bridge acquire

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

bridge *bridge-group* **acquire**

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

Syntax Description

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

Defaults

Enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

```
no bridge 1 acquire
```

Related Commands

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

bridge address

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

Related Commands

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

bridge bitswap-layer3-addresses

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

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

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

Syntax Description

bridge-group	Bridge group number.

Defaults

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
no ip routing
!
interface ethernet 0
 bridge-group 1
!
interface token-ring 0
 bridge-group 1
!
!
bridge 1 protocol ieee
bridge 1 bitswap-layer3-addresses
```

bridge bridge

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

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

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

Syntax Description

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

Defaults

Bridge every protocol.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

```
no bridge 1 bridge ip
```

Related Commands

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

bridge circuit-group pause

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

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

Syntax Description

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

Defaults

The default forward delay interval is 0.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

bridge circuit-group source-based

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

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

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

Syntax Description

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

Defaults

No bridge-group interface is assigned.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge cmf

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

bridge cmf

no bridge cmf

Syntax Description

This command has no arguments or keywords.

Defaults

CMF is disabled.

Command Modes

Global configuration

Command History

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

Examples

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

```
bridge cmf
```

Related Commands

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

bridge crb

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

bridge crb

no bridge crb

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
bridge crb
```

Related Commands

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

bridge domain

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

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

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

Syntax Description

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

Defaults

Single bridge domain. The default domain number is 0.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

```
bridge 1 domain 3
```

Related Commands

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

bridge forward-time

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

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

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

Syntax Description

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

Defaults

30-second delay.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

bridge hello-time

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

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

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

Syntax Description

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

Defaults

1 second.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge irb

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

bridge irb

no bridge irb

Syntax Description

This command has no arguments or keywords.

Defaults

Integrated routing and bridging (IRB) is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following shows how to enable integrated routing and bridging:

```
bridge irb
```

Related Commands

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

bridge lat-service-filtering

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

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

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

Syntax Description

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

Defaults

LAT service filtering is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge max-age

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

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

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

Syntax Description

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

Defaults

15 seconds.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge multicast-source

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

```
bridge 2 multicast-source
```

Related Commands

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

bridge priority

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

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

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
bridge 1 priority 100
```

Related Commands

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

bridge protocol

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

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

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

Syntax Description

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

Defaults

No Spanning Tree Protocol is defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
bridge 1 protocol dec
```

Related Commands

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

bridge protocol ibm

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

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

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

Syntax Description

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

Defaults

No bridge group is defined.

Command Modes

Global configuration

Command History

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

Examples

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

```
bridge 1 protocol ibm
```

Related Commands

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

bridge route

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

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

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

Syntax Description

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

Defaults

No default bridge group or protocol is specified.

Command Modes

Global configuration

Command History

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

Examples

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

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

Related Commands

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

bridge subscriber-policy

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

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

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

Syntax Description

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

Defaults

Table 5 shows the default values that are applied if no forward or filter decisions have been specified for the subscriber policy:

Table 10 Packet Default Values

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge-group

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

bridge-group *bridge-group*

no bridge-group *bridge-group*

Syntax Description

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

Defaults

No bridge group interface is assigned.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
bridge-group cbus-bridging	Enables autonomous bridging on a ciscoBus2 controller.
bridge-group circuit-group	Assigns each network interface to a bridge group.
bridge-group input-pattern-list	Associates an extended access list with a particular interface in a particular bridge group.
bridge-group output-pattern-list	Associates an extended access list with a particular interface.
bridge-group spanning-disabled	Disables the spanning tree on a given interface.

bridge-group aging-time

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

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

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

Syntax Description

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

Defaults

300 seconds.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example sets the aging time to 200 seconds:

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

Related Commands

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

bridge-group cbus-bridging

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

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

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

Syntax Description

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

Defaults

Autonomous bridging is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

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

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

Related Commands

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

bridge-group circuit-group

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

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

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

Syntax Description

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

Defaults

No bridge group interface is assigned.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

bridge-group input-address-list

To assign an access list to a particular interface, use the **bridge-group input-address-list** command in interface configuration mode. This access list is used to filter packets received on that interface based on their MAC source addresses. To remove an access list from an interface, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

No access list is assigned.

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

bridge-group input-lat-service-deny

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

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

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

Syntax Description

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

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

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

Examples

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

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

Related Commands

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

bridge-group input-lat-service-permit

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

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

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

Syntax Description

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

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

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

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

Examples

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

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

Related Commands

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

bridge-group input-lsap-list

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

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

Examples

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

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

Related Commands

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

bridge-group input-pattern-list

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

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

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

Related Commands

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

bridge-group input-type-list

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

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

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

Examples

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

```
interface tokenring 0
 ip address 131.108.1.1 255.255.255.0
 bridge-group 1
 bridge-group 1 input-type-list 201
```

Related Commands

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

bridge-group lat-compression

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

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

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

Examples

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

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

Related Commands

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

bridge-group output-address-list

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

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

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

Syntax Description

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

Defaults

No access list is assigned.

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

bridge-group output-lat-service-deny

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

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

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

Syntax Description

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

Defaults

No group codes are assigned.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

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

Examples

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

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

Related Commands

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

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

bridge-group output-lat-service-permit

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

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

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

Syntax Description

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

Defaults

No group codes are specified.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

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

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

Examples

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

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

Related Commands

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

bridge-group output-lsap-list

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

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

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

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

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

Examples

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

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

Related Commands

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

bridge-group output-pattern-list

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

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

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

Related Commands

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

bridge-group output-type-list

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

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

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

Syntax Description

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

Defaults

Disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Examples

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

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

Related Commands

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

bridge-group path-cost

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

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

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

Syntax Description

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

Defaults

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

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

bridge-group priority

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

Related Commands

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

bridge-group spanning-disabled

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

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

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

Syntax Description

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

Defaults

Spanning tree is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

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

Related Commands

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

bridge-group sse

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

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

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

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

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

Examples

The following shows how to enable SSE switching:

```
bridge-group 1 sse
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.

bridge-group subscriber-loop-control

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

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

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

Syntax Description

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

Defaults

Loop control is disabled.

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

bridge-group subscriber-trunk

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

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

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

Syntax Description

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

Defaults

The interface is set to a non-trunking port.

Command Modes

Interface configuration

Command History

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

Examples

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

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

Related Commands

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

bsc char-set

To specify the character set used by the Bisync support feature in this serial interface as either EBCDIC or ASCII, use the **bsc char-set** command in interface configuration mode. To cancel the character set specification, use the **no** form of this command.

bsc char-set {**ascii** | **ebcdic**}

no bsc char-set {**ascii** | **ebcdic**}

Syntax Description

ascii	ASCII character set.
ebcdic	EBCDIC character set. This character set is the default.

Defaults

EBCDIC

Command Modes

Interface configuration

Command History

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

Examples

The following command specifies that the ASCII character set will be used:

```
bsc char-set ascii
```

bsc contention

To specify an address on a contention interface, use the **bsc contention** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc contention *address*

no bsc contention

Syntax Description

address	Address assigned to contention interface. The range is from 1 to 255. The default is 0x01.

Defaults

The default address is 0x01 to accommodate backward compatibility to the previous point-to-point contention implementation.

Command Modes

Interface configuration

Command History

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

Examples

The following command specifies address 20 on the remote device:

```
bsc contention 20
```

Related Commands

Command	Description
bsc dial-contention	Specifies a router at the central site as a central router with dynamic allocation of serial interfaces.

bsc dial-contention

To specify a router at the central site as a central router with dynamic allocation of serial interfaces, use the **bsc dial-contention** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc dial-contention *timeout*

no bsc dial-contention

Syntax Description

timeout	Amount of time (in seconds) the interface can sit idle before it is returned to the idle interface pool. The range is from 2 to 30 seconds. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	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 timeout value is configurable to ensure that an interface does not get locked out because of a device outage during sending of data.

Examples

The following command defines a dial-in interface at the central site with an idle timeout of 10 seconds:

```
bsc dial-contention 10
```

Related Commands

Command	Description
bsc contention	Specifies an address on a contention interface.

bsc host-timeout

To detect deactivation of devices at the host, use the **bsc host-timeout** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

bsc host-timeout *interval*

no host-timeout *interval*

Syntax Description

interval	Timeout interval within which a poll or select for a control unit must be received. If this interval expires, the remote router is sent a teardown peer signal. The range is from 30 to 3000 deciseconds. The default is 600 deciseconds (60 seconds).

Defaults

The default interval is 600 deciseconds (60 seconds).

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	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 used to detect deactivation of devices at the host. If the host is told to deactivate or not poll a device, time will be required for the signal to propagate the network and get the remote end from polling. The timeout can be used to fine-tune the delay in detecting the host outage. The remote peer will stop polling the control unit that has timed out in the interval one to two times the configured timeout value.

Examples

The following example shows how to configure a timeout of 500 deciseconds:

```
bsc host-timeout 500
```

Related Commands

Command	Description
bsc secondary	Specifies that the router is acting as the secondary end of the Bisync link connected to the serial interface, and the attached remote device is a Bisync control station.
bstun group	Specifies the BSTUN group to which the interface belongs.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.

bsc pause

To specify the interval, to the tenth of a second, between starts of the polling cycle, use the **bsc pause** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc pause *time*

no bsc pause *time*

Syntax Description

time	Interval in tenths of a second. The default value is 30 (that is, 30 tenths of a second, or 3 seconds). The maximum time is 255 tenths of a second (25.5 seconds).

Defaults

30 tenths of a second (3 seconds)

Command Modes

Interface configuration

Command History

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

Examples

The following command sets the interval to 20 tenths of a second (2 seconds):

```
bsc pause 20
```

bsc poll-timeout

To specify the timeout, in tenths of a second, for a poll or select sequence, use the **bsc poll-timeout** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc poll-timeout *time*

no bsc poll-timeout *time*

Syntax Description

time	Time in tenths of a second. The default value is 30 (that is, 30 tenths of a second, or 3 seconds).

Defaults

30 tenths of a second (3 seconds).

Command Modes

Interface configuration

Command History

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

Examples

The following command sets the interval to 20 tenths of a second (2 seconds):

```
bsc poll-timeout 20
```

bsc primary

To specify that the router is acting as the primary end of the Bisync link connected to the serial interface, and that the attached remote devices are Bisync tributary stations, use the **bsc primary** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc primary

no bsc primary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The Bisync support feature in the serial interface uses the address of the incoming encapsulation for reply.

Examples

The following example specifies the router as the primary role:

```
bsc primary
```

Related Commands

Command	Description
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

bsc retries

To specify the number of retries performed before a device is considered to have failed, use the **bsc retries** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc retries *retries*

no bsc retries *retries*

Syntax Description

retries	Number of retries before a device fails. The default is 5.

Defaults

Five retries.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This commands 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 command sets the retry count to 10:

```
bsc retries 10
```

bsc secondary

To specify that the router is acting as the secondary end of the Bisync link connected to the serial interface, and the attached remote device is a Bisync control station, use the **bsc secondary** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc secondary

no bsc secondary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The Bisync support feature in this serial interface uses the address of the poll or selection block in the framing encapsulation. It also generates an end of transmission (EOT) frame preceding each Bisync poll and selection.

Examples

The following example specifies the router as the secondary role:

```
bsc secondary
```

Related Commands

Command	Description
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

bsc servlim

To specify the number of cycles of the active poll list that are performed between polls to control units in the inactive poll list, use the **bsc servlim** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc servlim *servlim-count*

no bsc servlim *servlim-count*

Syntax Description

servlim-count	Number of cycles. The range is from 1 to 50. The default is 3.

Defaults

Three cycles.

Command Modes

Interface configuration

Command History

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

Examples

The following command sets the number of cycles to 2:

```
bsc servlim 2
```

bsc spec-poll

To set specific polls, rather than general polls, used on the host-to-router connection, use the **bsc spec-poll** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bsc spec-poll

no spec-poll

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	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

Use the **bsc spec-poll** command when a router is connected to a host, and only when that host issues specific polls rather than general polls. Tandem hosts that poll ATM cash machines are typically configured to use specific polls rather than general polls.

Configuring a downstream (control-unit/device connected) router to support specific polling has no effect.

Examples

The following commands configure serial interface 0 to use specific poll:

```
interface serial 0
 description Connection to host.
 encapsulation bstun
 bstun group 1
 bsc secondary
 bsc spec-poll
 bsc char-set ebcdic
 bstun route all tcp 10.10.14.122
```

bstun group

To specify the block serial tunnel (BSTUN) group to which the interface belongs, use the **bstun group** command in interface configuration mode. To remove the interface from the BSTUN group, use the **no** form of this command.

bstun group *group-number*

no bstun group *group-number*

Syntax Description

group-number	BSTUN group to which the interface belongs.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Each BSTUN-enabled interface must be placed in a BSTUN group that was previously defined by the **bstun protocol-group** command. Packets travel only between BSTUN-enabled interfaces that are in the same group.

Examples

The following example specifies that serial interface 1 belongs to the previously defined protocol group 1:

```
interface serial 1
 encapsulation bstun
 bstun group 1
```

Related Commands

Command	Description
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
encapsulation bstun	Configures BSTUN on a particular serial interface.

bstun keepalive-count

To define the number of times to attempt a peer connection before declaring the peer connection to be down, use the **bstun keepalive-count** command in global configuration mode. To cancel the definition, use the **no** form of this command.

bstun keepalive-count *count*

no bstun keepalive-count

Syntax Description

count	Number of connection attempts. The range is from 2 to 10 retries.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.1	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

The following example sets the number of times to retry a connection to a peer to 4:

```
bstun keepalive-count 4
```

Related Commands

Command	Description
bstun remote-peer-keepalive	Enables detection of the loss of a peer.

bstun lisnsap

To configure a service access point (SAP) on which to listen for incoming calls, use the **bstun lisnsap** command in global configuration mode. To cancel the SAP on which to listen, use the **no** form of this command.

bstun lisnsap *sap-value*

no bstun lisnsap

Syntax Description

sap-value	SAP on which to listen for incoming calls. The default is 04.

Defaults

The default SAP value is 04.

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	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

Changes to the **bstun lisnsap** command configuration will not take effect until after the router has been reloaded.

Examples

The following example shows how to configure SAP for listening:

```
bstun lisnsap
```

Related Commands

Command	Description
bstun route (Frame Relay)	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer over Frame Relay.
frame-relay map bstun	Configures BSTUN over Frame Relay for passthrough.
frame-relay map llc2	Configures BSTUN over Frame Relay when using Bisync local acknowledgment.

bstun peer-map-poll

To map the state of the peer to polling, use the **bstun peer-map-poll** command in global configuration mode. To disable mapping of the peer state to polling and map to the received status messages, use the **no** form of this command.

bstun peer-map-poll

no bstun peer-map-poll

Syntax Description

This command has no arguments or keywords.

Defaults

The received status messages are mapped to polling.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)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 **bstun peer-map-poll** command to map the peer state to polling. If you configure this command, Bisync-to-IP protocol (BIP) activates polling when the BIP tunnel becomes active and stops polling when the tunnel connection is terminated. When the peer state-to-polling is not mapped, BIP waits for the host to issue an "active" status message across the BIP tunnel before polling the Automated Teller Machine (peer) device and polling is stopped when an "inactive" status message is received across the tunnel or the tunnel connection is terminated.

Related Commands

Command	Description
bstun peer-name	Enables the BSTUN function.
bstun reconnect-interval	Set the amount of time for the system to wait before trying to reconnect to a peer.
show bstun	Displays the current status of STUN connections.

bstun peer-name

To enable the block serial tunnel (BSTUN) function, use the **bstun peer-name** command in global configuration mode. To disable the function, use the **no** form of this command.

bstun peer-name *ip-address*

no bstun peer-name *ip-address*

Syntax Description

ip-address	Address by which this BSTUN peer is known to other BSTUN peers that are using the TCP transport.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The IP address defines the address by which this BSTUN peer is known to other BSTUN peers that are using the TCP transport. If this command is unconfigured or the **no** form of this command is specified, all BSTUN routing commands with IP addresses are deleted. BSTUN routing commands without IP addresses are not affected by this command.

Examples

The following example enables the BSTUN function:

```
bstun peer-name 10.10.254.201
```

Related Commands

Command	Description
bstun protocol-group	Defines a BSTUN group and the protocol it uses.

bstun protocol-group

To define a block serial tunnel (BSTUN) group and the protocol it uses, use the **bstun protocol-group** command in global configuration mode. To delete the BSTUN group, use the **no** form of this command.

bstun protocol-group *group-number protocol*

no bstun protocol-group *group-number protocol*

Syntax Description

group-number	BSTUN group number. Valid numbers are decimal integers in the range from 1 to 255.
protocol	Block serial protocol, selected from the following: • **adplex** • **adt-poll-select** • **adt-vari-poll** • **apos** • **async-generic** • **bsc** • **bsc-local-ack** • **diebold** • **mdi** • mosec • gddb

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.3(2)T	The **apos** keyword was added as a Block serial protocol.
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 **rxspeed**, **txspeed**, **databits**, **stopbits**, and **parity** line configuration commands must be set to match the device they are communicating with.

Interfaces configured to run the Adplex protocol should set the baud rate set to 4800 bps, use 8 data bits, 1 start bit, 1 stop bit, and use even parity.

Interfaces configured to run the adt-vari-poll and adt-poll-select protocols should set their baud rate set to 600 bps, use 8 data bits, 1 start bit, 1.5 stop bits, and use even parity.

Interfaces configured to run the MDI protocol should set their baud rate set to 4800 bps, 7 data bits, 1 start bit, 2 stop bits, and use odd parity. The MDI protocol allows alarm panels to be sent to the MDI alarm console.

Examples

The following example defines BSTUN group 1, specifies that it uses the Bisync protocol, and indicates that frames will be locally acknowledged:

```
Router(config)# bstun protocol-group 1 bsc-local-ack
```

Related Commands

Command	Description
bstun group	Specifies the BSTUN group to which the interface belongs.

bstun reconnect-interval

To set the amount of time for the system to wait before trying to reconnect to a peer, use the **bstun reconnect-interval** command in global configuration mode. To return to the default setting, use the **no** form of the command.

bstun reconnect-interval *time-value*

no bstun reconnect-interval *time-value*

Syntax Description

time-value	Amount of time (in seconds). The range is from 1 to 600 seconds. The default is 60 seconds.

Defaults

60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(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

This command applies only to Block Serial Tunneling (BSTUN) route Bisync-to-IP (BIP) connections that are defined as active.

Examples

In the following example, the system is configured to wait 300 seconds before trying to reestablish a peer connection:

```
bstun reconnect-interval 300
```

Related Commands

Command	Description
bstun route (BIP)	Specifies how frames will be forwarded from a BSTUN interface to a remote host over an IP network.

bstun remote-peer-keepalive

To enable detection of the loss of a peer, use the **bstun remote-peer-keepalive** command in global configuration mode. To disable detection, use the **no** form of this command.

bstun remote-peer-keepalive *seconds*

no bstun remote-peer-keepalive

Syntax Description

seconds	Keepalive interval, in seconds. The range is from 1 to 300 seconds. The default is 30 seconds.

Defaults

30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.1	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

In the following example, the remote peer keepalive interval is set to 60 seconds:

```
bstun remote-peer-keepalive 60
```

Related Commands

Command	Description
bstun keepalive-count	Defines the number of times to attempt a peer connection before declaring the peer connection to be down.

bstun route

To define how frames will be forwarded from a block serial tunnel (BSTUN) interface to a remote BSTUN peer, use the **bstun route** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

bstun route {**all** | **address** *address-number*} {**tcp** *ip-address* | **interface serial** *number*}

no bstun route {**all** | **address** *address-number*} {**tcp** *ip-address* | **interface serial** *number*}

Syntax Description

all	All BSTUN traffic received on the input interface is propagated, regardless of the address contained in the serial frame.
address	Serial frame that contains a specific address is propagated.
address-number	Poll address, a hexadecimal number from 01 to FF (but not all values are valid). The reply address to be used on the return leg is calculated from the configured poll address.
tcp	TCP encapsulation is used to propagate frames that match the entry.
ip-address	IP address of the remote BSTUN peer.
interface serial	High-level data link control (HLDC) encapsulation is used to propagate the serial frames.
number	Serial line to an appropriately configured router on the other end.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When the ADplex protocol is specified in the **bstun protocol-group** command, ADplex device addresses are limited to the range from 1 to 127 because ADplex alarm panels invert the device address in the ADplex frame when responding to alarm console commands.

When the adt-poll-select protocol is specified in the **bstun protocol-group** command, routes for specific addresses cannot be specified on the downstream router (connected to the alarm panel) because no address field is provided within frames that are sent back to the alarm console. The only way to route traffic back to the alarm console is to use the **bstun route all** form of the **bstun route** command. This is also true for the diebold protocol and any other protocol supported by the asynchronous-generic protocol group that does not include a device address in the frame.

When the adt-vari-poll protocol is specified in the **bstun protocol-group** command, ADT device addresses are limited to the range from 0 to 255, and address 0 is reserved for use as a broadcast address for adt-vari-poll only. If address 0 is specified in the **bstun route address** form of the **bstun route** command, the address is propagated to all configured BSTUN peers.

It is possible to use both the **all** and the **address** keywords on different **bstun route** commands on the same serial interface. When this is done, the **address** specifications take precedence; if none of these match, then the **all** specification is used to propagate the frame.

Examples

In the following example, all BSTUN traffic received on serial interface 0 is propagated, regardless of the address contained in the serial frame:

```
bstun route all interface serial 0
```

bstun route (BIP)

To specify how frames will be forwarded from a Block Serial Tunneling (BSTUN) interface to a remote host over an IP network, use the **bstun route** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

bstun route {**address** *cu-address*} {**bip** *ip-address*} {**fport** *port-number*} {**lport** *port-number* | **passive**} [**tcp-queue-max**] [**transparent**]

no bstun route {**address** *cu-address*} {**bip** *ip-address*} {**fport** *port-number*} {**lport** *port-number* | **passive**} [**tcp-queue-max**] [**transparent**]

Syntax Description

address	Propagates serial frames that contain a specific address.
cu-address	Control unit poll address for the Bisync end station. This address is a hexadecimal number from 01 to FF.
bip	Specifies that the Bisync-to-IP (BIP) translation form of TCP is to be used for propagating the frames that match the entry.
ip-address	Specifies the IP address of the remote BIP host computer.
fport	Indicates that a foreign or remote port number is either being listened on or connected from.
port-number	Specifies the foreign port number. The port number range is from 1025 to 32000.
lport	Indicates that a local port is being sourced from this router, and represents a specific control unit.
port-number	Specifies a local port number. The port number range is from 1025 to 32000.
passive	Indicates that an outbound connection will not be attempted. Instead, the system listens on port number 1963 for any connection requests from the host computer.
tcp-queue-max	(Optional) Sets the maximum size of the outbound TCP queue. The default is 100 packets.
transparent	(Optional) Specifies the method of sending text on a defined route. The default is nontransparent bisync text.

Defaults

The default is 100 packets.
The default is nontransparent bisync text.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.

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

Usage Guidelines

The remote or foreign IP address and port number are required for all connection types.

The user selects the connection type by either configuring a unique local port or by using the **passive** keyword. If the **passive** keyword is used, the foreign port must be unique and the system does not attempt an outbound connection but instead listens on port number 1963 for any connection requests from the host computer. If the **active** keyword is configured (that is, if a local port is configured), the system attempts an outbound connection but also listens for the connection to be established inbound.

The *cu-address* argument is the control unit poll address for the Bisync end station. This address is a hexadecimal number from 01 to FF. Valid addresses vary depending on the setting of the **bsc char-set** interface configuration command.

The TCP queue length, an optional configuration parameter, defaults to 100 packets.

By default, the method of sending text on a defined route is to use nontransparent Bisync text. To send in transparent Bisync text, specify the optional **transparent** keyword.

Examples

In the following example, BSTUN traffic with the control unit address C5 is routed to and from the host computer specified by the IP address 192.168.60.100:

```
bstun route address C5 bip 192.168.60.100 fport 2000 lport 3005
```

Related Commands

Command	Description
bstun group	Specifies the BSTUN group to which the interface belongs.
bstun peer-name	Enables the BSTUN function.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.

bstun route (Frame Relay)

To define how frames will be forwarded from a Block Serial Tunneling (BSTUN interface to a remote BSTUN peer over Frame Relay, use the **bstun route** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

bstun route {**all** | **address** *cu-address*} **interface serial** *number* [**dlci** *dlci rsap*] [**priority** *priority*]

no bstun route {**all** | **address** *cu-address*} **interface serial** *number* [**dlci** *dlci rsap*] [**priority** *priority*]

Syntax Description

all	All BSTUN traffic received on the input interface is propagated, regardless of the address contained in the serial frame.
address	Serial frames that contain a specific address are propagated.
cu-address	Control unit address for the Bisync end station.
interface serial *number*	Specify a serial interface on which Frame Relay encapsulation is used to propagate serial frames.
dlci *dlci*	(Optional) Data-link connection identifier to be used on the Frame Relay interface.
rsap	(Optional) Remoteservice access point (SAP), to be used when initiating an Logical Link Control (LLC)2 session. This argument is configurable only if the interface group number supports local acknowledgment.
priority *priority*	(Optional) Priority port to be used for this LLC2 session. Configurable only if the interface group number supports local acknowledgment.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.1	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 shows how toexample shows how to configure BSTUN over Frame Relay. All BSTUN traffic is propagated to serial interface 0 regardless of the address contained in the serial frame:

```
bstun route all interface serial 0 dlci 16
```

bstun route all apip

To define how asynchronous point of sale-to-IP conversion (APIP) frames will be forwarded from a block serial tunnel (BSTUN) interface to an APIP remote peer, use the **bstun route all apip** command in interface configuration mode. To disable the forwarding of APIP frames, use the **no** form of this command.

bstun route all apip *ip-address* [**fport** *port*] [**tcp-queue-max** *size*] [**header** {**vo** | **v1** | **v2**}] [**alternate** *ip-address2* [**dialstring** *phone-number*]]

no bstun route all apip *ip-address* [**fport**] [**tcp-queue-max**] [**header**]

Syntax Description

ip-address	The IP address of the BSTUN peer.
fport	(Optional) Specifies the port number of the remote (foreign) device.
port	(Optional) The remote port number.
tcp-queue-max	(Optional) Customizes the size of the TCP queue.
size	(Optional) The size of the TCP queue.
header	(Optional) Customizes the APIP header version.
v0	(Optional) A two-byte header that includes the header length in the length field.
v1	(Optional) A two-byte header that excludes the header length in the length field.
v2	(Optional) A four-byte header that excludes the header length from the length field.
alternate	(Optional) Specifies an alternate BSTUN peer.
ip-address2	(Optional) The IP address of the BSTUN peer.
dialstring	(Optional) Specifies that the router connects to the alternate BSTUN peer only when it receives the dial string from the POS device. If the connection to the alternate peer fails, a "No Carrier" message is sent to the POS device. If the dial string received from the POS device does not match the configured dial string on the router, then the router connects to the primary BSTUN peer. If the connection to the primary peer fails, a "No Carrier" message is sent to the POS device.
phone-number	(Optional) Dial string sent from the POS device to the router.

Defaults

The **bstun route all apip** command is disabled by default.
port: 10550
size: 100
The default APIP header version is **v0**.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.3(4)T1	The **alternate** and **dialstring** keywords and *ip-address2* and *phone-number* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

There are 2 options for configuring an alternate BSTUN peer: automatic and manual.

- Automatic: Specified by configuring the **alternate** *ip-address2* option. In this situation, if the router is unable to connect to the primary BSTUN peer, the router automatically attempts to connect to the alternate BSTUN peer. The router does not notify the POS device until either the router connects to one of the BSTUN peers or the both connection attempts fail.
- Manual: Specified by configuring the **alternate** *ip-address2* **dialstring** *phone-number* option. In this situation, the router only attempts to connect to the alternate BSTUN peer if the dial string recieved from the POS device matches the dial string specified by the *phone-number* argument. If the connection to the primary peer fails, a “No Carrier” message is sent to the POS device.

Examples

The following example shows a complete APIP configuration. The **bstun route all apip** command is configured such that the primary BSTUN peer is at IP address 10.122.2.1 and the alternate peer is at IP address 10.122.2.2. The router only attempts to connect to the alternate BSTUN peer if the POS device sends it the dialstring 4085555309.

```
bstun peer-name 10.122.2.10
bstun protocol-group 20 apos
bstun remote-peer-keepalive 100
bstun keepalive-count 5
!
interface serial 1
 physical-layer async
 no ip address
 encapsulation bstun
 bstun group 20
 bstun route all apip 10.122.2.1 alternate 10.122.2.2 dialstring 4085555309
 asp role primary
 asp dcd always
!
line 1
 databits 7
 parity even
 stopbits 1
```