CHAPTER 21

Transparent Bridging Commands

Use the commands in this chapter to configure and monitor transparent bridging networks. For transparent bridging configuration information and examples, refer to the "Configuring Transparent Bridging" chapter in the *Router Products Configuration Guide*.

access-list (standard)

Use the **access-list** global configuration command to establish MAC address access lists. Use the **no** form to remove a single access list entry.

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

Syntax Description

access-list-number	Integer from 700 to 799 that you select for the list.
permit	Permits the frame.
deny	Denies the frame.
address mask	48-bit MAC addresses written in dotted triplet form. The ones bits in the *mask* argument are the bits to be ignored in *address*.

Default

No MAC address access lists are established.

Command Mode

Global configuration

Example

This following example assumes that you want to disallow the bridging of Ethernet packets of all Sun workstations on Ethernet 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, while the second line permits everything else. You then assign the access list to the input side of Ethernet 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

access-list (extended)
access-list (type-code)

access-list (extended)

Use the **access-list** global configuration command to provide extended access lists that allow finer granularity of control. These lists allow you to specify both source and destination addresses and arbitrary bytes in the packet.

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

Syntax Description

access-list-number

Integer from 1100 through 1199 that you assign to identify one or more **permit**/**deny** conditions as an extended access list. Note that a list number in the range 1100 through 1199 distinguishes an extended access list from other access lists.

permit

Allows a connection when a packet matches an access condition. The router stops checking the extended access list after a match occurs. All conditions must be met to make a match.

deny

Disallows a connection when a packet matches an access condition. The router stops checking the extended access list after a match occurs. All conditions must be met to make a match.

source

MAC Ethernet address in the form *xxxx.xxxx.xxxx.*

source-mask

Mask of MAC Ethernet source address bits to be ignored. The router uses the *source* and *source-mask* arguments to match the source address of a packet.

destination

MAC Ethernet value used for matching the destination address of a packet.

destination-mask

Mask of MAC Ethernet destination address bits to be ignored. The router uses the *destination* and *destination mask* arguments to match the destination address of a packet.

offset

Range of values that must be satisfied in the access list. Specified in decimal or in hexadecimal format in the form 0x*nn*. The offset is the number of bytes from the destination address field; it is not an offset from the start of the packet. The number of bytes you need to offset from the destination address varies depending on the media encapsulation type you are using.

size — Range of values that must be satisfied in the access list. Must be an integer 1 through 4.

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

operand — Compares arbitrary bytes within the packet. The value to be compared to or masked against.

Default

No extended access lists are established.

Command Mode

Global configuration

Usage Guidelines

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

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

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

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

Example

The following example permits packets from MAC addresses 000c.1B*xx.xxxx* to any MAC address if the packet contains a value less than 0x55AA in the 2 bytes that begins 0x1E bytes into the packet:

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

The following example permits a NOP operation:

```
interface ethernet 0
bridge-group 3 output-pattern 1102
access-list 1101 permit 0000.0000.0000 ffff.ffff.ffff 0000.0000.0000 ffff.ffff.ffff
```

Related Commands

access-list (standard)
access-list (type-code)
bridge-group output-pattern

access-list (type-code)

Use the **access-list** global configuration command to build type-code access lists. Use the **no** form of the command to remove a single access list entry.

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

Syntax Description

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

Default

No type-code access lists are built.

Command Mode

Global configuration

Usage Guidelines

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

Access lists are evaluated according to the following algorithm:

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

If the length/type field is greater than 1500, the packet is treated as an LSAP packet unless the DSAP and SSAP fields are AAAA. If the latter is true, the packet is treated using type-code filtering.

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

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

Examples

The following example permits only LAT frames (type 0x6004) and filters out all other frame types:

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

The following example filters out only type codes assigned to DEC (0x6000 through 0x600F) and lets all other types pass:

```
access-list 202 deny   0x6000 0x600F
access-list 202 permit  0x0000 0xFFFF
```

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

Related Commands

access-list (standard)
access-list (extended)

bridge acquire

Use the **bridge acquire** global configuration command to use the system default behavior of forwarding any frames for stations that it has learned about dynamically. Use the **no bridge acquire** global configuration command to change the default behavior.

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

Syntax Description

bridge-group	Bridge group number. Must be the same as that specified in the **bridge protocol** command.

Default

Enabled

Command Mode

Global configuration

Usage Guidelines

When using the command default, the router forwards any frames from stations that its 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.

Example

The following example prevents the forwarding of dynamically determined source and destination addresses:

```
no bridge 1 acquire
```

Related Command

bridge address

bridge address

Use the **bridge address** global configuration command to filter frames with a particular MAC layer station source or destination address. Use the **no bridge address** command followed by the MAC address to disable the forwarding ability.

bridge *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface*]
no bridge *bridge-group* **address** *mac-address*

Syntax Description

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

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

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

Note MAC addresses on Ethernets 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, keep this point in mind. Note that when a bridged packet traverses a serial link, it has an Ethernet-style address.

Examples

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

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

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

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

Related Commands

bridge acquire
bridge-group input-address-list
bridge-group output-address-list

bridge circuit-group pause

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

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

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs.
circuit-group	Number of the circuit group to which the interface belongs.
milliseconds	Forward delay interval. It must be a value in the range 0 through 10000 milliseconds.

Default

0 millisecond pause

Command Mode

Global configuration

Usage Guidelines

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

Example

The following example sets the circuit group pause to 5000 milliseconds:

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

Related Commands

bridge circuit-group source-based
bridge-group circuit-group
show bridge circuit-group

bridge circuit-group source-based

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

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

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs
circuit-group	Number of the circuit group to which the interface belongs

Default

No bridge group interface is assigned

Command Mode

Global configuration

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.

Example

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

bridge circuit-group pause
bridge-group circuit-group
show bridge circuit-group

bridge domain

Use the **bridge domain** global configuration command to establish a domain by assigning it a decimal value between 1 and 10. Use the **no** form of the command to return it to a single bridge domain by choosing domain zero (0).

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

Syntax Description

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

Default

Single bridge domain

Command Mode

Global configuration

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 router/bridges within the domain. The devices in the domain, and only those devices, will then share spanning-tree information.

Use this feature when multiple routers share the same cable, and you wish to use only certain discrete subsets of those routers to share spanning-tree information with each other. This function is most useful when running other router applications, such as IP UDP flooding, that use the IEEE spanning tree. It also can 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.

Example

The following example places 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

bridge protocol
bridge-group

bridge forward-time

Use the **bridge forward-time** global configuration command to specify the forward delay interval for the router. Use the **no** form of this command to return the default interval.

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

Syntax Description

bridge-group	Bridge group number. It must be the same as specified in the **bridge protocol** command.
seconds	Forward delay interval. It must be a value in the range 10 through 200 seconds.

Default

30 seconds

Command Mode

Global configuration

Usage Guidelines

The forward delay interval is the amount of time the router 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 what its individual configuration might be.

Example

The following example sets the forward delay interval to 60 seconds:

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

Related Commands

bridge hello-time
bridge max-age

bridge hello-time

Use the **bridge hello-time** global configuration command to specify the interval between Hello Bridge Protocol Data Units (BPDUs). Use the **no** form of this command to return the default interval.

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

Syntax Description

bridge-group	Bridge group number. It must be the same as specified in the **bridge protocol** command.
seconds	Any value between 1 and 10 seconds.

Default

1 second

Command Mode

Global configuration

Usage Guidelines

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

Example

The following example sets the interval to 5 seconds:

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

Related Commands

bridge forward-time
bridge max-age

bridge lat-service-filtering

Use the **bridge lat-service-filtering** global configuration command to specify LAT group-code filtering. Use the **no** form of the command to disable the use of LAT service filtering on the bridge group.

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

Syntax Description

bridge-group	Bridge group in which this special processing is to take place

Default

LAT service filtering is disabled.

Command Mode

Global configuration

Usage Guidelines

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

Example

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

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

bridge max-age

Use the **bridge max-age** global configuration command to change the interval the bridge will wait to hear BPDUs from the root bridge. If a bridge does not hear BPDUs from the root bridge within this specified interval, it assumes that the network has changed and will recompute the spanning-tree topology. Use the **no** form of this command to return the default interval.

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

Syntax Description

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

Default

15 seconds

Command Mode

Global configuration

Usage Guidelines

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

Example

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

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

Related Commands

bridge forward-time
bridge hello-time

bridge multicast-source

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

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

Syntax Description

bridge-group	Bridge group number. It must be the same as specified in the **bridge protocol** command.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

If you need to bridge Token Ring over other medium, RSRB is recommended.

Example

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

```
bridge 2 multicast-source
```

bridge priority

Use the **bridge priority** global configuration command to configure the priority of an individual bridge, or the likelihood that it will be selected as the root bridge.

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

Syntax Description

bridge-group — The bridge group number. It must be the same as specified in the **bridge protocol** command.

number — The lower the number, the more likely the bridge will be chosen as root. When the IEEE spanning-tree protocol is enabled on the router, *number* ranges from 0 through 65535. When the DEC spanning-tree protocol is enabled, *number* ranges from 0 through 255.

Default

When the IEEE spanning-tree protocol is enabled on the router: 32768

When the DEC spanning-tree protocol is enabled on the router: 128

Command Mode

Global configuration

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** interface configuration command to control an interface priority.

Example

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

```
bridge 1 priority 100
```

Related Command

bridge-group priority

bridge protocol

Use the **bridge protocol** global configuration command to define the type of spanning-tree protocol. Use the **no bridge protocol** command, with the appropriate keywords and arguments, to delete the bridge group.

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

Syntax Description

bridge-group	Number in the range 1 through 9 that you choose to refer to a particular set of bridged interfaces. Frames are bridged only among interfaces in the same group. You will use the group number you assign in subsequent bridge configuration commands.
ieee	IEEE Ethernet spanning-tree protocol.
dec	DEC spanning-tree protocol.

Default

No spanning-tree protocol is defined.

Command Mode

Global configuration

Usage Guidelines

The router/bridges support two spanning-tree protocols: the IEEE 802.1 standard and the earlier DEC spanning-tree protocol upon which the IEEE standard is based. Multiple domains are supported for the IEEE spanning tree.

Note The IEEE 802.1D spanning-tree protocol is the preferred way of running the bridge. Use the DEC spanning-tree protocol only for backwards compatibility.

Example

The following example shows bridge 1 as using the DECnet spanning-tree protocol:

```
bridge 1 protocol dec
```

Related Command

bridge domain
bridge-group

bridge-group

Use the **bridge-group** interface configuration command to assign each network interface to a bridge group. Use the **no** form of this command to remove the interface from the bridge group.

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

Syntax Description

bridge-group	Number of the bridge group to which the interface belongs.

Default

No bridge group interface is assigned.

Command Mode

Interface configuration

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 HDLC, 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 reinitialized.

Example

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

```
interface ethernet0
bridge-group 1
```

Related Commands

bridge protocol
bridge-group cbus-bridging
bridge-group circuit
bridge-group input-pattern
bridge-group output-pattern
bridge-group spanning-disabled

bridge-group aging-time

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

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.
seconds	Aging-time, in the range 0 through 1000000 seconds. The default is 300 seconds.

Default

300 seconds

Command Mode

Global configuration

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 transmit continuously, increase the aging-time to record the dynamic entries for a longer time and thus reduce the possibility of flooding when the hosts transmit again.

Example

The following example sets the aging-time to 200 seconds:

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

Related Command

bridge-group

bridge-group cbus-bridging

Use the **bridge-group cbus-bridging** interface configuration command to enable autonomous bridging on a ciscoBus II-resident interface. Use the **no** form of this command to disable autonomous bridging.

bridge-group *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

Default

Autonomous bridging is disabled.

Command Mode

Interface configuration

Usage Guidelines

Normally, bridging takes place on the processor card at interrupt level. When autonomous bridging is enabled, bridging takes place entirely on the ciscoBus II, significantly improving performance.

You can enable autonomous bridging on Ethernet, FDDI (FCIT) and HSSI interfaces that reside on a ciscoBus II. Autonomous bridging is not supported on Token Ring interfaces, regardless of the type of bus in use.

To enable autonomous bridging on an interface, that interface must first be defined 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 ciscoBus II, use the **bridge-group cbus-bridging** command to enable autonomous bridging on any Ethernet, FDDI or HSSI interface.

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

Example

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

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

Related Command

bridge-group

bridge-group circuit-group

Use the **bridge-group circuit-group** interface configuration command to assign each network interface to a bridge group. Use the **no** form of this command to remove the interface from the bridge group.

bridge-group *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.
circuit-group	Circuit group number. The range is 1 through 9.

Default

No bridge group interface is assigned

Command Mode

Interface configuration

Usage Guidelines

Circuit groups are primarily intended for use with HDLC-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 as well.

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

Example

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

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

Related Commands

bridge circuit-group pause
bridge circuit-group source-based
show bridge circuit-group

bridge-group input-address-list

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

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

Syntax Description

bridge-group	Bridge group number. It must be in the range 1 through 9 and the same as defined by the **bridge-group** command.
access-list-number	Access list number you assigned with the bridge **access-list** command. It must be in the range 700 through 799.

Default

No access list is assigned.

Command Mode

Interface configuration

Example

The following example assumes you want to disallow the bridging of Ethernet packets of all Sun workstations on Ethernet 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, while the second line permits everything else. You then assign the access list to the input side of Ethernet 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

access-list
bridge address
bridge-group output-address-list

bridge-group input-lat-service-deny

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

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

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

Syntax Description

bridge-group — Bridge group number defined by the **bridge-group** command. It must be a value in the range 1 through 9.

group-list — List of LAT service groups. Single numbers and ranges are permitted. Specify a zero (0) to disable the LAT group code for the bridge group.

Default

No group codes are specified.

Command Mode

Interface configuration

Usage Guidelines

Autonomous bridging must be disabled to use this command.

This command causes the system to not bridge any LAT service advertisement that has any of the specified groups set.

Example

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

bridge-group input-lat-service-permit
bridge-group output-lat-service-deny

bridge-group input-lat-service-permit

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

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

Syntax Description

bridge-group	Bridge group number defined in the **bridge-group** command. It must be a value in the range 1 through 9.
group-list	LAT service groups. Single numbers and ranges are permitted. Specify a zero (0) to disable the LAT group code for the bridge group.

Default

No group codes are specified.

Command Mode

Interface configuration

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.

Example

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

bridge-group output-lat-service-permit
bridge-group input-lat-service-deny

bridge-group input-lsap-list

Use the **bridge-group input-lsap-list** interface configuration command to filter IEEE 802.2-encapsulated packets on input. Use the **no** form of this command to disable this capability.

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

Syntax Description

bridge-group

Bridge group number. It must be the same as defined in the **bridge-group** command. It must be a value in the range 1 through 9.

access-list-number

Access list number you assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Default

Disabled

Command Mode

Interface configuration

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. SNAP frames also must pass any applicable Ethernet type-code access list.

Example

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

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

Related Commands

access-list
bridge-group output-lsap-list

bridge-group input-pattern

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

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

Syntax Description

bridge-group	The bridge group number. It must be the same as defined in the **bridge-group** command. It must be a value in the range 1 through 9.
access-list-number	Access list number you assigned using the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the interface.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Example

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

```
interface Ethernet 0
bridge-group 3 input-pattern 1
```

Related Commands

access-list
bridge-group
bridge-group output-pattern

bridge-group input-type-list

Use the **bridge-group input-type-list** interface configuration command to filter Ethernet- and SNAP-encapsulated packets on input. Use the **no** form of this command to disable this capability.

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

Syntax Description

bridge-group	Bridge group number. It must be the same as defined in the **bridge-group** command.
access-list-number	Access list number you assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Default

Disabled

Command Mode

Interface configuration

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 DSAP/SSAP/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 also must pass any applicable IEEE 802 DSAP/SSAP access lists.

Example

The following example shows how to configure a Token Ring interface with an access list that allows only the 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

access-list
bridge-group output-type-list

bridge-group lat-compression

Use the **bridge-group lat-compression** interface configuration command to reduce the amount of bandwidth that LAT traffic consumes on the serial interface by specifying a LAT-specific form of compression. Use the **no** form of this command to disable LAT compression on the bridge group.

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

Syntax Description

bridge-group	Bridge group number. It must be the same as defined in the **bridge-group** command.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Compression is applied to LAT frames being sent out the router/bridge 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.

Example

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

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

bridge-group output-address-list

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

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

Syntax Description

bridge-group

Bridge group number in the range 1 through 9. It must be the same as defined in the **bridge-group** command.

access-list-number

Access list number you assigned with the bridge **access-list** command.

Default

No access list is assigned.

Command Mode

Interface configuration

Example

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

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

Related Commands

access-list
bridge address
bridge-group input-address-list

bridge-group output-lat-service-deny

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

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

Syntax Description

bridge-group	Bridge group number in the range 1 through 9. It must be the same as specified in the **bridge-group** command.
group-list	List of LAT groups. Single numbers and ranges are permitted.

Default

No group codes are assigned.

Command Mode

Interface configuration

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.

Example

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

access-list
bridge-group input-lat-service-deny
bridge-group output-lat-service-permit

bridge-group output-lat-service-permit

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

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

Syntax Description

bridge-group	Bridge group number in the range 1 through 9. It must be the same as specified in the **bridge-group** command.
group-list	LAT service advertisements.

Default

No group codes are specified.

Command Mode

Interface configuration

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.

Example

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

bridge-group input-lat-service-permit
bridge-group output-lat-service deny

bridge-group output-lsap-list

Use the **bridge-group output-lsap-list** interface configuration command to filter IEEE 802-encapsulated packets on output. Use the **no** form of this command to disable this capability.

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

Syntax Description

bridge-group	Bridge group number in the range 1 through 9. It must be the same as specified in the **bridge-group** command.
access-list-number	Access list number you assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Autonomous bridging must be disabled to use this command.

SNAP frames also must 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, it is not a good idea to have both input and output type code filtering on the same interface.

Access lists for Ethernet- and IEEE 802-encapsulated packets affect only bridging functions. It is not possible to use such access lists to block frames with protocols that are being routed.

Example

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

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

Related Commands

access-list
bridge-group input-lsap-list

bridge-group output-pattern-list

Use the **bridge-group output-pattern-list** interface configuration command to associate an extended access list with a particular interface. Use the **no** form of this command to disable this capability.

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

Syntax Description

bridge-group — Bridge group number in the range 1 through 9. It must be the same as specified in the **bridge-group** command.

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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Example

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

access-list (extended)
bridge-group
bridge-group input-pattern

bridge-group output-type-list

Use the **bridge-group output-type-list** interface configuration command to filter Ethernet- and SNAP-encapsulated packets on output. Use the **no** form of this command to disable this capability.

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

Syntax Description

bridge-group	Bridge group number in the range 1 through 9. It must be the same as specified in the **bridge-group** command.
access-list-number	Access list number you assigned with the bridge **access-list** command. Specify a zero (0) to disable the application of the access list on the bridge group. This access list is applied just before sending out a frame to an interface.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Autonomous bridging must be disabled to use this command.

Example

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

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

Related Commands

access-list
bridge-group input-type-list

bridge-group path-cost

Use the **bridge-group path-cost** interface configuration command to set a different path cost. Use the **no** form of this command to choose the default path cost for the interface.

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

Syntax Description

bridge-group	Bridge group number. It must be the same as specified in the **bridge-group** command.
cost	Path cost can range from 1 through 65535, with higher values indicating higher costs. This range applies regardless of whether the IEEE or DEC spanning tree protocol has been specified.

Default

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

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

Command Mode

Interface configuration

Usage Guidelines

By convention, the path cost is 10000/data rate of the attached LAN (IEEE), or 100000/data rate of the attached LAN (DEC), in Mbps.

Example

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

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

bridge-group priority

Use the **bridge-group priority** interface configuration command to set an interface priority when two bridges tie for position as the root bridge. The priority you set breaks the tie.

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

Syntax Description

bridge-group	Bridge group number. It must be the same as specified in the **bridge-group** command.
number	Priority number ranging from 0 through 255 (DEC), or 0 through 64000 (IEEE).

Default

128—DEC spanning tree protocol
32768—IEEE spanning tree protocol

Command Mode

Interface configuration

Usage Guidelines

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

Example

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

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

Related Command

bridge priority

bridge-group spanning-disabled

Use the **bridge-group spanning-disabled** interface configuration command to disable the spanning tree on a given interface.

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

Syntax Description

bridge-group	Bridge group number of the interface. It must be the same as specified in the **bridge-group** command.

Default

Spanning tree enabled

Command Mode

Interface configuration

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 BPDUs 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.

Example

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

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

Related Commands

bridge-group
bridge protocol

bridge-group sse

Use the **bridge-group sse** interface configuration command to enable Cisco's silicon switching engine (SSE) switching function. Use the **no** form of this command to disable SSE switching.

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

Syntax Description

bridge-group	Bridge group number. It must be a value in the range 1 through 9.

Default

Disabled

Command Mode

Interface configuration

Example

The following example enables SSE switching:

```
bridge-group 1 sse
```

Related Command

source-bridge

clear bridge

Use the **clear bridge** privileged EXEC command to remove any learned entries from the forwarding database and to clear the transmit and receive counts for any statically or system configured entries.

clear bridge *bridge-group*

Syntax Description

bridge-group	Bridge group number. It must be a value in the range 1 through 9.

Command Mode

Privileged EXEC

Example

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

```
clear bridge 1
```

Related Command

bridge address

clear sse

Use the **clear sse** privileged EXEC command to reinitialize the Silicon Switch Processor (SSP) on the Cisco 7000 series.

clear sse

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Privileged EXEC

Usage Guidelines

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

Example

The following example causes the SSP to be reinitialized:

```
clear sse
```

ethernet-transit-oui

Use the **ethernet-transit-oui** interface configuration command to choose the Organizational Unique Identifier (OUI) code to be used in the encapsulation of Ethernet Type II frames across Token Ring backbone networks. Various versions of this OUI code are used by Ethernet/Token Ring translational bridges. The default OUI form is **90-compatible**, which can be chosen with the **no** form of the command.

ethernet-transit-oui [**90-compatible** | **standard** | **cisco**]
no ethernet-transit-oui

Syntax Description

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

Default

90-compatible

Command Mode

Interface configuration

Usage Guidelines

This command replaces and extends the **bridge old-oui** command in release 9.0.

The actual OUI codes that are used, when they are used, and how they compare to Software Release 9.0-equivalent commands is shown in Table 21-1.

Table 21-1 Bridge OUI Codes

Keyword	OUI Used	When Used/Benefits	9.0 Command Equivalent
90-compatible	0000F8	By default, when talking to other Cisco routers. Provides the most flexibility.	**no bridge old-oui**
cisco	00000C	Provided for compatibility with future equipment.	None
standard	000000	When talking to IBM 8209 bridges and other vendor equipment. Does not provide for as much flexibility as the other two choices.	**bridge old-oui**

Do not use the keyword **standard** unless you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity. The use of the **standard** OUI of 000000 in the encapsulation of Ethernet Type II frames creates encapsulated frames on Token Rings that have formats identical to SNAP-encapsulated frames. The router receiving such a frame on a Token Ring for delivery on the Ethernet cannot distinguish between the two, and therefore must make an arbitrary choice between presenting the frame on the Ethernet as a SNAP-encapsulated frame or as an Ethernet Type II frame. The choice has been made to present all such frames as Ethernet Type II. Therefore, it is impossible to use the **standard** keyword if you wish to bridge SNAP-encapsulated frames between Token Rings and Ethernets. Using either the **cisco** or **90-compatible** keywords does not present such a restriction, because SNAP frames and Ethernet Type II-encapsulated frames have different OUI codes on Token Ring networks.

Example

The following example specifies Cisco's OUI form:

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

Related Commands

bridge-group
bridge protocol

frame-relay map bridge broadcast

Use the **frame-relay map bridge broadcast** interface configuration command to bridge over a Frame Relay network. Use the **no** form of this command to delete the mapping entry.

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

Syntax Description

dlci	DLCI number. The valid range is 16 to 1007.

Default

No mapping entry is established.

Command Mode

Interface configuration

Usage Guidelines

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

Example

The following example allows bridging over a Frame Relay network:

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

Related Command

A dagger (†) indicates that the command is documented in another chapter.

encapsulation frame-relay †

ip routing

Use the **ip routing** command to enable IP routing. Use the **no ip routing** global configuration command to disable IP routing so that you can then bridge IP.

ip routing
no ip routing

Syntax Description

This command has no arguments or keywords.

Default

IP routing

Command Mode

Global configuration

Usage Guidelines

All protocols except IP are bridged by a router/bridge unless their routing is explicitly enabled. Refer to the "IP Commands" chapter of this manual for the procedures to enable routing of individual protocols. IP is normally routed by the router/bridge.

Also note that bridging and routing are done on a per-system basis. If a protocol is being routed, it must be routed on all interfaces that are handling that protocol. This is similar for bridging. You cannot route IP on one interface and bridge it on another interface.

Assign the *same* IP address to all network interfaces to manage the system with Telnet, TFTP, SNMP, ICMP (ping), and so forth. Once bridging is enabled, all IP and ARP frames are forwarded or flooded by the router/bridge according to standard bridging and spanning-tree rules. IP routing processes such as IGRP or RIP must not be running.

Example

The following example disables IP routing:

```
no ip routing
```

show bridge

Use the **show bridge** privileged EXEC command to view classes of entries in the bridge forwarding database.

show bridge [*bridge-group*] [*interface*]
show bridge [*bridge-group*] [*address* [*mask*]]

Syntax Description

bridge-group (Optional) Number you chose that specifies a particular spanning tree.

interface (Optional) Specific interface, such as Ethernet 0.

address (Optional) 48-bit canonical (Ethernet ordered) MAC address. This may be entered with an optional mask of bits to be ignored in the address, which is specified with the *mask* argument.

mask (Optional) Bits to be ignored in the address. You must specify the *address* argument if you want to specify a mask.

Command Mode

Privileged EXEC

Sample Display of Various Possible Show Bridge Command Strings

The following is sample output of the **show bridge** command strings:

```
router# show bridge

show bridge ethernet 0
show bridge 0000.0c00.0000  0000.00FF.FFFF
show bridge 0000.0c00.0e1a
show bridge
```

In the sample output, the first command would display all entries for hosts reachable via interface Ethernet 0, the second command would display all entries with the vendor code of 0000.0c00.0000, and the third command would display the entry for address 0000.0c00.0e1a. In the fourth command, all entries in the forwarding database would be displayed. In all four examples, the bridge group number has been omitted.

Sample Display of Show Bridge Output

The following is sample output from the **show bridge** command:

```
router# show bridge

Total of 300 station blocks, 295 free
BG   Hash    Address         Action     Interface  Age  RX count  TX count
1    00/0    FFFF.FFFF.FFFF  discard    -          P    0         0
1    09/0    0000.0C00.0009  forward    Ethernet0  0    2         0
1    49/0    0000.0C00.4009  forward    Ethernet0  0    1         0
1    CA/0    AA00.0400.06CC  forward    Ethernet0  0    25        0
```

Table 21-2 describes significant fields shown in the display.

Table 21-2 Show Bridge Field Descriptions

Field	Description
Total of 300 station blocks	Total number of forwarding database elements in the system. The memory to hold bridge entries is allocated in blocks of memory sufficient to hold 300 individual entries. When the number of free entries falls below 25, another block of memory sufficient to hold another 300 entries is allocated. Therefore, the size of the bridge forwarding database is limited to the amount of free memory in the router.
295 free	Number in the free list of forwarding database elements in the system. The total number of forwarding elements is expanded dynamically, as needed.
BG	Bridging group to which the address belongs.
Hash	Hash key/relative position in the keyed list.
Address	Canonical (Ethernet ordered) MAC address.
Action	Action to be taken when that address is looked up; choices are to discard or forward the datagram.
Interface	Interface, if any, on which that address was seen.
Age	Number of minutes since a frame was received from or sent to that address. The letter “P” indicates a permanent entry. The letter “S” indicates the system as recorded by the router. On the modular systems, this is typically the broadcast address and the router’s own hardware address; on the IGS, this field will also include certain multicast addresses.
RX count	Number of frames received from that address.
TX count	Number of frames forwarded to that address.

show bridge circuit-group

Use the **show bridge circuit-group** EXEC command to display the interfaces configured in each circuit group and show whether they are currently participating in load distribution.

show bridge [*bridge-group*] **circuit-group** [*circuit-group*] [*src-mac-address*]
[*dst-mac-address*]]

Syntax Description

bridge-group	(Optional) Number that specifies a particular bridge group.
circuit-group	(Optional) Number that specifies a particular circuit group.
src-mac-address	(Optional) 48-bit canonical (Ethernet ordered) source MAC address.
dst-mac-address	(Optional) 48-bit canonical (Ethernet ordered) destination MAC address.

Command Mode

EXEC

Sample Display

The following is sample output of various **show bridge circuit-group** command strings:

```
routerA> show bridge circuit-group

Bridge group 1 Circuit group 1:
 Interface Serial0 : inserted, learning, forwarding
 Interface Serial3 : inserted, learning, forwarding
Bridge group 1 Circuit group 2:
 Interface Serial2 : inserted, learning, forwarding

routerA> show bridge 1 circuit-group 1

Bridge group 1 Circuit group 1:
 Interface Serial0 : inserted, learning, forwarding
 Interface Serial3 : inserted, learning, forwarding

routerA> show bridge 1 circuit-group 2

Bridge group 1 Circuit group 2:
 Interface Serial2 : inserted, learning, forwarding

routerA> show bridge 1 circuit-group 1 0000.6502.23EA 0000.1234.4567

Output circuit group interface is Serial3

routerA> show bridge 1 circuit-group 1 0000.6502.23EA

%Destination MAC address required

routerB> show bridge 1 circuit-group 1

Bridge group 1 Circuit group 1:
 Transmission pause interval is 250ms
 Output interface selection is source-based
 Interface Serial0 : inserted, learning, forwarding
 Interface Serial3 : inserted, learning, forwarding
 Interface Serial2 is unavailable

routerB> show bridge 1 circuit-group 1 0000.6502.23EA 0000.1234.4567

%Please enter source MAC address only
```

Table 21-3 describes significant fields shown in the display.

Table 21-3 Show Bridge Circuit-Group Field Descriptions

Field	Description
inserted/not inserted	Indicates whether interface is included or not included in circuit-group operation. If the interface is administratively down, or if line protocol is not up, the interface is not included in the circuit-group operation.
learning/not learning	Indicates whether this interface is in spanning tree protocol (IEEE or DEC) learning or not learning state.
forwarding/not forwarding	Indicates whether this port is in spanning tree protocol (IEEE or DEC) forwarding or not forwarding state

show span

Use the **show span** privileged EXEC command to display the spanning-tree topology known to the router/bridge. The display indicates whether LAT group code filtering is in effect.

show span

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

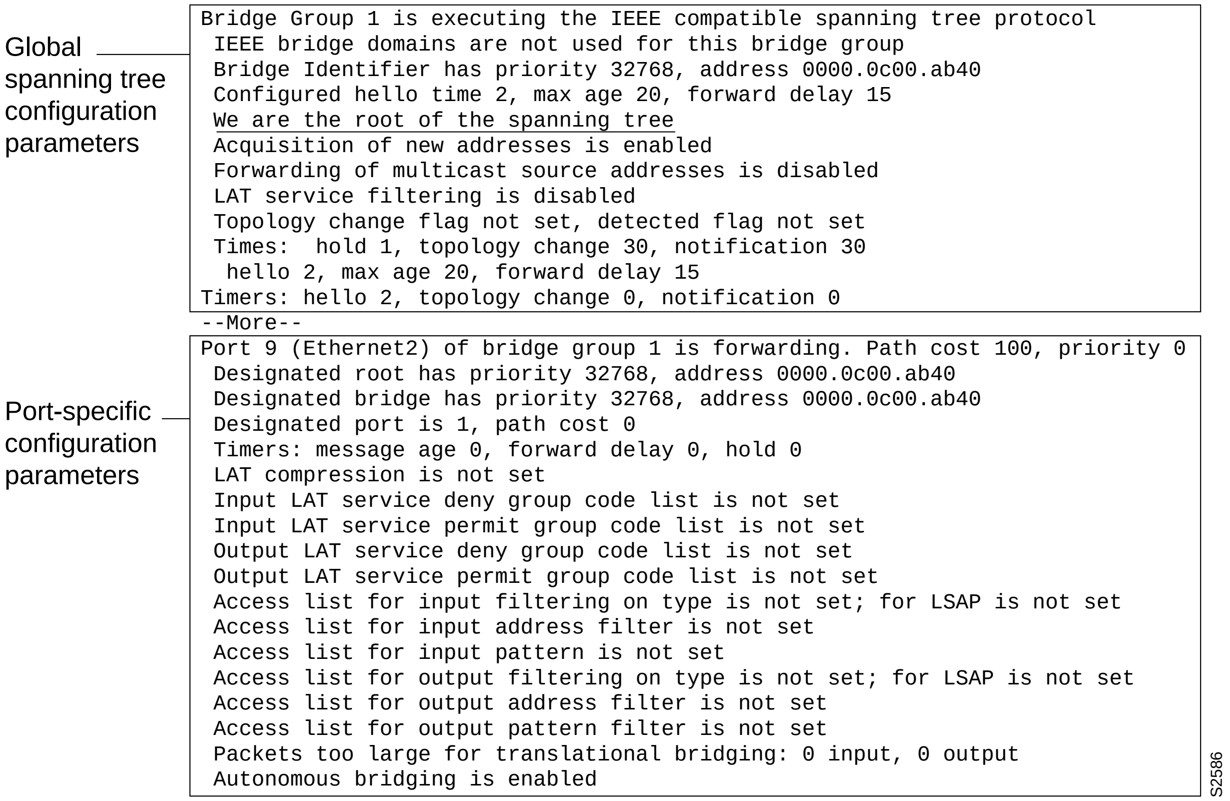
The following **bridge-group** commands are incompatible with autonomous bridging:

bridge-group input-type-list
bridge-group output-type-list
bridge-group input-lsap-list
bridge-group output-lsap-list
bridge-group input-pattern
bridge-group output-pattern
bridge-group input-lat-service-deny
bridge-group input-lat-service-permit
bridge-group output-lat-service-deny
bridge-group output-lat-service-permit
bridge-group lat-compression
bridge-group circuit

Sample Displays

The following is sample output for the **show span** command when the router is the root of the spanning tree.

```
router# show span
```



```
Bridge Group 1 is executing the IEEE compatible spanning tree protocol
 IEEE bridge domains are not used for this bridge group
 Bridge Identifier has priority 32768, address 0000.0c00.ab40
 Configured hello time 2, max age 20, forward delay 15
 We are the root of the spanning tree
 Acquisition of new addresses is enabled
 Forwarding of multicast source addresses is disabled
 LAT service filtering is disabled
 Topology change flag not set, detected flag not set
 Times:  hold 1, topology change 30, notification 30
  hello 2, max age 20, forward delay 15
Timers: hello 2, topology change 0, notification 0
--More--
Port 9 (Ethernet2) of bridge group 1 is forwarding. Path cost 100, priority 0
 Designated root has priority 32768, address 0000.0c00.ab40
 Designated bridge has priority 32768, address 0000.0c00.ab40
 Designated port is 1, path cost 0
 Timers: message age 0, forward delay 0, hold 0
 LAT compression is not set
 Input LAT service deny group code list is not set
 Input LAT service permit group code list is not set
 Output LAT service deny group code list is not set
 Output LAT service permit group code list is not set
 Access list for input filtering on type is not set; for LSAP is not set
 Access list for input address filter is not set
 Access list for input pattern is not set
 Access list for output filtering on type is not set; for LSAP is not set
 Access list for output address filter is not set
 Access list for output pattern filter is not set
 Packets too large for translational bridging: 0 input, 0 output
 Autonomous bridging is enabled
```

Global spanning tree configuration parameters
Port-specific configuration parameters
S2586

As the sample display shows, the first part of the **show span** output lists global spanning-tree configuration parameters, followed by those that are specific to given interfaces.

Explanations for representative lines of output in the display follow.

The first line of output indicates which type of spanning tree protocol (IEEE or DEC) the bridge group is executing:

```
Bridge Group 1 is executing the IEEE compatible spanning tree protocol
```

The following lines of output show the current operating parameters of the spanning tree. For more information, refer to the IEEE Standard 802.1D-1990.

```
IEEE bridge domains are not used for this bridge group
Bridge Identifier has priority 32768, address 0000.0c00.ab40
Configured hello time 2, max age 20, forward delay 15
```

The following line of output shows that the router is the root of the spanning tree:

```
We are the root of the spanning tree
```

The following lines of output have nothing to do with the spanning tree protocol, but are included in **show span** output for convenience, so that the user can avoid using the **write terminal** command to find out this information:

```
Acquisition of new addresses is enabled
Forwarding of multicast source addresses is disabled
LAT service filtering is disabled
```

The following lines of output show additional current operating parameters of the spanning tree. For more information, refer to the IEEE Standard 802.1D-1990.

```
Topology change flag not set, detected flag not set
Times:  hold 1, topology change 30, notification 30
       hello 2, max age 20, forward delay 15
Timers: hello 2, topology change 0, notification 0
```

Table 21-4 describes the fields in the following line of output.

```
Port 1 (Ethernet0) of bridge group 1 is forwarding. Path cost 100, priority 0
```

Table 21-4 Show Span Field Descriptions—First Port-Specific Line

Field	Description
Port 1	Port number associated with the interface. The port number and the port priority form the port ID.
(Ethernet0)	Interface on which Translational Bridging has been configured.
of bridge group 1	Bridge group to which the interface has been assigned.
is forwarding	State of the interface. Possible values follow: • Down • Listening • Learning • Forwarding • Blocking
Path cost 100	Path cost associated with the interface, as determined by default, or using the **bridge-group path cost** command.
priority 0	Port priority.

The following lines of output show the priority and the MAC address. Together they form the Root Identifier and the Bridge Identifier, respectively.

```
Designated root has priority 32768, address 0000.0c00.ab40
Designated bridge has priority 32768, address 0000.0c00.ab40
```

The following lines of output are self-explanatory:

```
Designated port is 1, path cost 0
Timers: message age 0, forward delay 0, hold 0
```

The following lines of output have nothing to do with the spanning tree protocol, but are included in **show span** output for convenience, so that the user can avoid using the **write terminal** command to find out this information:

```
LAT compression is not set
Input LAT service deny group code list is not set
Input LAT service permit group code list is not set
Output LAT service deny group code list is not set
Output LAT service permit group code list is not set
Access list for input filtering on type is not set; for LSAP is not set
Access list for input address filter is not set
Access list for input pattern is not set
Access list for output filtering on type is not set; for LSAP is not set
Access list for output address filter is not set
Access list for output pattern filter is not set
```

The following line of output indicates the number of packets destined for an interface which have been discarded by the bridge because they are larger than the MTU for the output media:

```
Packets too large for translational bridging: 0 input, 0 output
```

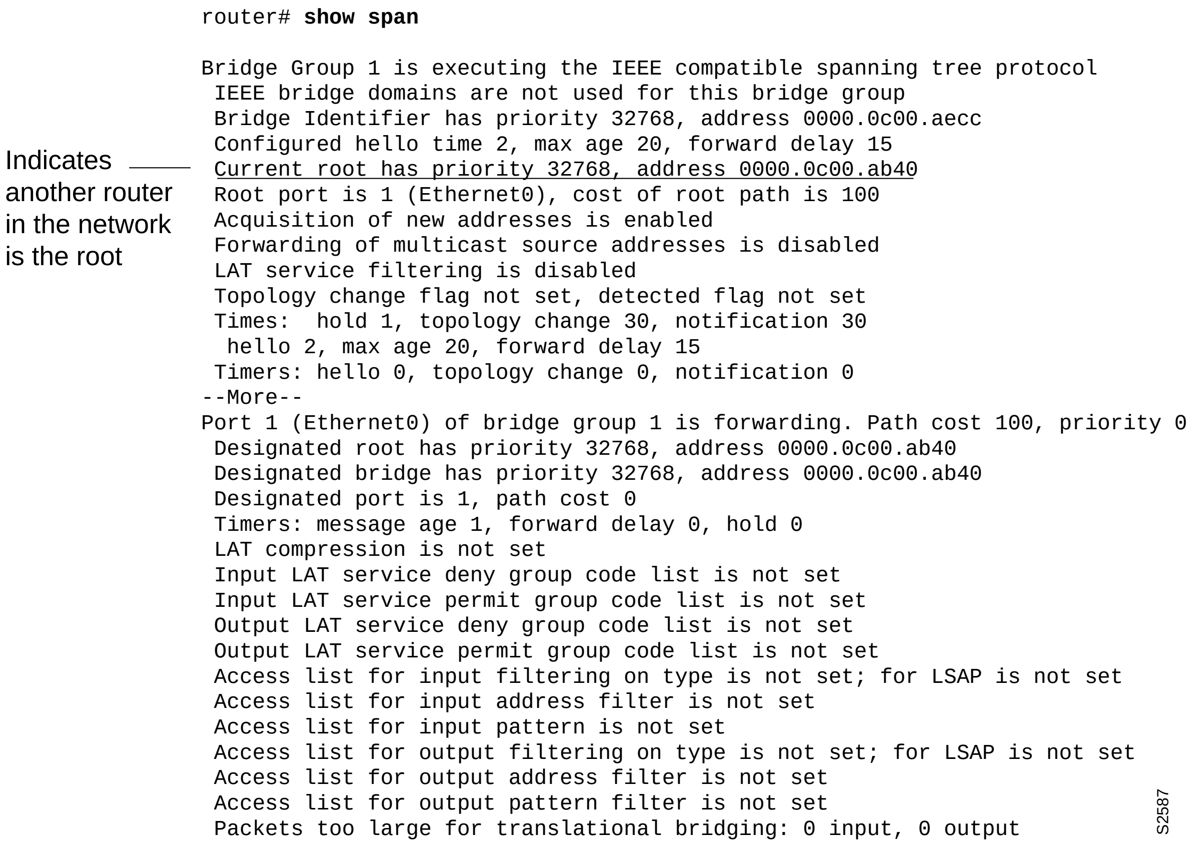
The following line of output indicates that autonomous bridging is enabled and no other incompatible bridge group commands have been defined:

```
Autonomous bridging is enabled
```

If autonomous bridging is configured on an interface and one or more incompatible bridge group commands have been defined the following line of output displays:

```
Autonomous bridging is suppressed
```

The following is a sample output from **show span** command when the router is *not* the root of the spanning tree.



```
router# show span

Bridge Group 1 is executing the IEEE compatible spanning tree protocol
 IEEE bridge domains are not used for this bridge group
 Bridge Identifier has priority 32768, address 0000.0c00.aecc
 Configured hello time 2, max age 20, forward delay 15
 Current root has priority 32768, address 0000.0c00.ab40
 Root port is 1 (Ethernet0), cost of root path is 100
 Acquisition of new addresses is enabled
 Forwarding of multicast source addresses is disabled
 LAT service filtering is disabled
 Topology change flag not set, detected flag not set
 Times:  hold 1, topology change 30, notification 30
  hello 2, max age 20, forward delay 15
 Timers: hello 0, topology change 0, notification 0
--More--
Port 1 (Ethernet0) of bridge group 1 is forwarding. Path cost 100, priority 0
 Designated root has priority 32768, address 0000.0c00.ab40
 Designated bridge has priority 32768, address 0000.0c00.ab40
 Designated port is 1, path cost 0
 Timers: message age 1, forward delay 0, hold 0
 LAT compression is not set
 Input LAT service deny group code list is not set
 Input LAT service permit group code list is not set
 Output LAT service deny group code list is not set
 Output LAT service permit group code list is not set
 Access list for input filtering on type is not set; for LSAP is not set
 Access list for input address filter is not set
 Access list for input pattern is not set
 Access list for output filtering on type is not set; for LSAP is not set
 Access list for output address filter is not set
 Access list for output pattern filter is not set
 Packets too large for translational bridging: 0 input, 0 output
```

This sample **show span** output is similar to the **show span** output for a router acting as the spanning tree root, except for the following lines of output.

The following line of output indicates that the root at address 0000.0c00.ab40 has a priority of 32768:

```
Current root has priority 32768, address 0000.0c00.ab40
```

The following line of output indicates the root port and the path cost:

```
Root port is 1 (Ethernet0), cost of root path is 100
```

show sse summary

Use the **show sse summary** EXEC command to display a summary of Silicon Switch Processor (SSP) statistics:

show sse summary

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Display

The following is sample output from the **show sse summary** command:

```
Router# show sse summary
SSE utilization statistics

               Program words  Rewrite bytes  Internal nodes  Depth
Overhead                 499              1               8
IP                         0              0               0      0
IPX                        0              0               0      0
SRB                        0              0               0      0
CLNP                       0              0               0      0
IP access lists            0              0               0
Total used               499              1               8
Total free             65037         262143
Total available        65536         262144

Free program memory
 [499..65535]
Free rewrite memory
 [1..262143]

Internals
 75032 internal nodes allocated, 75024 freed
 SSE manager process enabled, microcode enabled, 0 hangs
 Longest cache computation 4ms, longest quantum 160ms at 0x53AC8
```

x25 map bridge broadcast

Use the **x25 map bridge broadcast** interface configuration command to configure the bridging of packets in X.25 frames. Use the **no** form of this command to disable the Internet-to-X.121 mapping.

x25 map bridge *x.121-address* **broadcast** [*options-keywords*]
no x25 map bridge

Syntax Description

x.121-address	The X.121 address.
options-keywords	(Optional) The services that can be added to this map; these services are listed in the section "Setting Address Mappings" in the *Router Products Configuration Guide*.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

The X.25 bridging software uses the same spanning-tree algorithm as the other bridging functions, but allows packets to be encapsulated in X.25 frames and transmitted across X.25 media. This command specifies Internet-to-X.121 address mapping and maintains a table of both the Ethernet and X.121 addresses.

Example

The following example allows bridging over an X.25 network:

```
x25 map bridge 31370054065 broadcast
```

Related Command

x25 address