 400 ring-group 100
```

Note that the ring number must be the same for the **source-bridge ring-group**, **source-bridge**, and **source-bridge trcrf-vlan** commands. In this example, the ring number of the pseudoring also matches the virtual ring number.

Related Commands

Command	Description
multiring trcrf-vlan	Creates pseudoring on the RSM and terminates the RIF when routing IP or IPX source-routed traffic on Token Ring VLAN (TrBRF) interfaces.
show source-bridge	Displays the current source bridge configuration and miscellaneous statistics.
source-bridge	Configure an interface for SRB.
source-bridge ring-group	Defines or removes a ring group from the configuration.

spanning-tree portfast (interface mode)

To enable PortFast on a specific interface, use the **spanning-tree portfast** command in interface configuration mode. To disable PortFast, use the **no** form of this command.

spanning-tree portfast {**disable** | **trunk**}

no spanning-tree portfast

Syntax Description

disable	Disables PortFast on the interface.
trunk	Enables PortFast on the interface when it is in trunk mode.

Command Default

Portfast on an interface defaults to the state of portfast on the device.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1E	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	Support for the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command only with interfaces that connect to end stations; otherwise, an accidental data-packet loop could form that disrupts operations of both the Cisco 7600 series router and the network.

An interface with PortFast mode enabled moves directly to the spanning-tree forwarding state when linkup occurs. No waiting for the standard forward-time delay is required.

The **spanning-tree portfast** command has four states:

- **spanning-tree portfast**—Enables PortFast unconditionally on the given port.
- **spanning-tree portfast disable**—Explicitly disables PortFast for the given port. The configuration line displays in the running configuration because it is not the default.
- **spanning-tree portfast trunk**—Allows you to configure PortFast on trunk ports. When you enter this command, the port is configured for PortFast even in the access mode.
- **no spanning-tree portfast**—Implicitly enables PortFast if you define the **spanning-tree portfast default** command in global configuration mode and if the port is not a trunk port. If you do not configure PortFast globally, the **no spanning-tree portfast** command is equivalent to the **spanning-tree portfast disable** command.

The **no spanning-tree portfast** command does not disable PortFast if the **spanning-tree portfast default** command is enabled.

Examples

The following example shows how to enable PortFast on an interface:

```
Router(config-if)# spanning-tree portfast
```

Related Commands

Command	Description
show spanning-tree	Displays information about the spanning-tree state.
spanning-tree portfast default	Enables PortFast by default on all access ports.

Appendix: Ethernet Type Codes

Table 29 lists known Ethernet type codes. You can use these type codes in transparent bridging and source-route bridging access lists for filtering frames by protocol type. For configuration information on filtering by protocol type, refer to the following two sections of the *Cisco IOS Bridging and IBM Networking Configuration Guide*:

- "Filtering Transparently Bridged Packets" in the "Configuring Transparent Bridging" chapter
- "Securing the SRB Network" in the "Configuring Source-Route Bridging" chapter

Table 29 Ethernet Type Codes

Hexadecimal	Description (Notes)
0000-05DC	IEEE 802.3 Length Field
0101-01FF	Experimental; for development (conflicts with 802.3 length fields)
0200	Xerox PARC Universal Protocol (PUP) (conflicts with IEEE 802.3 length fields)
0201	Xerox PUP Address Translation (conflicts with IEEE 802.3 length fields)
0400	Nixdorf Computers (Germany)
0600	Xerox XNS IDP
0660-0661	DLOG (Germany)
0800	DOD Internet Protocol (IP) *[1] #[2]
0801	X.75 Internet
0802	NBS Internet
0803	ECMA Internet
0804	CHAOSnet
0805	X.25 Level 3
0806	Address Resolution Protocol (for IP and CHAOS)
0807	XNS Compatibility
081C	Symbolics Private
0888-088A	Xyplex
0900	Ungermann-Bass (UB) Network Debugger
0A00	Xerox IEEE 802.3 PUP
0A01	Xerox IEEE 802.3 PUP Address Translation

Table 29 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
0BAD	Banyan VINES IP
0BAE	Banyan VINES Loopback
0BAF	Banyan VINES Echo
1000	Berkeley trailer negotiation
1001-100F	Berkeley trailer encapsulation for IP
1600	VALID system protocol
4242	PCS Basic Block Protocol
5208	BBN Simnet Private
6000	DEC unassigned
6001	DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
6002	DEC MOP Remote Console
6003	DEC DECnet Phase IV Route
6004	DEC Local Area Transport (LAT)
6005	DEC DECnet Diagnostics
6006	DEC Customer Protocol
6007	DEC Local-Area VAX Cluster (LAVC), SCA
6008	DEC unassigned
6009	DEC unassigned
6010-6014	3Com Corporation
7000	Ungermann-Bass (UB) Download
7001	UB diagnostic/loopback
7002	UB diagnostic/loopback
7020-7029	LRT (England)
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe protocol
8006	Nestar
8008	AT&T
8010	Excelan
8013	Silicon Graphics diagnostic (obsolete)
8014	Silicon Graphics network games (obsolete)
8015	Silicon Graphics reserved type (obsolete)
8016	Silicon Graphics XNS NameServer, bounce server (obsolete)

Table 29 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
8019	Apollo Computers
802E	Tymshare
802F	Tigan, Inc.
8035	Reverse Address Resolution Protocol (RARP) (Stanford)
8036	Aeonic Systems
8038	DEC LANBridge Management
8039-803C	DEC unassigned
803D	DEC Ethernet CSMA/CD Encryption Protocol
803E	DEC unassigned
803F	DEC LAN Traffic Monitor Protocol
8040-8042	DEC unassigned
8044	Planning Research Corporation
8046-8047	AT&T
8049	ExperData (France)
805B	*Versatile Message Translation Protocol*, RFC 1045 (Stanford)
805C	Stanford V Kernel, production
805D	Evans & Sutherland
8060	Little Machines
8062	Counterpoint Computers
8065-8066	University of Massachusetts at Amherst
8067	Veeco Integrated Automation
8068	General Dynamics
8069	AT&T
806A	Autophon (Switzerland)
806C	ComDesign
806D	Compugraphic Corporation
806E-8077	Landmark Graphics Corporation
807A	Matra (France)
807B	Dansk Data Elektronik A/S
807C	University of Michigan
807D-807F	Vitalink Communications
8080	Vitalink TransLAN III Management
8081-8083	Counterpoint Computers
809B	Kinetics EtherTalk (AppleTalk over Ethernet)
809C-809E	Datability
809F	Spider Systems, Ltd.

Table 29 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
80A3	Nixdorf Computers (Germany)
80A4-80B3	Siemens Gammasonics, Inc.
80C0-80C3	Digital Communications Association (DCA), Inc.
80C1	DCA Data Exchange Cluster
80C4	Banyan VINES IP
80C5	Banyan VINES Echo
80C6	Pacer Software
80C7	Applitek Corporation
80C8-80CC	Intergraph Corporation
80CD-80CE	Harris Corporation
80CF-80D2	Taylor Instrument
80D3-80D4	Rosemount Corporation
80D5	IBM SNA Services over Ethernet
80DD	Varian Associates
80DE	Integrated Solutions Transparent Remote File System (TRFS)
80DF	Integrated Solutions
80E0-80E3	Allen-Bradley
80E4-80F0	Datability
80F2	Retix
80F3	Kinetics AppleTalk Address Resolution Protocol (AARP)
80F4-80F5	Kinetics
80F7	Apollo Computer
80FF-8103	Wellfleet Communications
8107-8109	Symbolics Private
8130	Hayes Microcomputer Products, Ltd. (formerly Waterloo Microsystems, Inc.)
8131	VG Laboratory Systems
8132-8136	Bridge Communications, Inc.
8137	Novell NetWare IPX (old)
8137-8138	Novell, Inc.
8139-813D	KTI
8148	Logicraft, Inc.
8149	Network Computing Devices
814A	Alpha Micro
814C	SNMP
814D-814E	BIIN
814F	Technically Elite Concepts, Inc.

Table 29 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
8150	Rational Corporation
8151-8153	Qualcomm, Inc.
815C-815E	Computer Protocol Pty, Ltd.
8164-8166	Charles River Data Systems, Inc.
817D-818C	Protocol Engines, Inc.
818D	Motorola Computer X
819A-81A3	Qualcomm, Inc.
81A4	ARAI Bunkichi
81A5-81AE	RAD Network Devices
81B7-81B9	Xyplex
81CC-81D5	Apricot Computers
81D6-81DD	Artisoft, Inc.
81DE-81E0	Hewlett Packard
81E6-81EF	Polygon, Inc.
81F0-81F2	Comsat Laboratories
81F3-81F5	Science Applications International Corporation (SAIC)
81F6-81F8	VG Analytical, Ltd.
8203-8205	Quantum Software Systems, Ltd.
8221-8222	Ascom Banking Systems, Ltd.
823E-8240	Advanced Encryption Systems, Inc.
827F-8282	Athena Programming, Inc.
8263-826A	Charles River Data Systems
829A-829B	Institute for Industrial Information Technology, Ltd.
829C-82AB	Taurus Controls, Inc.
82AC-838F	Walker Richer & Quinn, Inc.
8390	LANSoft, Inc.
8391-8693	Walker Richer & Quinn, Inc.
8694-869D	Idea Courier
869E-86A1	Computer Network Technology Corporation
86A3-86AC	Gateway Communications, Inc.
86DB	SECTRA - Secure Transmission AB
86DE	Delta Controls, Inc.
86DF	USC-ISI
86E0-86EF	Landis & Gyr Powers, Inc.
8700-8710	Motorola, Inc.
8711-8720	Cray Communications

Table 29 Ethernet Type Codes (continued)

Hexadecimal	Description (Notes)
8725-8728	Phoenix Microsystems
8739-873C	Control Technology, Inc.
8755-8759	LANSoft, Inc.
875A-875C	Norland
875D-8766	University of Utah Dept./Computer Science
8780-8785	Symbol Technologies, Inc.
8A96-8A97	Invisible Software
9000	Loopback (Configuration Test Protocol)
9001	3Com (Bridge) XNS Systems Management
9002	3Com (Bridge) TCP/IP Systems Management
9003	3Com (Bridge) loop detect
FF00	BBN VITAL LANBridge cache wakeups
FF00-FF0F	ISC-Bunker Ramo

1. An asterisk (*) indicates the current connection in various informational displays.
2. A pound sign (#) is a delimiting character for configuration commands that contain arbitrary text strings.