# source-bridge max-out-hops

To control the forwarding or blocking of spanning-tree explorer frames sent from this interface, use the **source-bridge max-out-hops** command in interface configuration mode. To reset the count to the maximum value, use the **no** form of this command.

**source-bridge max-out-hops** *count*

**no source-bridge max-out-hops**

## Syntax Description

| | |
|---|---|
| *count* | Determines the number of bridges an explorer packet can traverse. Typically, the maximum number of bridges for interoperability with IBM equipment is seven. |

## Defaults

The maximum number of bridge hops is seven.

## Command Modes

Interface 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

Frames are forwarded only if the number of hops in the routing information field of the frame (including the hops appended by the router) is fewer than or equal to the specified count. This applies only to spanning-tree explorer frames output from the specified interface.

## Examples

The following example limits the maximum number of source-route bridge hops to five:

```
source-bridge max-out-hops 5
```

## Related Commands

| Command | Description |
|---|---|
| **source-bridge** | Configures an interface for SRB. |
| **source-bridge max-hops** | Controls the forwarding or blocking of all-route explorer frames received on an interface. |
| **source-bridge max-in-hops** | Controls the forwarding or blocking of spanning-tree explorer frames received on an interface. |

# source-bridge output-address-list

To apply an access list to an interface configured for source-route bridging, use the **source-bridge output-address-list** command in interface configuration mode. To remove the application of the access list, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of the access list. The value must be in the range from 700 to 799. |

## Defaults

No access list is assigned.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

This command filters source-routed packets sent to the router interface based upon the destination MAC address.

## Examples

To disallow the bridging of Token Ring packets of all IBM workstations on Token Ring 1, use this sample configuration. The software assumes that all such hosts have Token Ring addresses with the vendor code 1000.5A00.0000. The vendor portion of the MAC address is the first three bytes (left to right) of the address. The first line of the access list denies access to all IBM workstations, and the second line permits access to all other devices on the network. Then, the access list can be assigned to the input side of Token Ring 1.

```
access-list 700 deny 1000.5A00.0000   8000.00FF.FFFF
access-list 700 permit 0000.0000.0000   FFFF.FFFF.FFFF
interface tokenring 1
 source-bridge output-address-list 700
```

**Related Commands**

| Command | Description |
|---|---|
| **access-list** | Configures the access list mechanism for filtering frames by protocol type or vendor code. |
| **source-bridge input-address-list** | Applies an access list to an interface configured for source-route bridging, and filters source-routed packets received from the router interface based on the source MAC address. |

# source-bridge output-lsap-list

To filter, on output, FDDI and IEEE 802-encapsulated packets that have destination service access point (DSAP) and source service access point (SSAP) fields in their frame formats, use the **source-bridge output-lsap-list** command in interface configuration mode.

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

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

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of the access list. This access list is applied just before sending out a frame to an interface. Specify zero (0) to disable the filter. The value must be in the range from 200 to 299. |

## Defaults

No filters are applied.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

The access list specifying the type codes to be filtered is given by this command.

## Examples

The following example specifies access list 251:

```
access-list 251 permit 0xE0E0 0x0101
access-list 251 deny 0x0000 0xFFFF
!
interface tokenring 0
 source-bridge output-lsap-list 251
```

## Related Commands

| Command | Description |
|---|---|
| **access-list** | Configures the access list mechanism for filtering frames by protocol type or vendor code. |
| **source-bridge input-lsap-list** | Filters, on input, FDDI and IEEE 802-encapsulated packets that include the DSAP and SSAP fields in their frame formats. The access list specifying the type codes to be filtered is given by this variation of the **source-bridge** command in interface configuration mode. |

# source-bridge output-type-list

To filter Subnetwork Access Protocol (SNAP)-encapsulated frames by type code on output, use the **source-bridge output-type-list** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**source-bridge output-type-list** *access-list-numbers*

**no source-bridge output-type-list** *access-list-numbers*

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of the access list. This access list is applied just before sending out a frame to an interface. Specify zero (0) to disable the application of the access list on the bridge group. The value must be in the range from 200 to 299. |

## Defaults

No filters are applied.

## 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

Input and output type code filtering on the same interface reduces performance and is not recommended.

Access lists for Token Ring- and IEEE 802-encapsulated packets affect only source-route bridging functions. Such access lists do not interfere with protocols that are being routed.

Use the access list specifying the types codes in this command.

## Examples

The following example filters SNAP-encapsulated frames on output:

```
access-list 202 deny 0x6000 0x0007
access-list 202 permit 0x0000 0xFFFF
!
! apply interface configuration commands to interface tokenring 0
interface tokenring 0
! filter SNAP-encapsulated frames on output using access list 202
 source-bridge output-type-list 202
```

**Related Commands**

| Command | Description |
|---|---|
| **access-list** | Configures the access list mechanism for filtering frames by protocol type or vendor code. |
| **source-bridge input-type-list** | Filters SNAP-encapsulated packets on input. |

# source-bridge passthrough

To configure some sessions on a few rings to be locally acknowledged and the remaining to pass through, use the **source-bridge passthrough** command in global configuration mode. To disable passthrough on all the rings and allow the session to be locally acknowledged, use the **no** form of this command.

**source-bridge passthrough** *ring-group*

**no source-bridge passthrough** *ring-group*

## Syntax Description

| | |
|---|---|
| *ring-group* | Ring group number. This ring is either the start ring or destination ring of the two IBM end machines for which the pass through feature is to be configured. This ring group number must match the number you specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095. |

## 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

Use this command in conjunction with the **source-bridge remote-peer tcp** command that has the **local-ack** keyword specified, which causes every new Logical Link Control, type 2 (LLC2) session to be locally terminated. If a machine on the Token Ring attempts to start an LLC2 session to an end host that exists on the *ring-group* value specified in the **source-bridge passthrough** command, the session will "pass through" and not use local acknowledgment for LLC2.

If you specify pass through for a ring, LLC2 sessions will never be locally acknowledged on that ring. This is true even if a remote peer accessing the ring has set th**e local-ack** keyword in the **source-bridge remote-peer tcp** command. The **source-bridge passthrough** command overrides any setting in the **source-bridge remote-peer tcp** command.

You can define more than one **source-bridge passthrough** command in a configuration.

## Examples

The following example configures the router to use local acknowledgment on remote peer at 10.1.1.2 but pass through on rings 9 and 4:

```
source-bridge ring-group 100
source-bridge remote-peer 100 tcp 10.1.1.1
source-bridge remote-peer 100 tcp 10.1.1.2 local-ack
source-bridge passthrough 9
source-bridge passthrough 4
```

## Related Commands

| Command | Description |
|---|---|
| **source-bridge remote-peer tcp** | Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP. |
| **source-bridge ring-group** | Defines or removes a ring group from the configuration. |

# source-bridge proxy-explorer

To configure the interface to respond to any explorer packets from a source node that meet the conditions described below, use the **source-bridge proxy-explorer** command in interface configuration mode. To cancel responding to explorer packets with proxy explorers, use the **no** form of this command.

**source-bridge proxy-explorer**

**no source-bridge proxy-explorer**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

The proxy explorer function allows the source-route bridge interface to respond to a source node on behalf of a particular destination node. The interface responds with proxy explorers. The following conditions must be met in order for the interface to respond to a source node with proxy explorers on behalf of a destination node:

- The destination node must be in the Routing Information Field (RIF) cache.
- The destination node must not be on the same ring as the source node.
- The explorer packet must be an IEEE 802.2 XID or TEST packet.
- The packet cannot be from the IBM Token Ring LAN Network Manager source service access point (SAP).

If all of the conditions are met, the source-route bridge interface will turn the packet around, append the appropriate RIF, and reply to the source node.

Use proxy explorers to limit the amount of explorer traffic propagating through the source-bridge network, especially across low-bandwidth serial lines. The proxy explorer is most useful for multiple connections to a single node.

## Examples

The following example configures the router to use proxy explorers on Token Ring 0:

```
interface tokenring 0
 source-bridge proxy-explorer
```

# source-bridge proxy-netbios-only

To enable proxy explorers for the NetBIOS name-caching function, use the **source-bridge proxy-netbios-only** command in global configuration mode. To disable the NetBIOS name-caching function, use the **no** form of this command.

**source-bridge proxy-netbios-only**

**no source-bridge proxy-netbios-only**

## Syntax Description

This command has no arguments or keywords.

## 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. |

## Examples

The following example configures the router to use proxy explorers:

```
source-bridge proxy-netbios-only
```

# source-bridge qllc-local-ack

To enable or disable Qualified Logical Link Control (QLLC) local acknowledgment for all QLLC conversion connections, use the **source-bridge qllc-local-ack** command in global configuration mode. To disable this capability, use the **no** form of this command.

**source-bridge qllc-local-ack**

**no source-bridge qllc-local-ack**

## Syntax Description

This command has no arguments or keywords.

## Defaults

QLLC local acknowledgment is disabled.

## 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

In a remote source-route bridged topology, QLLC local acknowledgment is used to configure the QLLC conversion router (connecting the remote X.25 devices) to exchange local acknowledgment information with the Token Ring router (on the Token Ring side of the cloud). This Token Ring device has been configured for Logical Link Control, type 2 (LLC2) local acknowledgment using the **source-bridge remote-peer tcp local-ack** command.

You must issue the **source-bridge qllc-local-ack** command only on the QLLC conversion router. When this command is issued, all of the QLLC conversion sessions are locally acknowledged at the Token Ring interface of the Token Ring router with which it is communicating using QLLC conversion.

## Examples

The following configuration indicates that the local router (10.108.2.2) QLLC conversion sessions will be locally acknowledged at the remote router:

```
source-bridge ring-group 100
source-bridge remote-peer 100 tcp 10.108.1.1 local-ack
source-bridge remote-peer 100 tcp 10.108.2.2
source-bridge qllc-local-ack
```

**Related Commands**

| Command | Description |
|---|---|
| **source-bridge remote-peer tcp** | Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP. |
| **source-bridge sdllc-local-ack** | Activates local acknowledgment for SDLLC sessions on a particular interface. |

# source-bridge remote-peer frame-relay

To specify a point-to-point direct encapsulation connection, use the **source-bridge remote-peer frame-relay** command in global configuration mode. To disable previous interface assignments, use the **no** form of this command.

**source-bridge remote-peer** *ring-group* **frame-relay interface** *name number* [*mac-address*] [*dlci-number*] [**lf** *size*]

**no source-bridge remote-peer** *ring-group* **frame-relay interface** *name number*

## Syntax Description

| | |
|---|---|
| *ring-group* | Ring group number. This ring group number must match the number you specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095. |
| **interface** *name number* | Name and number of the interface over which to send source-route bridged traffic. |
| *mac-address* | (Optional) MAC address for the interface on the other side of the virtual ring. This argument is required for nonserial interfaces. You can obtain the value of this MAC address by using the **show interface** command, and then scanning the display for the interface specified by the *name* argument. |
| *dlci-number* | (Optional) Data-link connection identifier (DLCI) number for Frame Relay encapsulation. |
| **lf** *size* | (Optional) Maximum-sized frame to be sent to this remote peer, in bytes. The Cisco IOS software negotiates all transit routes down to this size or lower. Use the size argument to prevent timeouts in end hosts by reducing the amount of data they must send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800. |

## Defaults

No point-to-point direct encapsulation connection is specified.

## 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

Use this command to identify the interface over which to send source-route bridged traffic to another router in the ring group. A serial interface does not require that you include a MAC-level address; all other types of interfaces do require MAC addresses.

You must specify one **source-bridge remote-peer** command for each peer router that is part of the virtual ring. You must also specify one **source-bridge remote-peer** command to identify the IP address of the local router.

It is possible to mix all types of transport methods within the same ring group.

**Note** The two peers using the serial-transport method will function correctly only if there are routers at the end of the serial line that have been configured to use the serial transport. The peers must also belong to the same ring group.

## Examples

The following example sends source-route bridged traffic over serial interface 0 and Ethernet interface 0:

```
! send source-route bridged traffic over serial 0
source-bridge remote-peer 5 frame-relay interface serial 0
! specify MAC address for source-route bridged traffic on Ethernet 0
source-bridge remote-peer 5 interface Ethernet 0 0000.0c00.1234
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays statistics for the interfaces configured on a router or access server. |
| **source-bridge** | Configures an interface for source-route bridging (SRB). |
| **source-bridge remote-peer fst** | Specifies an FST encapsulation connection. |
| **source-bridge remote-peer tcp** | Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP. |

# source-bridge remote-peer fst

To specify a Fast-Sequenced Transport (FST) encapsulation connection, use the **source-bridge remote-peer fst** command in global configuration mode. To disable the previous assignments, use the **no** form of this command.

**source-bridge remote-peer** *ring-group* **fst** *ip-address* [**lf** *size*]

**no source-bridge remote-peer** *ring-group* **fst** *ip-address*

## Syntax Description

| | |
|---|---|
| *ring-group* | Ring group number. This ring group number must match the number you specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095. |
| *ip-address* | IP address of the remote peer with which the router will communicate. |
| **lf** *size* | (Optional) Maximum-sized frame to be sent to this remote peer, in bytes. The Cisco IOS software negotiates all transit routes down to this size or lower. Use the size argument to prevent timeouts in end hosts by reducing the amount of data they must send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800. |

## Defaults

No FST encapsulation connection is specified.

## 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 two peers using the serial-transport method will function correctly only if there are routers at the end of the serial line that have been configured to use the serial transport. The peers must also belong to the same ring group.

You must specify one **source-bridge remote-peer** command for each peer router that is part of the virtual ring. You must also specify one **source-bridge remote-peer** command to identify the IP address of the local router.

## Examples

In the following example, the **source-bridge-fst-peername** command specifies an IP address of 10.136.64.98 for the local router. The **source-bridge ring-group** command assigns the device to a ring group. The **source-bridge remote-peer fst** command specifies ring group number 100 for the remote peer at IP address 10.136.64.97.

```
source-bridge fst-peername 10.136.64.98
source-bridge ring-group 100
source-bridge remote-peer 100 fst 10.136.64.97
```

# source-bridge remote-peer interface

When specifying a point-to-point direct encapsulation connection, use the **source-bridge remote-peer interface** command in global configuration mode. To disable previous interface assignments, use the **no** form of this command.

**source-bridge remote-peer** *ring-group* **interface** *name number* [*mac-address*] [**lf** *size*]

**no source-bridge remote-peer** *ring-group* **interface** *name number*

## Syntax Description

| | |
|---|---|
| *ring-group* | Ring group number. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095. |
| **interface** *name number* | Name of the serial interface over which to send source-route bridged traffic. |
| *mac-address* | (Optional) MAC address for the interface you specify using the *name* argument. This argument is required for nonserial interfaces. You can obtain the value of this MAC address by using the **show interfaces** command, and then scanning the display for the interface specified by the *name* argument. |
| **lf** *size* | (Optional) Maximum size frame to be sent to this remote peer in bytes. The Cisco IOS software negotiates all transit routes down to this size or lower. The size argument is useful in preventing timeouts in end hosts by reducing the amount of data they must send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800. |

## Defaults

No point-to-point direct encapsulation connection is specified.

## 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

Use this command to identify the interface over which to send source-route bridged traffic to another router or bridge in the ring group. A serial interface does not require that you include a MAC-level address; all other types of interfaces do require MAC addresses.

It is possible to mix all types of transport methods within the same ring group.

**Note** The two peers using the serial-transport method will function correctly only if there are routers at the end of the serial line that have been configured to use the serial transport. The peers must also belong to the same ring group.

## Examples

The following example shows how to send source-route bridged traffic over serial interface 0 and Ethernet interface 0:

```
! send source-route bridged traffic over serial 0
source-bridge remote-peer 5 interface serial 0
! specify MAC address for source-route bridged traffic on Ethernet 0
source-bridge remote-peer 5 interface ethernet 0 0000.0c00.1234
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays statistics for the interfaces configured on a router or access server. |
| **source-bridge remote-peer tcp** | Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP. |

# source-bridge remote-peer tcp

To identify the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP, use the **source-bridge remote-peer tcp** command in global configuration mode. To remove a remote peer for the specified ring group, use the **no** form of this command.

**source-bridge remote-peer** *ring-group* **tcp** *ip-address* [**lf** *size*] [**tcp-receive-window** *wsize*] [**local-ack**] [**priority**]

**no source-bridge remote-peer** *ring-group* **tcp** *ip-address*

## Syntax Description

| | |
|---|---|
| *ring-group* | Ring group number. This ring group number must match the number you specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095. |
| *ip-address* | IP address of the remote peer with which the router will communicate. The default is that no IP address is identified. |
| **lf** *size* | (Optional) Maximum size frame to be sent to this remote peer in bytes. The Cisco IOS software negotiates all transit routes down to this size or lower. The size argument is useful in preventing timeouts in end hosts by reducing the amount of data they must send in a fixed interval. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800. |
| **tcp-receive-window** *wsize* | (Optional) The TCP receive window size in bytes. The range is from 10240 to 65535 bytes. The default window size is 10240 bytes. |
| **local-ack** | (Optional) Logical Link Control, type 2 (LLC2) sessions destined for a specific remote peer are locally terminated and acknowledged. Use local acknowledgment for LLC2 sessions going to this remote peer. |
| **priority** | (Optional) Enables prioritization over a TCP network. You must specify the **local-ack** keyword earlier in the same **source-bridge remote-peer** command. The **priority** keyword is a prerequisite for features such as System Network Architecture (SNA) Class of Service (COS) and Systems Network Architecture (SNA) logical unit (LU) address prioritization over a TCP network. |

## Defaults

No IP address is identified.

The default window size is 10240 bytes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 11.1 | The **tcp-receive-window** keyword was added. |

| 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

If you change the default TCP receive window size on one peer, you must also change the receive window size on the other peer. Both sides of the connection should have the same window size.

If you configure one peer for LLC2 local acknowledgment, you need to configure both peers for LLC2 local acknowledgment. If only one peer is so configured, unpredictable results occur.

You must specify one **source-bridge remote-peer** command for each peer router that is part of the virtual ring. You must also specify one **source-bridge remote-peer** command to identify the IP address of the local router.

The two peers using the serial-transport method will function correctly only if there are routers at the end of the serial line that have been configured to use the serial transport. The peers must also belong to the same ring group.

## Examples

In the following example, the remote peer with IP address 10.108.2.291 belongs to ring group 5. It also uses LLC2 local acknowledgment, priority, and remote source-route bridging (RSRB) protocol version 2:

```
! identify the ring group as 5
source-bridge ring-group 5
! remote peer at IP address 10.108.2.291 belongs to ring group 5, uses
! tcp as the transport, is set up for local acknowledgment, and uses priority
source-bridge remote-peer 5 tcp 10.108.2.291 local-ack priority
```

The following example shows how to locally administer and acknowledge LLC2 sessions destined for a specific remote peer:

```
! identify the ring group as 100
source-bridge ring-group 100
! remote peer at IP address 10.1.1.1 does not use local acknowledgment
source-bridge remote-peer 100 tcp 10.1.1.1
! remote peer at IP address 10.1.1.2 uses local acknowledgment
source-bridge remote-peer 100 tcp 10.1.1.2 local-ack
!
interface tokenring 0
 source-bridge 1 1 100
```

Sessions between a device on Token Ring 0 that must go through remote peer 10.1.1.2 use local acknowledgment for LLC2, but sessions that go through remote peer 10.1.1.1 do *not* use local acknowledgment (that is, they “pass through”).

## Related Commands

| Command | Description |
|---|---|
| **source-bridge** | Configures an interface for source-route bridging (SRB). |
| **source-bridge remote-peer fst** | Specifies an FST encapsulation connection. |
| **source-bridge remote-peer frame-relay** | Specifies a point-to-point direct encapsulation connection. |

# source-bridge ring-group

To define or remove a ring group from the configuration, use the **source-bridge ring-group** command in global configuration mode. To cancel previous assignments, use the **no** form of this command.

**source-bridge ring-group** *ring-group* [*virtual-mac-address*]

**no source-bridge ring-group** *ring-group* [*virtual-mac-address*]

## Syntax Description

| | |
|---|---|
| *ring-group* | Ring group number. The valid range is from 1 to 4095. |
| *virtual-mac-address* | (Optional) 12-digit hexadecimal string written as a dotted triple of four-digit hexadecimal numbers (for example, 0010.0a00.20a6). |

## Defaults

No ring group is defined.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

To configure a source-route bridge with more than two network interfaces, the *ring group* arrangement is used. A ring group is a collection of Token Ring interfaces in one or more routers that are collectively treated as a virtual ring. The ring group is denoted by a ring number that must be unique for the network. The ring group's number is used just like a physical ring number, showing up in any route descriptors contained in packets being bridged.

To configure a specific interface as part of a ring group, set its target ring number parameter to the ring group number specified in this command. Do not use the number 0; it is reserved to represent the local ring.

To avoid an address conflict on the virtual MAC address, use a locally administered address in the form 4000.*xxxx.xxxx*.

## Examples

In the following example, multiple Token Rings are source-route bridged to one another through a single router. These Token Rings are all part of ring group seven.

```
! all token rings attached to this bridge/router are part of ring group 7
source-bridge ring-group 7
!
interface tokenring 0
 source-bridge 1000 1 7
!
interface tokenring 1
 source-bridge 1001 1 7
!
interface tokenring 2
 source-bridge 1002 1 7
!
interface tokenring 3
 source-bridge 1003 1 7
```

## Related Commands

| Command | Description |
|---|---|
| **source-bridge** | Configures an interface for SRB. |

# source-bridge route-cache

To enable fast switching, use the **source-bridge route-cache** command in interface configuration mode. To disable fast switching, use the **no** form of this command.

**source-bridge route-cache**

**no source-bridge route-cache**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(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 default, fast-switching software is enabled in the source-route bridging software. Fast switching allows for faster implementations of local source-route bridging between 4 to 16 MB Token Ring cards in the same router. This feature also allows for faster implementations of local source-route bridging between two routers using the 4 to 16 MB Token Ring cards and the direct interface encapsulation.

## Examples

The following example disables use of fast switching between two 4 to 16 MB Token Ring interfaces:

```
interface token 0
 source-bridge 1 1 2
 no source-bridge route-cache
!
interface token 1
 source-bridge 2 1 1
 no source-bridge route-cache
```

## Related Commands

| Command | Description |
|---|---|
| **source-bridge** | Configures an interface for SRB. |

# source-bridge route-cache cbus

To enable autonomous switching, use the **source-bridge route-cache cbus** command in interface configuration mode. To disable autonomous switching, use the **no** form of this command.

**source-bridge route-cache cbus**

**no source-bridge route-cache cbus**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Autonomous switching in source-route bridging software is available for local source-route bridging between ciscoBus Token Ring cards in the same router. Autonomous switching provides higher switching rates than does fast switching between 4 to 16 MB Token Ring cards. Autonomous switching works for both two-port bridges and multiport bridges that use ciscoBus Token Ring cards.

In a virtual ring that includes both ciscoBus Token Ring and 4 to 16 MB Token Ring interfaces, frames that flow from one ciscoBus Token Ring interface to another are autonomously switched, and the remainder of the frames are fast switched. The switching that occurs on the ciscoBus Token Ring interface takes advantage of the high-speed ciscoBus controller processor.

**Note** Using either NetBIOS byte offset access lists or the access-expression capability to logically combine the access filters disables the autonomous or fast switching of source-route bridging (SRB) frames.

## Examples

The following example enables use of autonomous switching between two ciscoBus Token Ring interfaces:

```
interface token 0
 source-bridge 1 1 2
 source-bridge route-cache cbus
 !
interface token 1
 source-bridge 2 1 1
```

```
source-bridge route-cache cbus
```

**Related Commands**

| Command | Description |
|---|---|
| **source-bridge** | Configures an interface for SRB. |

# source-bridge route-cache sse

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

**source-bridge route-cache sse**

**no source-bridge route-cache sse**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

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

## Examples

The following example enables use of SSE switching between two 4 to 16 MB Token Ring interfaces:

```
interface token 0
 source-bridge 1 1 2
 source-bridge route-cache sse
!
interface token 1
 source-bridge 2 1 1
 source-bridge route-cache sse
```

## Related Commands

| Command | Description |
|---|---|
| **source-bridge** | Configures an interface for SRB. |

# source-bridge sap-80d5

To allow non-IBM hosts (attached to a router with 80d5 processing enabled) to use the standard Token Ring to Ethernet LLC2 translation instead of the nonstandard Token Ring to Ethernet 80d5 translation, use the **source-bridge sap-80d5** command in global configuration mode. To disable this feature, use the **no** form of this command.

**source-bridge sap-80d5** *dsap*

**no source-bridge sap-80d5** *dsap*

## Syntax Description

| | |
|---|---|
| *dsap* | Destination service access point (DSAP). |

## 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

This command allows you to set the translation on a per-destination service access point (DSAP) basis.

By default, the following DSAPs are enabled for 0x80d5 translation by specifying the **source-bridge enable-80d5** command:

- For Systems Network Architecture (SNA)—04, 08, 0C, 00
- For NetBIOS—F0

Any of these DSAPs can be disabled with the **no** form of this command.

The parameters specifying the current parameters for the processing of 0x80d5 frames are given at the end of the output of the **show span** command.

**Note** The 80d5 frame processing option is available only with source-route translational bridging (SR/TLB). It is not available when source-route transparent bridging (SRT) is used.

Use the **show span** to verify that 80d5 processing is enabled for a particular DSAP. The following line is displayed in the output if 80d5 processing is enabled, listing each DSAP for which it is enabled:

```
Translation is enabled for the following DSAPs:
 04 0C 1C F0
```

## Examples

The following example enables 0x80d5 processing, removes the translation for SAP 08, and adds the translation for SAP 1c:

```
source-bridge enable-80d5
no source-bridge sap-80d5 08
source-bridge sap-80d5 1c
```

## Related Commands

| Command | Description |
|---|---|
| **show span** | Displays the spanning-tree topology known to the router. |
| **source-bridge enable-80d5** | Changes the Token Ring of the router to Ethernet translation behavior. |

# source-bridge sdllc-local-ack

To activate local acknowledgment for SDLC Logical Link Control. Cisco (SDLLC) sessions on a particular interface, use th**e source-bridge sdllc-local-ack** command in global configuration mode. To deactivate local acknowledgment for SDLLC sessions, use the **no** form of this command.

**source-bridge sdllc-local-ack**

**no source-bridge sdllc-local-ack**

## Syntax Description

This command has no arguments or keywords.

## 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

This command must be issued only on a router with a serial interface. Once the command is issued, *all* SDLLC sessions between the two devices will be locally acknowledged. You cannot selectively choose which SDLLC sessions are to be locally acknowledged and which are not. Also, local acknowledgment is not supported when the Logical Link Control, type 2 (LLC2) station is attached to Ethernet rather than to Token Ring.

**Note** You must use the TCP encapsulation option if you use local acknowledgment for SDLLC.

## Examples

The following example activates local acknowledgment for SDLLC sessions:

```
source-bridge ring-group 100
source-bridge remote-peer 100 tcp 10.108.1.1 local-ack
source-bridge remote-peer 100 tcp 10.108.2.2
source-bridge sdllc-local-ack
```

# source-bridge spanning (automatic)

To enable the automatic spanning-tree function for a specified group of bridged interfaces, use the automatic version of the **source-bridge spanning** command in interface configuration mode. To return to the default disabled state, use the **no** form of this command.

**source-bridge spanning** *bridge-group* [**path-cost** *path-cost*]

**no source-bridge spanning** *bridge-group* [**path-cost** *path-cost*]

## Syntax Description

| | |
|---|---|
| *bridge-group* | Number in the range from 1 to 9 that you choose to refer to a particular group of bridged interfaces. This must be the same number as assigned in the **bridge protocol ibm** command. |
| **path-cost** | (Optional) Assign a path cost for a specified interface. |
| *path-cost* | (Optional) Path cost for the interface. The valid range is from 0 to 65535. |

## Defaults

The automatic spanning-tree function is disabled. The default path cost is 16.

## 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

To return an assigned path cost to the default path cost of 16, use the **no source-bridge spanning path-cost** command.

## Examples

The following example adds Token Ring 0 to bridge group 1 and assigns a path cost of 12 to Token Ring 0:

```
interface tokenring 0
 source-bridge spanning 1 path-cost 12
```

## Related Commands

| Command | Description |
|---|---|
| **bridge protocol ibm** | Creates a bridge group that runs the automatic spanning-tree function. |
| **show source-bridge** | Displays the current source bridge configuration and miscellaneous statistics. |

# source-bridge spanning (manual)

To enable use of spanning explorers, use the **source-bridge spanning** command in interface configuration mode. To disable the use of spanning explorers, use the **no** form of this command.

**source-bridge spanning**

**no source-bridge spanning**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Only spanning explorers will be blocked; everything else will be forwarded. Use of the **source-bridge spanning** command is recommended. This command puts the interface into a forwarding or active state with respect to the spanning tree. Two types of explorer packets are used to collect Routing Information Field (RIF) information:

- All-rings, all-routes explorer packets follow all possible paths to a destination ring. In a worst-case scenario, the number of all-rings explorers generated may be exponentially large.
- Spanning or limited-route explorer packets follow a spanning tree when looking for paths, greatly reducing the number of explorer packets required. There is no dynamic spanning-tree algorithm to establish that spanning tree; it must be manually configured.

## Examples

The following example enables use of spanning explorers:

```
! Global configuration command establishing the ring group for the interface
! configuration commands
source-bridge ring-group 48
!
! commands that follow apply to interface token 0
interface tokenring 0
! configure interface tokenring 0 to use spanning explorers
 source-bridge spanning
```

**Related Commands**

| Command | Description |
|---|---|
| **source-bridge** | Configures an interface for SRB. |

# source-bridge tcp-queue-max

To modify the size of the backup queue for remote source-route bridging, use the **source-bridge tcp-queue-max** command in global configuration mode. To return to the default value, use the **no** form of this command.

**source-bridge tcp-queue-max** *number*

**no source-bridge tcp-queue-max**

## Syntax Description

| | |
|---|---|
| *number* | Number of packets to hold in any single outgoing TCP queue to a remote router. The default is 100 packets. |

## Defaults

The default number of packets is 100.

## 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

This backup queue determines the number of packets that can wait for transmission to a remote ring before packets start being thrown away.

## Examples

If, for example, your network experiences temporary bursts of traffic using the default packet queue length, the following command raises the limit from 100 to 150 packets:

```
source-bridge tcp-queue-max 150
```

# source-bridge transparent

To establish bridging between transparent bridging and source-route bridging (SRB), use the **source-bridge transparent** command in global configuration mode. To disable a previously established link between a source-bridge ring group and a transparent-bridge group, use the **no** form of this command.

**source-bridge transparent** *ring-group pseudoring bridge-number tb-group* [*oui*]

**no source-bridge transparent** *ring-group pseudoring bridge-number tb-group*

## Syntax Description

| | |
|---|---|
| *ring-group* | Virtual ring group created by the **source-bridge ring-group** command. This is the source-bridge virtual ring to associate with the transparent-bridge group. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095. |
| *pseudoring* | Ring number used to represent the transparent bridging domain to the source-route bridged domain. This number must be a unique number, not used by any other ring in your source-route bridged network. |
| *bridge-number* | Bridge number of the bridge that leads to the transparent bridging domain. |
| *tb-group* | Number of the transparent bridge group that you want to tie into your source-route bridged domain. The **no** form of this command disables this feature. |
| *oui* | (Optional) Organizational unique identifier. Values are the following:<br>• **90-compatible**<br>• **standard**<br>• **cisco** |

## Defaults

Not established

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

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

Specify the **90-compatible** keyword oui when talking to Cisco routers. This OUI provides the most flexibility. Specify the **standard** keyword oui when talking to IBM 8209 bridges and other vendor equipment. This oui does not provide for as much flexibility as the other two choices. The **cisco** keyword oui is provided for compatibility with future equipment.

Do not use the **standard** keyword oui 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. Use the **standard** keyword only when you are transferring data between IBM 8209 Ethernet/Token Ring bridges and routers running the source-route translational bridging (SR/TLB) software (to create a Token Ring backbone to connect Ethernets). Use of the **standard** keyword causes the OUI code in Token Ring frames to always be 0x000000. In the context of the **standard** keyword, an OUI of 0x000000 identifies the frame as an Ethernet Type II frame. If the OUI in Token Ring frame is 0x000000 SR/TLB will output an Ethernet Type II frame.

When 8209 compatibility is enabled with the **ethernet transit-oui standard** command, the SR/TLB chooses to translate all Token Ring Subnetwork Access Protocol (SNAP) frames into Ethernet Type II frames as described earlier in this chapter.

## Examples

The following example establishes bridging between a transparent-bridge network and a source-route network:

```
source-bridge ring-group 9
source-bridge transparent 9 6 2 2
!
interface tokenring 0
 source-bridge 5 2 9
!
interface token ring 1
 source bridge 4 2 9
!
interface ethernet 0
 bridge-group 2
!
interface ethernet 1
 bridge-group 2

bridge 2 protocol ieee
```

## Related Commands

| Command | Description |
|---|---|
| **bridge-group** | Assigns each network interface to a bridge group. |
| **ethernet transit-oui standard** | Chooses Organizational Unique Identifier (OUI) code to encapsulate Ethernet Type II frames across Token Ring backbone networks. |
| **source-bridge** | Configures an interface for SRB. |
| **source-bridge ring-group** | Defines or removes a ring group from the configuration. |

# source-bridge transparent fastswitch

To enable fast switching of packets between the source-route bridging (SRB) and transparent domains, use the **source-bridge transparent fastswitch** command in global configuration mode. To disable fast switching of packets, use the **no** form of this command.

**source-bridge transparent** *ring-group* **fastswitch**

**no source-bridge transparent** *ring-group* **fastswitch**

## Syntax Description

| | |
|---|---|
| *ring-group* | Virtual ring group created by the **source-bridge ring-group** command. This is the source-bridge virtual ring to associate with the transparent-bridge group. This ring group number must match the number you have specified with the **source-bridge ring-group** command. The valid range is from 1 to 4095. |
| **fastswitch** | Fast-switched source-route translational bridging (SR/TLB) enables the Cisco IOS software to process packets at the interrupt level. |

## Defaults

Fast-switched SR/TLB is enabled.

## 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

Because fast-switched SR/TLB is enabled by default when the router is configured for SR/TLB, there are no user-specified changes to the operation of the router, and the enabling command does not appear in the configuration.

The **no source-bridge transparent** *ring-group* **fastswitch** command is provided to disable fast-switched SR/TLB, causing the router to handle packets by process switching. When fast-switched SR/TLB is disabled, the **no** form of the command appears on a separate line of the configuration, immediately following the parent **source-bridge transparent** command.

If fast-switched SR/TLB has been disabled, it can be enabled using the **source-bridge transparent** *ring-group* **fastswitch** command, but the enabling form of the command will not appear in the configuration.

## Examples

The following example disables fast-switched SR/TLB between a transparent-bridge network and a source-route network:

```
source-bridge ring-group 9
source-bridge transparent 9 6 2 2
no source-bridge transparent 9 fastswitch
!
interface tokenring 0
 source-bridge 5 2 9
!
interface token ring 1
 source bridge 4 2 9
!
interface ethernet 0
 bridge-group 2
!
interface ethernet 1
 bridge-group 2

bridge 2 protocol ieee
```

## Related Commands

| Command | Description |
|---|---|
| **bridge-group** | Assigns each network interface to a bridge group. |
| **source-bridge** | Configures an interface for SRB. |
| **source-bridge ring-group** | Defines or removes a ring group from the configuration. |

# state-tracks-signal

To allow the channel interface state to track the state of the physical interface signal on a Channel Port Adapter (CPA), use the **state-tracks-signal** command in interface configuration mode. To disable tracking of the physical interface signal on a CPA interface, use the **no** form of this command.

**state-tracks-signal**

**no state-tracks-signal**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The physical interface signal is not tracked.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(4.1) | 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 **state-tracks-signal** command is useful in environments where you are using Hot Standby Router Protocol (HSRP) or Simple Network Management Protocol (SNMP) alerts to monitor channel interface status.

The **state-tracks-signal** command is valid only on channel interfaces which combine the functions of both a physical and virtual interface. The ESCON Channel Port Adapter (ECPA) and Parallel Channel Port Adapter (PCPA) are examples of this type of channel interface. The command is not valid for the Channel Interface Processor (CIP), which has a separate channel interface for the virtual channel functions.

When the **state-tracks-signal** command is used on an interface that has been started by the **no shutdown** command, then the state of the channel interface is reported according to the status of the physical channel interface signal. If the physical channel interface signal is not present, then the channel interface status is DOWN/DOWN.

When the **no state-tracks-signal** command is enabled on the channel interface (the default), and the interface has been started by the **no shutdown** command, the channel interface status is always reported as UP/UP, even when there is no signal present on the physical connection. This configuration is useful for TN3270 server environments that are operating in a mode without any physical channel interface connections.

## Examples

The following example specifies that the channel interface state tracks the physical channel interface signal and reports the channel interface state according to the presence or absence of the physical interface signal when the interface has been started by the **no shutdown** command:

```
interface channel 5/0
 state-tracks-signal
```

# stun group

To place each serial tunnel (STUN)-enabled interface on a router in a previously defined STUN group, use the **stun group** command in interface configuration mode. To remove an interface from a group, use the **no** form of this command.

**stun group** *group-number*

**no stun group** *group-number*

## Syntax Description

| | |
|---|---|
| *group-number* | Integer 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

Before using this command, perform the following steps:

- Enable STUN on a global basis with the **stun peer-name** command.
- Define the protocol group in which you want to place this interface using the **stun protocol-group** command.
- Enable STUN on the interface using the **encapsulation stun** command.

  Packets only travel between STUN-enabled interfaces that are in the same group. Once a given serial link is configured for the STUN function, it is no longer a shared multiprotocol link. All traffic that arrives on the link is transported to the corresponding peer as determined by the current STUN configuration.

## Examples

The following example places serial interface 0 in STUN group 2, which is defined to run the Synchronous Data Link Control (SDLC) transport:

```
! sample stun peer-name global command
stun peer-name 10.108.254.6
! sample protocol-group command telling group 2 to use the SDLC protocol
stun protocol-group 2 sdlc
!
interface serial 0
! sample ip address subcommand
 no ip address
! sample encapsulation stun subcommand
 encapsulation stun
! place interface serial0 in previously defined STUN group 2
 stun group 2
! enter stun route command
 stun route 7 tcp 10.108.254.7
```

## Related Commands

| Command | Description |
|---|---|
| **encapsulation stun** | Enables STUN encapsulation on a specified serial interface. |
| **priority-list protocol stun address** | Establishes STUN queueing priorities based on the address of the serial link. |
| **stun peer-name** | Enables STUN for an IP address. |
| **stun protocol-group** | Creates a protocol group. |

# stun keepalive-count

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

**stun keepalive-count** *count*

**no stun keepalive-count**

## Syntax Description

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

## Defaults

No default behavior or values

## Command Modes

Global configuration

## Command History

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

## Examples

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

```
stun keepalive-count 4
```

## Related Commands

| Command | Description |
|---|---|
| **stun remote-peer-keepalive** | Enables detection of the loss of a peer. |

# stun peer-name

To enable serial tunnel (STUN) for an IP address, use the **stun peer-name** command in global configuration mode. To disable STUN for an IP address, use the **no** form of this command.

**stun peer-name** *ip-address* **cls**

**no stun peer-name** *ip-address* **cls**

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address by which this STUN peer is known to other STUN peers. |
| **cls** | Use Cisco Link Services (CLS) to access the Frame Relay network. |

## Defaults

STUN 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

Use this command to enable any further STUN features. After using this command, perform the following steps:

- Define the protocol group in which you want to place this interface with the **stun protocol-group** command.
- Enable STUN on the interface using the **encapsulation stun** command.
- Place the interface in a STUN group using with the **stun group** command.

## Examples

The following example assigns IP address 10.108.254.6 as the STUN peer:

```
stun peer-name 10.108.254.6 cls
```

## Related Commands

| Command | Description |
|---|---|
| **encapsulation stun** | Enables STUN encapsulation on a specified serial interface. |
| **stun group** | Places each STUN-enabled interface on a router in a previously defined STUN group. |
| **stun protocol-group** | Creates a protocol group. |

# stun protocol-group

To create a protocol group, use the **stun protocol-group** command in global configuration mode. To remove an interface from the group, use the **no** form of this command.

**stun protocol-group** *group-number* {**basic** | **sdlc** [**sdlc-tg**] | **schema**}

**no stun protocol-group**

## Syntax Description

| | |
|---|---|
| *group-number* | Integer in the range from 1 to 255. |
| **basic** | Indicates a non-Synchronous Data Link Control (SDLC) protocol. |
| **sdlc** | Indicates an Synchronous Data Link Control (SDLC) protocol. |
| **sdlc-tg** | (Optional) Identifies the group as part of an Systems Network Architecture (SNA) Transmission Group (TG). |
| **schema** | Indicates a custom protocol. |

## Defaults

No protocol group established.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Use the **sdlc** keyword to specify an SDLC protocol. You must specify either the **sdlc** or the **sdlc-tg** keyword before you can enable SDLC local acknowledgment. SDLC local acknowledgment is established with the **stun route address tcp** command.

Use the **basic** keyword to specify a non-SDLC protocol, such as high-level data link control (HDLC).

Use the **schema** keyword to specify a custom protocol. The custom protocol must have been previously created with the **stun schema** command.

Use the optional **sdlc-tg** keyword, in conjunction with the **sdlc** keyword, to establish an SNA TG. A TG is a set of protocol groups providing parallel links to the same pair of IBM establishment controllers. This provides redundancy of paths. In case one or more links go down, an alternate path will be used. All serial tunnel (STUN) connections in a TG must connect to the same IP address. SDLC local acknowledgment must be enabled.

**Note** If you specify the **sdlc** keyword in the **stun protocol group** command string, you cannot specify the **stun route all** command on that interface.

## Examples

The following example specifies that group 7 will use the Synchronous Data Link Control (SDLC) STUN protocol to route frames within that group:

```
stun protocol-group 7 sdlc
```

The following example specifies that group 5 use the basic protocol, wherein the serial addressing is unimportant and you have a point-to-point link:

```
stun protocol-group 5 basic
```

## Related Commands

| Command | Description |
|---|---|
| **encapsulation stun** | Enables STUN encapsulation on a specified serial interface. |
| **stun route address interface serial** | Forwards all HDLC traffic on a serial interface. |
| **stun route address tcp** | Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for STUN. |
| **stun schema offset length format** | Defines a protocol other than SDLC for use with STUN. |

# stun quick-response

To enable serial tunnel (STUN) quick-response, which can be used with local acknowledgment, use the **stun quick-response** command in global configuration mode. To disable STUN quick-response, use the **no** form of this command.

**stun quick-response**

**no stun quick-response**

## Syntax Description

This command has no arguments or keywords.

## Defaults

STUN quick-response is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.3(5) | 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 with local acknowledgment (local ack).

When STUN quick-response is enabled, the router responds to an exchange identification (XID) or a Set Normal Response Mode (SNRM) request with a Disconnect Mode (DM) response when the device is not in the CONNECT state. The request is then passed to the remote router and, if the device responds, the reply is cached. The next time the device is sent an XID or SNRM, the router replies with the cached DM response.

**Note** Using STUN quick-response avoids an AS/400 line reset problem by eliminating the Non-Productive Receive Timer (NPR) expiration in the AS/400. With quick-response enabled, the AS/400 receives a response from the polled device, even when the device is down. If the device does not respond to the forwarded request, the router continues to respond with the cached DM response.

## Examples

The following example enables STUN quick-response:

```
stun quick-response
```

## Related Commands

| Command | Description |
|---|---|
| **stun route address interface dlci** | Configures direct Frame Relay encapsulation between STUN peers with Synchronous Data Link Control (SDLC) local acknowledgment. |
| **stun route address interface serial** | Forwards all high-level data link control (HDLC) traffic on a serial interface. |
| **stun route address tcp** | Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for STUN. |
| **stun route all interface serial** | Encapsulates and forwards all STUN traffic using HDLC encapsulation on a serial interface. |
| **stun route all tcp** | Used with TCP encapsulation, forwards all STUN traffic on an interface regardless of which address is contained in the serial frame. |

# stun remote-peer-keepalive

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

**stun remote-peer-keepalive** *seconds*

**no stun 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 |
|---|---|
| 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

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

```
stun remote-peer-keepalive 60
```

## Related Commands

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

# stun route address interface dlci

To configure direct Frame Relay encapsulation between serial tunnel (STUN) peers with Synchronous Data Link Control (SDLC) local acknowledgment, use the **stun route address interface dlci** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

**stun route address** *sdlc-addr* **interface** *frame-relay-port* **dlci** *number localsap* **local-ack cls**

**no stun route address** *sdlc-addr* **interface** *frame-relay-port* **dlci** *number localsap* **local-ack cls**

## Syntax Description

| | |
|---|---|
| *sdlc-addr* | Address of the serial interface. |
| *frame-relay-port* | Port number. |
| *number* | Data-link connection identifier (DLCI) number. |
| *localsap* | Local connecting service access point (SAP). |
| **local-ack** | Enable local acknowledgment. |
| **cls** | Use Cisco Link Services (CLS) to access the Frame Relay network. |

## Defaults

The configuration is disabled.

## 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 enables Frame Relay encapsulation between STUN peers with SDLC local acknowledgment:

```
stun route address c1 interface serial1 dlci 22 04 local-ack
```

## Related Commands

| Command | Description |
|---|---|
| **stun route all interface serial** | Encapsulates and forwards all STUN traffic using high-level data link control (HDLC) encapsulation on a serial interface. |

# stun route address interface serial

To forward all high-level data link control (HDLC) traffic on a serial interface, use the **stun route address interface serial** command in interface configuration mode. To disable this method of HDLC encapsulation, use the **no** form of this command.

**stun route address** *address-number* **interface serial** *number* [**direct**]

**no stun route address** *address-number* **interface serial** *number*

## Syntax Description

| | |
|---|---|
| *address-number* | Address of the serial interface. |
| *number* | Number assigned to the serial interface. |
| **direct** | (Optional) Forwards all HDLC traffic on a direct serial tunnel (STUN) link. |

## Defaults

The configuration 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. |

## Examples

In the following example, serial frames with a STUN route address of 4 are forwarded through serial interface 0 using HDLC encapsulation:

```
stun route address 4 interface serial 0
```

In the following example, serial frames with STUN route address 4 are propagated through serial interface 0 using STUN encapsulation:

```
stun route address 4 interface serial 0 direct
```

## Related Commands

| Command | Description |
|---|---|
| **stun route all interface serial** | Encapsulates and forwards all STUN traffic using HDLC encapsulation on a serial interface. |

# stun route address tcp

To specify TCP encapsulation and optionally establish Synchronous Data Link Control (SDLC) local acknowledgment (SDLC transport) for serial tunnel (STUN), use the **stun route address tcp** command in interface configuration mode. To disable this method of TCP encapsulation, use the **no** form of this command.

**stun route address** *address-number* **tcp** *ip-address* [**local-ack**] [**priority**] [**tcp-queue-max**] [**passive**]

**no stun route address** *address-number* **tcp** *ip-address* [**local-ack**] [**priority**] [**tcp-queue-max**] [**passive**]

## Syntax Description

| | |
|---|---|
| *address-number* | Number that conforms to SDLC addressing conventions. |
| *ip-address* | IP address by which this STUN peer is known to other STUN peers that are using the TCP as the STUN encapsulation. |
| **local-ack** | (Optional) Enables local acknowledgment for STUN. |
| **priority** | (Optional) Establishes the four levels used in priority queueing: low, medium, normal, and high. |
| **tcp-queue-max** | (Optional) Sets the maximum size of the outbound TCP queue for the SDLC link. The default is 100. |
| **passive** | (Optional) Prevents the STUN peer from initiating a TCP connection. Normally, the STUN peer connects to the SDLC primary device and initiates a TCP connection to another STUN peer. If the STUN peers connect to non-SDLC devices, such as voice equipment, both STUN peers might try to start a TCP connection at the same time, which can delay the TCP connection setup.<br>The **passive** keyword, used in STUN basic mode, enables this STUN peer to wait for the other STUN peer to initiate the TCP connection. |

## Defaults

TCP encapsulation is not established; TCP queue size default is 100.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 11.1 | The **tcp-queue-max** keyword was added. |
| 12.0 | The **passive** keyword was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

SDLC transport participates in SDLC windowing and resending through support of local acknowledgment. SDLC sessions require that end nodes send acknowledgments for a set amount of data frames received before allowing further data to be sent. Local acknowledgment provides local termination of the SDLC session, so that control frames no longer travel the WAN backbone networks. This means that end nodes do not time out, and a loss of sessions does not occur.

## Examples

In the following example, a frame with a source-route address of 10 is propagated using TCP encapsulation to a device with an IP address of 10.108.8.1:

```
stun route address 10 tcp 10.108.8.1
```

## Related Commands

| Command | Description |
|---|---|
| **sdlc address ff ack-mode** | Configures the IBM reserved address FF as a valid local address. |
| **stun route all tcp** | Used with TCP encapsulation, forwards all STUN traffic on an interface regardless of which address is contained in the serial frame. |

# stun route all interface serial

To encapsulate and forward all serial tunnel (STUN) traffic using high-level data link control (HDLC) encapsulation on a serial interface, use the **stun route all interface serial** command in interface configuration mode. To disable this method of encapsulation, use the **no** form of this command.

**stun route all interface serial** *number* [**direct**]

**no stun route all interface serial** *number* [**direct**]

## Syntax Description

| | |
|---|---|
| *number* | Number assigned to the serial interface. |
| **direct** | (Optional) Indicates that the specified interface is also a direct STUN link, rather than a serial connection to another peer. |

## Defaults

No default behavior or values

## 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

An appropriately configured router must exist on the other end of the designated serial line. The outgoing serial link still can be used for other kinds of traffic (the frame is not TCP encapsulated). This mode is used when TCP/IP encapsulation is not needed or when higher performance is required. Enter the serial line number connected to the router for the *number* argument.

## Examples

In the following example, all traffic on serial interface 0 is propagated using STUN encapsulation:

```
stun route all interface serial 0
```

In the following example, serial interface 1 is a direct STUN link, not a serial connection to another peer:

```
stun route all interface serial 1 direct
```

## Related Commands

| Command | Description |
|---|---|
| **stun route address interface serial** | Forwards all HDLC traffic on a serial interface. |

# stun route all tcp

To forward all serial tunnel (STUN) traffic on an interface regardless of which address is contained in the serial frame, use the **stun route all tcp** command in interface configuration mode with TCP encapsulation. To disable traffic from being forwarded with this method of encapsulation, use the **no** form of this command.

**stun route all tcp** *ip-address* [**passive**]

**no stun route all tcp** *ip-address* [**passive**]

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address by which this remote STUN peer is known to other STUN peers. Use the address that identifies the remote STUN peer that is connected to the remote serial link. |
| **passive** | (Optional) Prevents the STUN peer from initiating a TCP connection. Normally, the STUN peer connects to the Synchronous Data Link Control (SDLC) primary device and initiates a TCP connection to another STUN peer. If the STUN peers connect to non-SDLC devices, such as voice equipment, both STUN peers might start a TCP connection at the same time. The **passive** keyword enables a delay when setting up a TCP connection. |

## Defaults

Disabled

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

TCP/IP encapsulation allows movement of serial frames across arbitrary media types and topologies. This is particularly useful for building shared, multiprotocol enterprise network backbones.

## Examples

In the following example, all STUN traffic received will be propagated through the bridge:

```
stun route all tcp 10.108.10.1
```

# stun schema offset length format

To define a protocol other than Synchronous Data Link Control (SDLC) for use with serial tunnel (STUN), use the **stun schema offset length format** command in global configuration mode. To disable the new protocol, use the **no** form of this command.

**stun schema** *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*

**no stun schema** *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*

## Syntax Description

| | |
|---|---|
| *name* | Name that defines your protocol. It can be up to 20 characters in length. |
| *constant-offset* | Constant offset, in bytes, for the address to be found in the frame. |
| *address-length* | Length in one of the following formats: decimal (4 bytes), hexadecimal (8 bytes), or octal (4 bytes). |
| *format-keyword* | Identifies the format to be used to specify and display addresses for routes on interfaces that use this STUN protocol. Valid format keyword values and their ranges are:<br>• **decimal**—0 to 9<br>• **hexadecimal**—0 to F<br>• **octal**—0 to 7 |

## Defaults

No protocol is defined.

## Command Modes

Global configuration

## Command History

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

## Usage Guidelines

Use this command before defining the protocol group (**stun protocol-group** command). The serial protocol you define must meet the following criteria:

- The protocol uses full-duplex conventions (Request To Send [RTS]/Clear To Send [CTS] always high).
- The protocol uses standard high-level data link control (HDLC) checksum and framing (beginning and end of frames, data between frames).
- Addresses are contained in a constant location (offset) within the frame.
- Addresses are found on a byte boundary.

## Examples

In the following example, a protocol named new-sdlc is created. In the protocol frame structure, the constant offset is 0, the address length is 1 byte, and the address format is hexadecimal.

```
stun schema new-sdlc offset 0 length 1 format hexadecimal
```

## Related Commands

| Command | Description |
|---|---|
| **priority-list protocol stun address** | Establishes STUN queueing priorities based on the address of the serial link. |
| **stun protocol-group** | Creates a protocol group. |

# stun sdlc-role primary

To assign the router the role of Synchronous Data Link Control (SDLC) primary node, use the **stun sdlc-role primary** command in interface configuration mode. To disable the primary node role assignment, use the **no** form of this command.

**stun sdlc-role primary**

**no stun sdlc-role**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No role 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

Primary nodes poll secondary nodes in a predetermined order.

If the router is connected to a cluster controller, for example a 3x74, it should appear as a front-end processor (FEP) such as a 37x5, and must be assigned the role of a primary node.

## Examples

The following example assigns the router the role of SDLC primary node:

```
stun sdlc-role primary
```

## Related Commands

| Command | Description |
|---|---|
| **encapsulation stun** | Enables serial tunnel (STUN) encapsulation on a specified serial interface. |
| **stun sdlc-role secondary** | Assigns the router the role of SDLC secondary node. Secondary nodes respond to polls sent by the SDLC primary by sending any outgoing data they may have. |

# stun sdlc-role secondary

To assign the router the role of Synchronous Data Link Control (SDLC) secondary node, use the **stun sdlc-role secondary** command in interface configuration mode. To disable the assignment, use the **no** form of this command.

**stun sdlc-role secondary**

**no stun sdlc-role**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No secondary role 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

Secondary nodes respond to polls sent by the SDLC primary by sending any outgoing data they may have.

If the router is connected to a front-end processor (FEP), for example a 37x5, it should appear as a cluster controller such as a 3x74, and must be assigned the role of a secondary node.

## Examples

The following example assigns the router the role of SDLC secondary node:

```
stun sdlc-role secondary
```

## Related Commands

| Command | Description |
|---|---|
| **encapsulation stun** | Enables serial tunnel (STUN) encapsulation on a specified serial interface. |
| **stun sdlc-role primary** | Assigns the router the role of SDLC primary node. Primary nodes poll secondary nodes in a predetermined order. |

# subscriber-policy

To define or modify the forward and filter decisions of the subscriber policy, use the **subscriber-policy** command in global configuration mode.

**subscriber-policy** *policy* [[**no** | **default**] *packet* [**permit** | **deny**]]

## Syntax Description

| | |
|---|---|
| *policy* | Subscriber policy number in the range from 1 to 100. |
| **no** | (Optional) Turn off the permit for the packet (this is an equivalent of the **deny** keyword). |
| **default** | (Optional) Deny forwarding of the packet (this is an equivalent of the **deny** keyword). |
| *packet* | (Optional) One of the following packets:<br>• **arp**<br>• **broadcast**<br>• **cdp**<br>• **multicast**<br>• **st**<br>• **unknown unicast** |
| **permit** | (Optional) Permit forwarding of the packet. |
| **deny** | (Optional) Deny forwarding of the packet. |

## Defaults

Table 99 shows the default values that are applied if no forward or filter decisions have been specified for the subscriber policy:

***Table 99 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

As an alternative to the command syntax described, you can enter the **subscriber-policy** *policy* command, followed by the specific forward or filter decisions for each packet.

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

## Examples

The following example changes the Address Resolution Protocol (ARP) behavior and the multicast behavior from permit to deny:

```
subscriber-policy 3 arp deny
subscriber-policy 3 multicast deny
```

The following example changes the ARP behavior and the multicast behavior from permit to deny, using the alternative syntax shown in the usage guidelines section:

```
subscriber-policy 3
arp deny
multicast deny
```

## 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. |

# tcp-port

To override the default TCP port setting of 23, use the **tcp-port** command in TN3270 server, Dependent Logical Unit Requestor (DLUR) physical unit (PU), or PU configuration mode. To restore the default, use the **no** form of this command.

**tcp-port** *port-number*

**no tcp-port**

## Syntax Description

| | |
|---|---|
| *port-number* | A valid TCP port number in the range from 0 to 65534. The default is 23, which is the Internet Engineering Task Force (IETF) standard. The value 65535 is reserved by the TN3270 server. |

## Defaults

TN3270 server configuration mode: 23.

PU configuration mode: the value configured in TN3270 server configuration mode.

## Command Modes

TN3270 server configuration

DLUR PU configuration

PU 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

The **tcp-port** command is valid only on the virtual channel interface, and it can be entered in either TN3270 server, DLUR PU or PU configuration mode. A value entered in TN3270 mode applies to all PUs for that TN3270 server, except as overridden by values entered in PU configuration mode. The **tcp-port** command affects only future TN3270 sessions.

The **tcp-port** command entered in DLUR PU configuration mode applies to all PUs defined under DLUR configuration mode.

The **no tcp-port** command entered in PU configuration mode removes the override. In this mode, the **tcp-port** command applies only to the specified PU.

## Examples

The following example entered in TN3270 server configuration mode returns the TCP port value to 23:

```
no tcp-port
```

**Related Commands**

| Command | Description |
|---|---|
| **pu (listen-point)** | Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode. |
| **pu dlur (listen-point)** | Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode. |

# tg (CMPC)

**Note** Effective with release 12.3(4)T, the **tg (CMPC)** command is no longer available in Cisco IOS software.

To define Logical Link Control (LLC) connection parameters for the Cisco Multipath Channel (CMPC) transmission group, use the **tg** command in interface configuration mode. To remove the specified transmission group from the configuration, which also deactivates the transmission group, use the **no** form of this command.

**tg** *tg-name* **llc** *token-adapter adapter-number lsap* [**rmac** *rmac*] [**rsap** *rsap*]

**no tg** *tg-name* **llc**

## Syntax Description

| | |
|---|---|
| *tg-name* | Name of the CMPC Transmission Group (TG). The maximum length of the name is eight characters. This must match the name specified by the **cmpc** commands. |
| **llc** | Specifies that this TG is connected to the LLC stack on the Cisco Mainframe Channel Connection (CMCC) adapter card. |
| *token-adapter* | Internal adapter type on the CMCC adapter card. The supported type is token-adapter. |
| *adapter-number* | Internal adapter number on the CMCC adapter card, which is the same value specified in the **adapter** internal LAN configuration command. |
| *lsap* | Local service access point (SAP) number, 04 to FC, in hexadecimal. The value must be an even number and should be a multiple of four. It must be unique within the internal adapter in that no other IEEE 802.2 clients of that adapter, in the router or in a host, can use the same SAP. The default value is 04. |
| **rmac** *rmac* | (Optional) Remote MAC address of the form *xxxx.xxxx.xxxx* in hexadecimal. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed. |
| **rsap** *rsap* | (Optional) Remote SAP address, 04 to FC in hexadecimal. The value for the *rsap* argument must be an even number and should be a multiple of 4, but this requirement is not enforced. The default value for the *rsap* argument is 04. |

## Defaults

The *lsap* and *rsap* values default to 04.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.3(4)T | This command was removed and is no longer available in Cisco IOS software. |
| 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 **tg** (CMPC) command is valid only on the virtual channel interface. This command defines an LLC connection with a complete addressing 4-tuple. The *lsap*, *rmac*, and *rsap* arguments are specified explicitly by parameters. The *lmac* argument is the local MAC address of the adapter referred to by the *type* and *adapter-number* arguments.

To change any parameter of the **tg** (CMPC) command, first remove the existing TG by using the **no tg** command.

The **no tg** command removes the CMPC TG from the configuration. If the TG is used for a High-Performance Routing (HPR) connection, all sessions using the TG will be terminated immediately. If the TG is an HPR connection, all sessions using the TG will be terminated if no other HPR connection is available to the host.

## Examples

The following example configures a TG name and includes values for the *rmac* and *rsap* arguments:

```
tg LAGUNAA llc token-adapter 1 18 rmac 4000.0000.beef rsap 14
```

## Related Commands

| Command | Description |
|---|---|
| **adapter** | Configures internal adapters. |
| **lan** | Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode. |

# tg (CMPC+)

To define IP connection parameters for the Cisco Multipath Channel (CMPC+) transmission group, use the **tg** command in interface configuration mode. To remove the specified transmission group from the configuration and deactivate the transmission group, use the **no** form of this command.

**tg** *tg-name* {**ip** | **hsas-ip**} *host-ip-addr local-ip-addr* [**broadcast**]

**no tg** *tg-name* {**ip** | **hsas-ip**}

## Syntax Description

| | |
|---|---|
| *tg-name* | Name of the CMPC+ Transmission Group (TG). The maximum length of the name is eight characters. This name must match the name specified on the **cmpc** statements. |
| **ip** | Specifies that this TG is connected to the TCP/IP stack. |
| **hsas-ip** | Specifies that this TG is connected to the High Speed Access Services (HSAS) IP stack. |
| *host-ip-addr* | Specifies the IP address of the channel-attached host using this TG. A host may have more than one IP stack, therefore this is the IP address of the host IP stack as indicated by the HOME statement in the host TCP/IP profile. For HSAS, this address is the host address as indicated by the *source-IP-address* argument of the **oeifconfig** command. |
| *local-ip-addr* | This address must match an IP address configured on the virtual interface. Specifies the IP address of the router to be used for this TG. This is the IP address of the router as indicated by the DEFAULTNET statement in the host TCP/IP profile. For HSAS, this address is the router IP address as indicated by the *destination-IP-address* argument of the **oeifconfig** command. |
| **broadcast** | (Optional) Enables the sending of routing updates to the host. |

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)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

The **tg** (CMPC+) command is valid only on the Channel Interface Processor's (CIP) virtual channel interface and the Channel Port Adapter's (CPA) physical channel interface. This command defines either an IP connection or an HSAS IP connection.

To change any parameter of the **tg** (CMPC+) command, first remove the existing TG must be removed first by using **no tg** *name* command. At a minimum, *tg-name* must be specified to avoid ambiguity.

The **no tg** command removes the CMPC+ TG from the configuration. All sessions using the TG are terminated immediately.

## Examples

The following example configures a TG name for an HSAS stack configured with CMPC+:

```
interface Channel0/2
 ip address 10.12.165.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip route-cache same-interface
 no ip mroute-cache
 no keepalive
 tg TG00 hsas-ip 10.12.165.2 10.12.165.1
```

The following example configures a TG name for an IP stack configured with CMPC+:

```
interface Channel0/2
 ip address 10.12.165.1 255.255.255.0
 no ip redirects
 no ip directed-broadcast
 ip route-cache same-interface
 no ip mroute-cache
 no keepalive
 tg TG00 ip 10.12.165.2 10.12.165.1
```

## Related Commands

| Command | Description |
|---|---|
| **cmpc** | Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel. |

# tg delay

To configure the duration of time the router is to wait before ending an Multi-Path Channel (MPC) block and sending it to the host, use the **tg delay** command in interface configuration mode. To restore the default duration of time, use the **no** form of this command.

**tg** *tg-name* **delay** *delay*

**no tg** *tg-name* **delay**

## Syntax Description

| | |
|---|---|
| *tg-name* | Name of the Cisco Multipath Channel (CMPC+) Transmission Group (TG). The maximum length of the name is eight characters. This name must match the name specified by the **cmpc** commands. |
| *delay* | Duration of delay in milliseconds. Allowed values are from 0 to 20. The default is 10 milliseconds. |

## Defaults

10 milliseconds

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(11)T | This command was introduced. |

## Usage Guidelines

By default, the **tg delay** command does not appear in the running configuration. It is displayed in the configuration only when configured for a value that is not default.

## Examples

The following example configures a TG delay of 20 milliseconds:

```
router(config)# interface channel 0/2
router(config-if)# tg TG00 delay 20
```

The following example resets the TG delay to the default of 10 milliseconds:

```
router(config-if)# no tg TG00 delay
```

## Related Commands

| Command | Description |
|---|---|
| **cmpc** | Configures a CMPC (or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel. |

# timing-mark

To select whether a WILL TIMING-MARK is sent when the host application needs a Systems Network Architecture (SNA) response (definite or pacing response), use the **timing-mark** command in TN3270 server configuration mode. To turn off WILL TIMING-MARK transmission except as used by the keepalive function, use the **no** form of this command.

**timing-mark**

**no timing-mark**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No WILL TIMING-MARKS are sent except by keepalive.

## Command Modes

TN3270 server 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

If the **timing-mark** command is configured, the TN3270 server will send WILL TIMING-MARK as necessary to achieve an end-to-end response protocol. Specifically, TIMING-MARK will be sent if either of the following conditions is true:

- The host application has requested a pacing response.
- The host application has requested a Definite Response, and either the client is not using TN3270E, or the request is not Begin Chain.

The use of the **timing-mark** command can degrade performance. Some clients do not support the **timing-mark** command used in this way. Therefore, the **timing-mark** command should be configured only when both of the following conditions are true:

- All clients support this usage.
- The application benefits from end-to-end acknowledgment.

## Examples

The following example enables the sending of the TIMING-MARK:

```
timing-mark
```

**Related Commands**

| Command | Description |
|---|---|
| **idle-time** | Specifies how many seconds of logical unit (LU) inactivity, from both host and client, before the TN3270 session is disconnected. |
| **keepalive (TN3270)** | Specifies how many seconds of inactivity elapse before transmission of a DO TIMING-MARK or Telnet no operation (nop) to the TN3270 client. |

# tn3270-server

To start the TN3270 server on a Cisco Mainframe Channel Connection (CMCC) adapter or to enter TN3270 server configuration mode, use the **tn3270-server** command in interface configuration mode. To remove the existing TN3270 server configuration, use the **no** form of this command.

**tn3270-server**

**no tn3270-server**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No TN3270 server function is enabled.

## Command Modes

Interface 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

The **tn3270-server** command is valid only on the virtual channel interface. Only one TN3270 server can run on a CMCC adapter. It will always be configured on a virtual channel interface.

The **no tn3270-server** command shuts down TN3270 server immediately. All active sessions will be disconnected and all Dependent Logical Unit Requestor (DLUR) and physical unit (PU) definitions deleted from the router configuration. To restart a TN3270 server, you must reconfigure all parameters.

## Examples

The following example starts the TN3270 server and enters TN3270 server configuration mode:

```
tn3270-server
```

# unbind-action

To select what action to take when the TN3270 server receives an UNBIND request, use the **unbind-action** command in TN3270 server configuration mode. To restore the default, use the **no** form of this command.

**unbind-action** {**keep** | **disconnect**}

**no unbind-action**

## Syntax Description

| | |
|---|---|
| **keep** | No automatic disconnect will be made by the server on receipt of an UNBIND. |
| **disconnect** | Session will be disconnected upon receipt of an UNBIND. |

## Defaults

In TN3270 server configuration mode, the default is **disconnect**.
In physical unit (PU) configuration mode the default is the value configured in TN3270 server configuration mode.

## Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU 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

The **unbind-action** command is valid only on the virtual channel interface. The **unbind-action** command affects active and future TN3270 sessions.

In TN3270 server configuration mode, the **unbind-action** command applies to all PUs for that TN3270 server, except as overridden by values entered in PU configuration mode.

In listen-point configuration mode, the **unbind-action** command applies to all PUs defined at the listen point.

In DLUR PU configuration mode, the **unbind-action** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **unbind-action** command applies only to the specified PU. The **no unbind-action** command entered in PU configuration mode removes the override.

## Examples

The following example prevents automatic disconnect:

```
unbind-action keep
```

# vrn

To tell the Systems Network Architecture (SNA) session switch the connection network to which the internal adapter interface on the Cisco Mainframe Channel Connection (CMCC) adapter belongs, use the **vrn** Dependent Logical Unit Requestor (DLUR) service access point (SAP) configuration command. To remove a network name, use the **no** form of this command.

**vrn** *vrn-name*

**no vrn**

## Syntax Description

| | |
|---|---|
| *vrn-name* | Fully qualified name of the connection network. |

## Defaults

The adapter is not considered to be part of a connection network.

## Command Modes

DLUR SAP 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

The **vrn** command is valid only on the virtual channel interface. This command is used to discover routes without having to configure all possible links.

A connection network is also known as a shared-access transport facility (SATF), which means, at the MAC level, that all nodes in the network can reach each other using the same addressing scheme and without requiring the services of SNA session routing. A bridged LAN (whether source-route or transparent) is an example. Such a network is represented in the Advanced Peer-to-Peer Networking (APPN) topology as a kind of node, termed a virtual routing node (VRN).

To make use of this function, all APPN nodes must use the same VRN name for the SATF.

Refer to the virtual telecommunications access method (VTAM) operating system documentation for your host system for additional information regarding the VTAM VNGROUP and VNNAME parameters on the PORT statement of an XCA major node.

Several parameters in the DLUR configuration mode consist of fully qualified names, as defined by the APPN architecture. Fully qualified names consist of two case-insensitive alphanumeric strings, separated by a period. However, for compatibility with existing APPN products, including VTAM, the characters “#” (pound), “@” (at), and “$” (dollar) are allowed in the fully qualified name strings. Each string is from one to eight characters long; for example, RA12.NODM1PP. The portion of the name before the period is the network entity title (NET) ID and is shared between entities in the same logical network.

## Examples

The following example sets a VRN name:

```
vrn SYD.BLAN25
```

## Related Commands

| Command | Description |
|---|---|
| **client pool** | Nails clients to pools. |
| **adapter** | Configures internal adapters. |
| **lan** | Configures an internal LAN on a CMCC adapter interface and enters the internal LAN configuration mode. |
| **lsap** | Creates a service access point (SAP) in the SNA session switch and enters DLUR SAP configuration mode. |

# x25 map qllc

To specify the X.121 address of the remote X.25 device with which you plan to communicate using Qualified Logical Link Control (QLLC) conversion, use the **x25 map qllc** command in interface configuration mode. To disable QLLC conversion to this X.121 address, use the **no** form of this command.

**x25 map qllc** *virtual-mac-addr x121-addr* [**cud** *cud-value*] [*x25-map-options*]

**no x25 map qllc** *virtual-mac-addr x121-addr* [**cud** *cud-value*] [*x25-map-options*]

## Syntax Description

| | |
|---|---|
| *virtual-mac-addr* | Virtual MAC address. |
| *x121-addr* | X.121 address of the remote X.25 device you are associating with this virtual MAC address. It can be from 1 to 15 digits long. |
| **cud** cud-value | (Optional) Override of the standard Call User Data (CUD) value for outbound switched virtual circuits (SVCs). The value can range from 1 to 4 hex bytes. |
| *x25-map-options* | (Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in Table 100. |

## Defaults

No association is made.

## 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

The central notion that binds the QLLC conversion interface to the X.25 and source-route bridging (SRB) facilities is the X.25 address map. For each remote client an X.121 address is associated with a virtual MAC address. The rest of the configuration is specified by using the virtual Token Ring address to refer to the connection.

When a Token Ring device wants to open communications with another device, it will send the request to the address it knows, which is the MAC address. The Cisco IOS software accepts this connection request and must transform it into a known X.121 address. The **x25 map qllc** command matches the MAC address with the X.121 address.

You must enter a mapping for each X.25 device with which the router will exchange traffic.

All QLLC conversion commands use the *virtual-mac-addr* argument that you define with the **x25 map qllc** command to refer to the connection.

You use the **x25 map qllc** command in conjunction with the **qllc srb** command.

Table 100 shows the possible values for the *x25-map-options* argument.

***Table 100 x.25 map qllc Options***

| Option | Description |
|---|---|
| **compress** | Specifies that X.25 payload compression be used for mapping the traffic to this host. Each virtual circuit established for compressed traffic uses a substantial amount of memory (for a table of learned data patterns) and for computation (for compression and decompression of all data). Cisco recommends that compression be used with careful consideration to its impact on overall performance. |
| **method** {**cisco** \| **ietf** \| **snap** \| **multi**} | Specifies the encapsulation method. The choices are as follows:<br>• **cisco**—Cisco's proprietary encapsulation; not available if more than one protocol is to be carried.<br>• **ietf**—Default RFC 1356 operation: Protocol identification of single-protocol virtual circuits and protocol identification within multiprotocol virtual circuits uses the standard encoding, which is compatible with RFC 877. Multiprotocol virtual circuits are used only if needed.<br>• **snap**—RFC 1356 operation where IP is identified with Subnetwork Access Protocol (SNAP) rather than the standard Internet Engineering Task Force (IETF) method (the standard method is compatible with RFC 877).<br>• **multi**—Forces a map that specifies a single protocol to set up a multiprotocol virtual circuit when a call is originated; also forces a single-protocol permanent virtual circuit (PVC) to use multiprotocol data identification methods for all datagrams sent and received. |
| **no-incoming** | Use the map only to originate calls. |
| **no-outgoing** | Do not originate calls when using the map. |
| **idle** *minutes* | Specifies an idle timeout for calls other than the interface default; 0 minutes disables the idle timeout. |
| **reverse** | Specifies reverse charging for outgoing calls. |
| **accept-reverse** | Causes the Cisco IOS software to accept incoming reverse-charged calls. If this option is not present, the Cisco IOS software clears reverse-charged calls unless the interface accepts all reverse-charged calls. |
| **broadcast** | Causes the Cisco IOS software to direct any broadcasts sent through this interface to the specified X.121 address. This option also simplifies the configuration of OSPF; see the "Usage Guidelines" section for more detail. |
| **cug** *group-number* | Specifies a closed user group number (from 1 to 99) for the mapping in an outgoing call. |
| **nvc** *count* | Sets the maximum number of virtual circuits for this map or host. The default *count* is the **x25 nvc** setting of the interface. A maximum number of eight virtual circuits can be configured for each map. Compressed TCP may use only one virtual circuit. |

*Table 100 x.25 map qllc Options (continued)*

| Option | Description |
|---|---|
| **packetsize** *in-size out-size* | Proposes maximum input packet size (*in-size*) and maximum output packet size (*out-size*) for an outgoing call. Both values typically are the same and must be one of the following values: 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. |
| **windowsize** *in-size out-size* | Proposes the packet count for input window (*in-size*) and output window (*out-size*) for an outgoing call. Both values typically are the same, must be in the range from 1 to 127, and must be lower than the value set by the **x25 modulo** command. |
| **throughput** *in out* | Sets the requested throughput class values for input (*in*) and output (*out*) throughput across the network for an outgoing call. Values for *in* and *out* are in bits per second (bps) and range from 75 to 48000 bps. |
| **transit-delay** *milliseconds* | Specifies the transit delay value in milliseconds (0 to 65534) for an outgoing call, for networks that support transit delay. |
| **nuid** *username password* | Specifies that a network user ID (NUID) facility be sent in the outgoing call with the specified Terminal Access Controller Access Control System (TACACS) username and password (in a format defined by Cisco). This option should be used only when connecting to another Cisco router. The combined length of the username and password must not exceed 127 characters. |
| **nudata** *string* | Specifies the network user identification in a format determined by the network administrator (as allowed by the standards). This option is provided for connecting to non-Cisco equipment that requires an NUID facility. The string must not exceed 130 characters and must be enclosed in quotation marks (“ ”) if any spaces are present. |
| **roa** *name* | Specifies the name defined by the **x25 roa** command for a list of transit Recognized Operating Agencies (ROAs) to use in outgoing Call Request packets. |
| **passive** | Specifies that the X.25 interface should send compressed outgoing TCP datagrams only if they were already compressed when they were received. This option is available only for compressed TCP maps. |

## Examples

In the following example, the **x25 map qllc** command is used to associate the remote X.25 device at X.121 address 31104150101 with the virtual MAC address 0100.000.0001:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
```

## Related Commands

| Command | Description |
|---|---|
| **qllc accept-all-calls** | Enables the router to accept a call from any remote X.25 device. |
| **qllc srb** | Enables Qualified Logical Link Control (QLLC) conversion on a serial interface configured for X.25 communication. |

# x25 pvc qllc

To associate a virtual MAC address with a permanent virtual circuit (PVC) for communication using Qualified Logical Link Control (QLLC) conversion, use the **x25 pvc qllc** command in interface configuration mode. To remove the association, use the **no** form of this command.

**x25 pvc** *circuit* **qllc** *x121-address* [*x25-map-options*]

**no x25 pvc** *circuit* **qllc** *x121-address* [*x25-map-options*]

## Syntax Description

| | |
|---|---|
| *circuit* | PVC you are associating with the virtual MAC address. This must be lower than any number assigned to switched virtual circuits. |
| *x121-address* | X.121 address. |
| *x25-map-options* | (Optional) Additional functionality that can be specified for originated calls. Can be any of the options listed in Table 100. |

## Defaults

No association is made.

## 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 a Token Ring device wants to communicate with another device, it will send the request to the address it knows, which is the MAC address. The Cisco IOS software accepts this connection request and transforms it into the known X.121 address and virtual circuit. You must use the **x25 map qllc** command to specify the required protocol-to-X.121 address mapping before you use the **x25 pvc qllc** command. The **x25 map qllc** command associates the MAC address with the X.121 address, and the **x25 pvc qllc** command further associates that address with a known PVC.

You use the **x25 pvc** command in conjunction with the **x25 map qllc** and **qllc srb** commands.

## Examples

In the following example, the **x25 pvc qllc** command associates the virtual MAC address 0100.0000.0001, as defined in the previous **x25 map qllc** command entry, with PVC 3:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 x25 pvc 3 qllc 0100.0000.0001
```

**Related Commands**

| Command | Description |
|---|---|
| **qllc srb** | Enables QLLC conversion on a serial interface configured for X.25 communication. |
| **x25 map qllc** | Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion. |