

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	<i>bridge-group</i>	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

<i>bridge-group</i>	(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.
<i>group-address</i>	(Optional) Multicast IP address associated with a specific multicast group.
<i>interface-unit</i>	(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

<i>circuit-id</i>	(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	<i>multicast-ip-address</i>	(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		
	<i>vlanid</i>	Number identifying the VLAN.
	bridge-num <i>bridge-number</i>	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 12 shows the actual OUI codes used, when they are used, and how they compare to Software Release 9.0-equivalent commands.

Table 12 Bridge OUI Codes

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

Table 12 Bridge OUI Codes (continued)

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

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

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

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

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

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

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

Examples

The following example specifies standard OUI form:

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

Related Commands

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

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	<i>dlci</i>	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	<p>Bridging over a Frame Relay network is supported on networks that do and do not support a multicast facility.</p> <p>The following example allows bridging over a Frame Relay network:</p> <pre>frame-relay map bridge 144 broadcast</pre>	
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

<i>bridge-group</i>	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

<i>vlanid</i>	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.

Inm alternate



Note

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

To specify the threshold reporting link number, use the **Inm 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.

Inm alternate *number*

no Inm alternate

Syntax Description

<i>number</i>	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.

Inm 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.

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

Inm disabled



Note

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

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

inm disabled

no inm 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 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 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 inm rem** and **no inm rps** commands.

Examples

The following example disables LNM functionality:

```
inm disabled
```

Related Commands

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

Inm express-buffer



Note

Effective with Cisco IOS Release 12.3(4)T, the **Inm 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 **Inm express-buffer** command in interface configuration mode. To disable this function, use the **no** form of this command.

Inm express-buffer

no Inm 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:

```
Inm 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
```

Inm password



Note

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

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

inm password *number string*

no inm password *number*

Syntax Description

<i>number</i>	Number of the reporting link to which to apply the password. This value must be in the range from 0 to 3.
<i>string</i>	Password you enter at the keyboard. In order to maintain compatibility with LAN Network Manager (LNM), the parameter <i>string</i> 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.

Inm pathtrace-disabled



Note

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

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

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

no Inm 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 **Inm 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:

```
Inm pathtrace-disabled
```

Related Commands

Command	Description
Inm disabled	Disables LNM functionality.

Inm rem



Note

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

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

inm rem

no inm 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 **inm rem** command:

```
interface tokenring 0
  inm rem
```

Related Commands

Command	Description
inm crs	Monitors the current logical configuration of a Token Ring.
inm 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.

Inm snmp-only



Note

Effective with Cisco IOS Release 12.3(4)T, the **Inm 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 **Inm snmp-only** command in global configuration mode. To allow modifications, use the **no** form of this command.

Inm snmp-only

no Inm 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:

```
Inm snmp-only
```

Inm softerr



Note

Effective with Cisco IOS Release 12.3(4)T, the **Inm 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 **Inm softerr** command in interface configuration mode. To return to the default value, use the **no** form of this command.

Inm softerr *ten-milliseconds*

no Inm softerr

Syntax Description

<i>ten-milliseconds</i>	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:

```
Inm softerr 500
```

Related Commands

Command	Description
Inm 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

<i>ieee-address</i>	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

<i>protocol</i>	Specifies a protocol. The following protocols are supported: <ul style="list-style-type: none"> • 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 <i>all</i> frames.
other	Enables the multiring for <i>any</i> 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: <ul style="list-style-type: none"> • all-routes • spanning
12.2(13)T	The following values for the <i>protocol</i> argument were removed: <ul style="list-style-type: none"> • 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

<i>vlanid</i>	VLAN ID number. Valid VLAN ID numbers are 2 through 1000.
ring-group <i>ring-number</i>	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

<i>name</i>	Name of the access list being defined.
permit	Permits the condition.
deny	Denies the condition.
<i>offset</i>	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.
<i>pattern</i>	Hexadecimal string of digits representing a byte pattern. The <i>pattern</i> 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

<i>name</i>	Name of the access list being defined.
permit	Permits the condition.
deny	Denies the condition.
<i>pattern</i>	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 13 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 13](#) explains the pattern-matching characters that can be used.

Table 13 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	<i>name</i>	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 <i>marketing</i> 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	<i>name</i>	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	<p>The following example filters packets coming into Token Ring interface 1 using the NetBIOS access list named <i>marketing</i>:</p> <pre>interface tokenring 1 netbios access-list host marketing permit W?Y? netbios input-access-filter host marketing</pre>	
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

<i>mac-address</i>	The MAC address.
<i>netbios-name</i>	Server name linked to the MAC address.
<i>interface-name</i>	Name of the interface by which the server is accessible locally.
<i>interface-umber</i>	Number of the interface by which the server is accessible locally.
ring-group	Specifies that the link is accessible remotely.
<i>group-number</i>	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
<code>show netbios-cache</code>	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	<i>length</i>	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

<i>seconds</i>	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	<i>seconds</i>	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: <pre>netbios name-cache query-timeout 15</pre>	
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	<i>minutes</i>	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

<i>name</i>	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.