

# 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 <b>bridge protocol</b> command.
--------------------	---------------------	--

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	10.0	This command was introduced.

Examples	The following example shows the use of the <b>clear bridge</b> command:
----------	---

```
Router# clear bridge 1
```

Related Commands	Command	Description
	<b>bridge address</b>	Filters frames with a particular MAC-layer station source or destination address.
	<b>bridge protocol</b>	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 <b>bridge protocol</b> command.
<b>router-ports</b>	(Optional)	Clear multicast router ports.
<b>groups</b>	(Optional)	Clear multicast groups.
<b>counts</b>	(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.

**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
	<b>bridge cmf</b>	Enables CMF for all configured bridge groups.
	<b>show bridge multicast</b>	Displays transparent bridging multicast state information.

# 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.

**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
	<b>interface vlan</b>	Configures a Token Ring or Ethernet interface on the RSM.
	<b>show drip</b>	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.

**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
	<b>netbios enable-name-cache</b>	Enables NetBIOS name caching.
	<b>netbios name-cache timeout</b>	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.
	<b>show netbios-cache</b>	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.

**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
	<b>rif</b>	Enters static source-route information into the RIF cache.
	<b>rif timeout</b>	Determines the number of minutes an inactive RIF entry is kept. RIF information is maintained in a cache whose entries are aged.
	<b>show rif</b>	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.

**Examples** The following example clears the source-bridge statistical counters:

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

Related Commands	Command	Description
	<b>clear bridge</b>	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

---

Release	Modification
10.3	This command was introduced.

---

---

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

---

**Examples** The following example re initializes the SSP:

```
Router# clear sse
```

# clear vlan statistics

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

## clear vlan statistics

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.

**Examples** The following example clears VLAN statistics:

```
Router# clear vlan statistics
```

# 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.
	<b>bridge-num</b> <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.

**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
	<b>clear drip counters</b>	Clears DRiP counters.
	<b>clear vlan statistics</b>	Removes virtual LAN statistics from any statically or system configured entries.
	<b>multiring</b>	Enables collection and use of RIF information.
	<b>multiring trcrf-vlan</b>	Creates a pseudo ring to terminate the RIF for source-routed traffic and assigns it to a VLAN.
	<b>show drip</b>	Displays the status of the DRiP database.
	<b>show vlans</b>	Displays virtual LAN subinterfaces.
	<b>source-bridge trcrf-vlan</b>	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. Various versions of this OUI code are used by Ethernet/Token Ring translational bridges. To return the default OUI code, use the **no** form of this command.

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

**no ethernet-transit-oui**

Syntax Description	<b>90-compatible</b>	(Optional) Default OUI form.
	<b>standard</b>	(Optional) Standard OUI form.
	<b>cisco</b>	(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.

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

The **standard** keyword is used when you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity.

[Table 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
<b>90-compatible</b>	0000F8	By default, when talking to other Cisco routers. Provides the most flexibility.	<b>no bridge old-oui</b>
<b>cisco</b>	00000C	Provided for compatibility with future equipment.	None
<b>standard</b>	000000	When talking to IBM 8209 bridges and other vendor equipment. Does not provide for as much flexibility as the other two choices.	<b>bridge old-oui</b>

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
<b>source-bridge transparent</b>	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 *dci* broadcast**

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

<b>Syntax Description</b>	<i>dci</i>	Data Link Connection Identifier (DLCI) number. The valid range is from 16 to 1007.
---------------------------	------------	--

<b>Defaults</b>	No mapping entry is established.
-----------------	----------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>encapsulation frame-relay</b>	Enables Frame Relay encapsulation.

# hsma control-sap

To override the default control service access point (SAP) for (hot standby MAC address) HSMA peer communications, use the **hsma control-sap** command in control adapter configuration mode. To restore the default SAP for peer communications, use the **no** form of this command.

**hsma control-sap** *sap-address*

**no hsma control-sap** *sap-address*

<b>Syntax Description</b>	<i>sap-address</i>	SAP address used by the HSMA protocol on the control adapter. This is a hexadecimal value. The allowed range is from 0x4 to 0xFC, and the default is 0xEC.
---------------------------	--------------------	--

<b>Defaults</b>	The default SAP address, 0xEC, is used.
-----------------	---

<b>Command Modes</b>	Control adapter configuration
----------------------	-------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(3)	This command was introduced.

<b>Usage Guidelines</b>	This command allows you to override the default control SAP used for HSMA peer communications. The same value must be configured for both HSMA peers or they will not be able to communicate. This command is valid only on the control adapter.
-------------------------	--

When the **hsma control-sap** command is changed, it will take effect only after you restart the interface by using the **shutdown** and **no shutdown** commands.

<b>Examples</b>	The following example configures the SAP address E8 on control adapter 26:
-----------------	--

```
interface Channel3/0
  csna 0190 09
  lan TokenRing 23
  source-bridge 330 3 100
  adapter 9 4043.1313.9009 hsma-partner 4043.1111.001a
  lan TokenRing 31
  source-bridge 339 9 100
  adapter 26 4043.3333.001a
  hsma enable
  hsma control-sap E8
```

# hsma dead-interval

To configure the time interval during which at least one hello packet must be received from the peer (hot standby MAC address) HSMA adapter or else the router declares that neighbor down, use the **hsma dead-interval** command in peered adapter configuration mode. To restore the default value, use the **no** form of this command.

**hsma dead-interval** *time-interval*

**no hsma dead-interval** *time-interval*

<b>Syntax Description</b>	<i>time-interval</i>	Time interval used by the HSMA protocol between the control and peered HSMA adapters. Range: 3 to 180. Default: 10.
---------------------------	----------------------	---

<b>Defaults</b>	The time interval is set to the default value of 10 seconds.
-----------------	--

<b>Command Modes</b>	Peered adapter configuration
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(3)	This command was introduced.

<b>Examples</b>	The following example configures the time interval on adapter 26 to be 8 seconds:
-----------------	---

```
interface Channell1/0
 load-interval 30
 csna 0190 09
 lan TokenRing 20
  source-bridge 310 3 100
  adapter 9 4043.1313.9009 hsma-partner 4043.3333.001a
   hsma dead-interval 8
 lan TokenRing 26
  source-bridge 319 9 100
  adapter 26 4043.1111.001a
   hsma enable
```

# hsma enable

To enable (hot standby MAC address) HSMA on an adapter, use the **hsma enable** command in control adapter configuration mode. To disable HSMA, use the **no** form of this command.

**hsma enable**

**no hsma enable**

---

**Syntax Description** This command has no keywords or arguments.

---

**Defaults** HSMA is disabled.

---

**Command Modes** Control adapter configuration

---

Command History	Release	Modification
	12.3(3)	This command was introduced.

---



---

**Usage Guidelines** The **hsma enable** command instructs HSMA to use the adapter it is configured on as the control adapter. The control adapter is the adapter that is used to send and receive hello updates. HSMA is not enabled on the router until a control adapter is specified by the **hsma enable** command. The **no** form of this command is not valid unless all of the HSMA partners have been removed; similarly, the adapter context itself may not be removed unless all of the HSMA partners have been removed.

This command is only valid on the control adapter.

The control adapter can be configured under any LAN Token Ring adapter.

---

**Examples** The following example enables HSMA on control adapter 26:

```
interface Channell/0
  lan TokenRing 20
    source-bridge 310 3 100
    adapter 9 4043.1313.9009 hsma-partner 4043.3333.001a
  lan TokenRing 26
    source-bridge 319 9 100
    adapter 26 4043.1111.001a
    hsma enable
```

# hsma hello-interval

To configure the time interval between hello messages between the peered (hot standby MAC address) HSMA Cisco Channel Interface Processors (CIPs) or Channel Port Adapters (CPAs), use the **hsma hello-interval** command in peered adapter configuration mode. To restore the default value, use the **no** form of this command.

**hsma hello-interval** *time-interval*

**no hsma hello-interval** *time-interval*

## Syntax Description

*time-interval* Time interval, in seconds, used by the HSMA protocol between the peered HSMA CIP or CPAs. Range: 1 to 60. Default: 3.

## Defaults

The time interval is set to the default value of 3 seconds.

## Command Modes

Peered adapter configuration

## Command History

Release	Modification
12.3(3)	This command was introduced.

## Usage Guidelines

The **hsma hello-interval** is the time interval between hello messages that pass between the peered HSMA CIP or CPAs. The control adapter in the enabled mode sends hello messages to the peered adapter after every 2 seconds.

## Examples

The following example configures the interval between hello messages on adapter 26 to be 2 seconds:

```
interface Channell1/0
  csna 0190 09
  lan TokenRing 20
  source-bridge 310 3 100
  adapter 9 4043.1313.9009 hsma-partner 4043.3333.001a
    hsma hello-interval 2
    lan TokenRing 26
  source-bridge 319 9 100
  adapter 26 4043.1111.001a
    hsma enable
```

# hsma preferred

To assign priority to a peer as a control adapter, use the **hsma preferred** command in peered adapter configuration mode. To allow priority to be set without configuring a peer, use the **no** form of this command.

**hsma preferred**

**no hsma preferred**

---

**Syntax Description** This command has no keywords or arguments.

---

**Defaults** Disabled

---

**Command Modes** Peered adapter configuration

---

Command History	Release	Modification
	12.3(3)	This command was introduced.

---



---

**Usage Guidelines** The **hsma preferred** command is used in situations when both HSMA peers are becoming active at the same time or both were active because of an interruption of communication between the control adapters. In such situations, the adapter with the **hsma preferred** command configured becomes the active adapter, and the other adapter is disabled. Sessions that are connected to the disabled adapter will be dropped. If the **hsma preferred** command is not configured on either peer, the control adapter with the higher MAC address is used.

---

**Examples** The following example disables adapter 9 as the HSMA adapter and enables adapter 26 as the active HSMA adapter:

```
interface Channel1/0
  csna 0190 09
  lan TokenRing 20
    source-bridge 310 3 100
    adapter 9 4043.1313.9009 hsma-partner 4043.3333.001a
      hsma preferred
      hsma shutdown
  lan TokenRing 26
    source-bridge 319 9 100
    adapter 26 4043.1111.001a
      hsma enable
```

# hsma shutdown

To stop (hot standby MAC address) HSMA on an adapter and hence enable the partner adapter, use the **hsma shutdown** command. To restart the HSMA adapter, use the **no** form of this command.

**hsma shutdown**

**no hsma shutdown**

---

**Syntax Description** This command has no keywords or arguments.

---

**Defaults** HSMA is not shut down.

---

**Command Modes** Peered adapter configuration

---

Command History	Release	Modification
	12.3(3)	This command was introduced.

---



---

**Usage Guidelines** Use the **hsma shutdown** command when you wish to force the other adapter of a pair to become active.

---

**Examples** The following example disables adapter 9 as the HSMA adapter and enables adapter 26 as the active HSMA adapter:

```
interface Channell1/0
  csna 0190 09
  lan TokenRing 20
  source-bridge 310 3 100
  adapter 9 4043.1313.9009 hsma-partner 4043.3333.001a
    hsma preferred
    hsma shutdown
  lan TokenRing 26
  source-bridge 319 9 100
  adapter 26 4043.1111.001a
    hsma enable
```

# 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 interface configuration mode. To delete the BVI, use the **no** form of this command.

```
interface bvi bridge-group
```

```
no interface bvi bridge-group
```

<b>Syntax Description</b>	<i>bridge-group</i>	Bridge group number specified in the <b>bridge protocol</b> command.
---------------------------	---------------------	--

<b>Defaults</b>	No BVI is created.
-----------------	--------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.2	This command was introduced.

<b>Usage Guidelines</b>	<p>You must enable integrated routing and bridging (IRB) before attempting to create a BVI.</p> <p>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.</p>
-------------------------	--

<b>Examples</b>	<p>The following example creates a bridge group virtual interface and associates it with bridge group 1:</p> <pre>interface bvi 1</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>bridge irb</b>	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 the Route Switch Module (RSM), use the **interface vlan** command in interface configuration mode.

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

Syntax Description		
	<i>vlanid</i>	Unique VLAN ID number used to create a VLAN.
	<b>type trbrf</b>	Configures a Token Ring interface on the RSM.
	<b>type ethernet</b>	Configures an Ethernet interface on the RSM.

**Defaults** The RSM interfaces are not configured.

**Command Modes** Interface configuration

Command History	Release	Modification
	11.3(5)T	This command was introduced.

**Usage Guidelines** 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.

**Examples** The following example configures an RSM Token Ring interface with VLAN 998:

```
interface vlan 998 type trbrf
 ip address 10.5.5.1 255.255.255.0
```

Related Commands	Command	Description
	<b>clear drip counters</b>	Clears DRiP counters.
	<b>multiring trcrf-vlan</b>	Creates a pseudoring to terminate the RIF for source-routed traffic and assigns it to a VLAN.
	<b>source-bridge trcrf-vlan</b>	Attaches a TrCRF VLAN to the virtual ring of the router.
	<b>show drip</b>	Displays the status of the DRiP database.

# Inm alternate

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**

<b>Syntax Description</b>	<i>number</i>	Threshold reporting link number. It must be in the range from 0 to 3.
---------------------------	---------------	---

<b>Defaults</b>	The default threshold reporting link number is 0.
-----------------	---

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	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.

<b>Examples</b>	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
inm 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  
Inm alternate 3
```

---

**Related Commands**

Command	Description
<b>Inm password</b>	Sets the password for the reporting link.

# Inm crs

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 lnm crs** 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.

**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
	<b>lnm rem</b>	Monitors errors reported by any station on the ring.
	<b>lnm rps</b>	Ensures that all stations on a ring are using a consistent set of reporting parameters.

# Inm disabled

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.

**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
	<b>inm pathtrace-disabled</b>	Disables pathtrace reporting to LNM stations.
	<b>inm rem</b>	Monitors errors reported by any station on the ring.
	<b>inm rps</b>	Ensures that all stations on a ring are using a consistent set of reporting parameters.
	<b>inm snmp-only</b>	Prevents any LNM stations from modifying parameters in the Cisco IOS software.
	<b>show inm bridge</b>	Displays all currently configured bridges and all parameters that are related to the bridge as a whole, not to one of its interfaces.

# Inm express-buffer

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.

**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
```

# Inm loss-threshold

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 **inm loss-threshold** command in interface configuration mode. To return to the default value, use the **no** form of this command.

**inm loss-threshold** *number*

**no inm loss-threshold**

<b>Syntax Description</b>	<i>number</i>	Single number expressing the percentage loss rate in hundredths of a percent. The valid range is from 0 to 9999. The default is
---------------------------	---------------	---

<b>Defaults</b>	10 (0.10 percent)
-----------------	-------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	<p>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.</p> <p>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.</p>
-------------------------	---

<b>Examples</b>	In the following example, the loss threshold is set to 0.02 percent:
-----------------	--

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

# Inm password

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.

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

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

Characters allowable in the *string* are the following:

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

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



## Note

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

---

**Examples**

In the following example, the password Zephyr@ is assigned to reporting link 2:

```
! provide appropriate global configuration command if not currently in your config.  
!  
Inm password 2 Zephyr@
```

---

**Related Commands**

Command	Description
<b>Inm alternate</b>	Specifies the threshold reporting link number. In order for an LRM to change parameters, it must be attached to the reporting link with the lowest reporting link number, and that reporting link number must be lower than this threshold reporting link number.

# Inm pathtrace-disabled

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.
	<b>origin</b>	(Optional) Disable pathtrace reporting to originating stations only.

Defaults	Enabled
----------	---------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	11.2	This command was introduced.

**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
	<b>inm disabled</b>	Disables LNM functionality.
	<b>show inm bridge</b>	Displays all currently configured bridges and all parameters that are related to the bridge as a whole, not to one of its interfaces.

# Inm rem

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

---

Release	Modification
10.0	This command was introduced.

---



---

**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
```

---

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

---

# lnm rps

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.

**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
	<b>lnm crs</b>	Monitors the current logical configuration of a Token Ring.
	<b>lnm rem</b>	Monitors errors reported by any station on the ring.

# Inm snmp-only

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

---

Release	Modification
10.0	This command was introduced.

---



---

**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

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-illiseconds*

**no inm softerr**

<b>Syntax Description</b>	<i>ten-milliseconds</i>	Time interval in tens of milliseconds between error messages. The valid range is from 0 to 65535.
---------------------------	-------------------------	---

<b>Defaults</b>	200 ms (2 seconds)
-----------------	--------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	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.
-------------------------	--

<b>Examples</b>	The following example changes the error-reporting frequency to once every 5 seconds:
-----------------	--

```
inm softerr 500
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>inm rem</b>	Monitors errors reported by any station on the ring.

# mac-address

To set the MAC layer address of the Cisco Token Ring, use the **mac-address** command in interface configuration mode. To return to the default value, use the **no** form of this command.

**mac-address** *ieee-address*

**no mac-address** *ieee-address*

<b>Syntax Description</b>	<i>ieee-address</i>	48-bit IEEE MAC address written as a dotted triple of four-digit hexadecimal numbers.
---------------------------	---------------------	---

<b>Defaults</b>	No MAC layer address is set.
-----------------	------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th style="border-right: none;">Release</th> <th style="border-left: none;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-right: none;">10.0</td> <td style="border-left: none;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.0	This command was introduced.
Release	Modification				
10.0	This command was introduced.				

**Usage Guidelines**

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
```

# 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"> <li>• <b>appletalk</b>—AppleTalk Phase 1 and 2</li> <li>• <b>clns</b>—ISO CLNS</li> <li>• <b>decnet</b>—DECnet Phase IV</li> <li>• <b>ip</b>—IP</li> <li>• <b>ipx</b>—Novell IPX</li> </ul>
	<b>all-routes</b>	(Optional) Uses all-routes explorers.
	<b>spanning</b>	(Optional) Uses spanning-tree explorers.
	<b>all</b>	Enables the multiring for <i>all</i> frames.
	<b>other</b>	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"> <li>• <b>all-routes</b></li> <li>• <b>spanning</b></li> </ul>
	12.2(13)T	The following values for the <i>protocol</i> argument were removed: <ul style="list-style-type: none"> <li>• <b>apollo</b></li> <li>• <b>vines</b></li> <li>• <b>xns</b></li> </ul>

**Usage Guidelines**

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



**Note**

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

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

**Examples**

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

```
! commands that follow apply to interface token 0
interface tokenring 0
! enable the Token Ring interface for IP
ip address 131.108.183.37 255.255.255.0
! generate RIFs for IP frames
multiring ip
! enable the Token Ring interface for Novell IPX
novell network 33
```

**Related Commands**

Command	Description
<b>clear rif-cache</b>	Clears the entire RIF cache.
<b>rif</b>	Enters static source-route information into the RIF cache.
<b>rif timeout</b>	Determines the number of minutes an inactive RIF entry is kept.
<b>show rif</b>	Displays the current contents of the RIF cache.
<b>xns encapsulation</b>	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.
<b>ring-group</b> <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.

**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 4.4.4.1 255.255.255.0
```

```
!
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**

<b>Command</b>	<b>Description</b>
<b>clear drip counters</b>	Clears DRiP counters.
<b>interface vlan</b>	Configures a Token Ring or Ethernet interface on the RSM.
<b>multiring</b>	Enables collection and use of RIF information.
<b>rif</b>	Enters static source-route information into the RIF cache.
<b>show drip</b>	Displays the status of the DRiP database.
<b>show rif</b>	Displays the current contents of the RIF cache.
<b>source-bridge</b>	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.
<b>permit</b>	Permits the condition.
<b>deny</b>	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.

## 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
<b>netbios input-access-filter bytes</b>	Defines a byte access list filter on incoming messages. T
<b>netbios output-access-filter bytes</b>	Defines a byte access list filter on outgoing messages.

## netbios access-list host

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

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

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

<b>Syntax Description</b>	<i>name</i>	Name of the access list being defined.
	<b>permit</b>	Permits the condition.
	<b>deny</b>	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. <a href="#">Table 6</a> in the “Usage Guidelines” section explains the pattern-matching symbols that can be used.

**Defaults** No access list is assigned.

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**Usage Guidelines** [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
<b>netbios input-access-filter host</b>	Defines a station access list filter on incoming messages.
<b>netbios output-access-filter host</b>	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.

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

# netbios input-access-filter bytes

To define a byte access list filter on incoming messages, use the **netbios input-access-filter bytes** command in interface configuration mode. The actual access filter byte offsets and patterns used are defined in one or more **netbios-access-list bytes** commands. To remove the entire access list, use the **no** form of this command with the appropriate name.

**netbios input-access-filter bytes** *name*

**no netbios input-access-filter bytes** *name*

<b>Syntax Description</b>	<i>name</i>	Name of a NetBIOS access filter previously defined with one or more of the <b>netbios access-list bytes</b> global configuration commands.
---------------------------	-------------	--

<b>Defaults</b>	No access list is defined.
-----------------	----------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>netbios access-list bytes</b>	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*

<b>Syntax Description</b>	<i>name</i>	Name of a NetBIOS access filter previously defined with one or more of the <b>netbios access-list host</b> global configuration commands.						
<b>Defaults</b>	No access list is defined.							
<b>Command Modes</b>	Interface configuration							
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.0	This command was introduced.			
Release	Modification							
10.0	This command was introduced.							
<b>Usage Guidelines</b>	The access lists of station names are defined in <b>netbios access-list host</b> commands.							
<b>Examples</b>	<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>							
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>netbios access-list host</b></td> <td>Assigns the name of the access list to a station or set of stations on the network.</td> </tr> <tr> <td><b>netbios output-access-filter host</b></td> <td>Defines a station access list filter on outgoing messages.</td> </tr> </tbody> </table>	Command	Description	<b>netbios access-list host</b>	Assigns the name of the access list to a station or set of stations on the network.	<b>netbios output-access-filter host</b>	Defines a station access list filter on outgoing messages.	
Command	Description							
<b>netbios access-list host</b>	Assigns the name of the access list to a station or set of stations on the network.							
<b>netbios output-access-filter host</b>	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.
<b>ring-group</b>	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 <b>source-bridge ring-group</b> 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.

## 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
<b>show netbios-cache</b>	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*

<b>Syntax Description</b>	<i>length</i>	Length of the NetBIOS type name. The range is from 8 to 16 characters.
---------------------------	---------------	--

<b>Defaults</b>	15 characters
-----------------	---------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	Release	Modification
	10.0	This command was introduced.

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

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

<b>Related Commands</b>	Command	Description
	<b>netbios enable-name-cache</b>	Enables NetBIOS name caching.
	<b>netbios name-cache</b>	Defines a static NetBIOS name cache entry.
	<b>netbios name-cache proxy-datagram</b>	Enables the Cisco IOS software to act as a proxy and send NetBIOS datagram type frames.
	<b>netbios name-cache query-timeout</b>	Specifies the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process.

Command	Description
<b>netbios name-cache recognized-timeout</b>	Specifies the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is only effective at the time of the login negotiation process.
<b>netbios name-cache timeout</b>	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.

## 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
<b>netbios enable-name-cache</b>	Enables NetBIOS name caching.
<b>netbios name-cache</b>	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.
<b>netbios name-cache query-timeout</b>	Specifies the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process.

Command	Description
<b>netbios name-cache recognized-timeout</b>	Specifies the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is only effective at the time of the login negotiation process.
<b>netbios name-cache timeout</b>	Enables NetBIOS name caching and sets the time that entries can remain in the NetBIOS name cache.

# netbios name-cache query-timeout

To specify the “dead” time, in seconds, that starts when a host sends any ADD\_NAME\_QUERY, ADD\_GROUP\_NAME, or STATUS\_QUERY frame, use the **netbios name-cache query-timeout** command in global configuration mode. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD\_NAME\_QUERY, ADD\_GROUP\_NAME, or STATUS\_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process. To restore the default of 6 seconds, use the **no** form of this command.

**netbios name-cache query-timeout** *seconds*

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

<b>Syntax Description</b>	<i>seconds</i>	Dead time period in seconds. Default is 6 seconds.
<b>Defaults</b>	6 seconds	
<b>Command Modes</b>	Global configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
<b>Examples</b>	The following example sets the timeout to 15 seconds: <pre>netbios name-cache query-timeout 15</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>netbios name-cache recognized-timeout</b>	Specifies the “dead” time, in seconds, that starts when a host sends any FIND_NAME or NAME_RECOGNIZED frame. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND_NAME or NAME_RECOGNIZED frame sent by the same host. This timeout is only effective at the time of the login negotiation process.

# netbios name-cache recognized-timeout

To specify the “dead” time, in seconds, that starts when a host sends any FIND\_NAME or NAME\_RECOGNIZED frame, use the **netbios name-cache recognized-timeout** command in global configuration mode. During this dead time, the Cisco IOS software drops any repeat, duplicate FIND\_NAME or NAME\_RECOGNIZED frame sent by the same host. This timeout is effective only at the time of the login negotiation process. To restore the default of 6 seconds, use the **no** form of this command.

**netbios name-cache recognized-timeout** *seconds*

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

<b>Syntax Description</b>	<i>seconds</i>	Dead time period in seconds. Default is 6 seconds.
---------------------------	----------------	--

<b>Defaults</b>	6 seconds
-----------------	-----------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	Release	Modification
	10.0	This command was introduced.

**Examples**

The following example sets the timeout to 15 seconds:

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

<b>Related Commands</b>	Command	Description
	<b>netbios name-cache query-timeout</b>	Specifies the “dead” time, in seconds, that starts when a host sends any ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame. During this dead time, the Cisco IOS software drops any repeat, duplicate ADD_NAME_QUERY, ADD_GROUP_NAME, or STATUS_QUERY frame sent by the same host. This timeout is only effective at the time of the login negotiation process.

# netbios name-cache timeout

To enable NetBIOS name caching and to set the time that entries can remain in the NetBIOS name cache, use the **netbios name-cache timeout** command in global configuration mode. To restore the default of 15 minutes, use the **no** form of this command.

**netbios name-cache timeout** *minutes*

**no netbios name-cache timeout** *minutes*

<b>Syntax Description</b>	<i>minutes</i>	Time, in minutes, that entries can remain in the NetBIOS name cache. Default is 15 minutes.
---------------------------	----------------	---

<b>Defaults</b>	15 minutes
-----------------	------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	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.
-------------------------	--

<b>Examples</b>	The following example sets the timeout to 10 minutes:
-----------------	---

```
interface tokenring 0
 netbios name-cache timeout 10
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show netbios-cache</b>	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*

<b>Syntax Description</b>	<i>name</i>	Name of a NetBIOS access filter previously defined with one or more of the <b>netbios access-list bytes</b> global configuration commands.
<b>Defaults</b>	No access list is defined.	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
<b>Examples</b>	<p>The following example filters packets leaving Token Ring interface 1 using the NetBIOS access list named engineering:</p> <pre>interface tokenring 1  netbios access-list bytes engineering permit 3 0xabcd  netbios output-access-filter bytes engineering</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>netbios access-list bytes</b>	Defines the offset and hexadecimal patterns with which to match byte offsets in NetBIOS packets.
	<b>netbios input-access-filter bytes</b>	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

<i>name</i>	Name of a NetBIOS access filter previously defined with one or more of the <b>netbios access-list host</b> global configuration commands.
-------------	---

## Defaults

No access list filter is defined.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.0	This command was introduced.

## 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
<b>netbios access-list host</b>	Assigns the name of the access list to a station or set of stations on the network.
<b>netbios input-access-filter host</b>	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. If a Token Ring host does not support the use of IEEE 802.2 TEST or XID datagrams as explorer packets, you may need to add static information to the RIF cache of the router. To remove an entry from the cache, use the **no** form of this command.

```
rif mac-address rif-string {interface-name | ring-group ring}
```

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

Syntax Description		
<i>mac-address</i>		12-digit hexadecimal string written as a dotted triple of four-digit hexadecimal numbers; for example, 0010.0a00.20a6.
<i>rif-string</i>		Series of 4-digit hexadecimal numbers separated by a period (.). This RIF string is inserted into the packets sent to the specified MAC address.
<i>interface-name</i>		Interface name (for example, tokenring 0) that indicates the origin of the RIF.
<b>ring-group</b>		Specifies the origin of the RIF is a ring group.
<i>ring</i>		Ring group number that indicates the origin of the RIF. This ring group number must match the number you have specified with the <b>source-bridge ring-group</b> command. The valid range is from 1 to 4095.

**Defaults** No static source-route information is entered.

**Command Modes** Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

**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
<b>multiring</b>	Enables collection and use of RIF information.
<b>source-bridge ring-group</b>	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**

<b>Syntax Description</b>	<i>minutes</i>	Number of minutes an inactive RIF entry is kept. The value must be greater than 0. Default is 15 minutes.
---------------------------	----------------	---

<b>Defaults</b>	15 minutes
-----------------	------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	<p>A RIF entry is cached based on the MAC address and the interface.</p> <p>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.</p> <p>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.</p>
-------------------------	---

<b>Examples</b>	The following example changes the timeout period to 5 minutes:
-----------------	--

```
rif timeout 5
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear rif-cache</b>	Clears the entire RIF cache.
	<b>rif validate-enable</b>	Enables RIF validation for entries learned on an interface (Token Ring or FDDI).
	<b>show rif</b>	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*

<b>Syntax Description</b>	<i>seconds</i>	Interval, in seconds, at which a proxy is sent. The valid range is any number greater than 0. Default is 2 seconds.
---------------------------	----------------	---

<b>Defaults</b>	2 seconds
-----------------	-----------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	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.
-------------------------	---

<b>Examples</b>	The following example specifies the interval at which a proxy is sent to be 3 seconds: <pre>rif validate-age 3</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>rif</b>	Enters static source-route information into the RIF cache.
	<b>rif timeout</b>	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.

**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
<b>rif timeout</b>	Determines the number of minutes an inactive RIF entry is kept.
<b>rif validate-age</b>	Defines the validation time when the Cisco IOS software is acting as a proxy for NetBIOS NAME_QUERY packet or for explorer frames.
<b>rif validate-enable-age</b>	Enables RIF validation for stations on a source-route bridge network that do not respond to an IEEE TEST command.
<b>rif validate-enable-route-cache</b>	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.

**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
	<b>rif validate-enable</b>	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.

**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
	<b>rif validate-enable</b>	Enables RIF validation for entries learned on an interface (Token Ring or FDDI).