sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI)

To enable Systems Network Architecture (SNA) on the interface, use the **sna enable-host** command in interface configuration mode. To disable SNA on the interface, use the **no** form of this command.

sna enable-host [**lsap** *lsap-address*]

no sna enable-host [**lsap** *lsap-address*]

Syntax Description

lsap	(Optional) Activate a local service access point (SAP) as an upstream SAP, for both receiving ConnectIn attempts and for starting ConnectOut attempts.
lsap-address	(Optional) The default is 12.

Defaults

The default LSAP parameter is 12.

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 example enables SNA on the interface and specifies that the local SAP (LSAP) 10 will be activated as an upstream SAP:

```
sna enable-host lsap 10
```

Related Commands

Command	Description
show sna	Displays the status of the SNA Service Point feature.
sna host (Frame Relay)	Defines a link to an SNA host over a Frame Relay connection.
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.

sna enable-host (QLLC)

To enable an X.121 subaddress for use by the Systems Network Architecture (SNA) Service Point feature on the interface, use the **sna enable-host** command in interface configuration mode. To disable SNA Service Point on the interface, use the **no** form of this command.

sna enable-host qllc *x121-subaddress*

no sna enable-host qllc *x121-subaddress*

Syntax Description

qllc	Required keyword for Qualified Logical Link Control (QLLC) data-link control.
x121-subaddress	X.121 subaddress.

Defaults

No default X.121 subaddress is specified.

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

In the following example, X.121 subaddress 320108 is enabled for use by host connections:

```
sna enable-host qllc 320108
```

Related Commands

Command	Description
sna host (QLLC)	Defines a link to an SNA host over an X.25/QLLC connection.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.

sna enable-host (SDLC)

To enable a Synchronous Data Link Control (SDLC) address for use by host connections, use the **sna enable-host** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

sna enable-host sdlc *sdlc-address*

no sna enable-host sdlc *sdlc-address*

Syntax Description

sdlc	Required keyword for SDLC data-link control.
sdlc-address	SDLC address.

Defaults

No default SDLC address is specified.

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

In the following example, SDLC address C1 is enabled for use by host connections:

```
encapsulation sdlc
sdlc role secondary
sdlc address c1
sna enable-host sdlc c1
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
sna host (SDLC)	Defines a link to a Systems Network Architecture (SNA) host over an SDLC connection.

sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)

To define a link to a Systems Network Architecture (SNA) host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control connections, use the **sna host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna host *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no sna host *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	SNA host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
rmac *remote-mac*	MAC address of the remote host physical unit (PU).
rsap *remote-sap*	(Optional) Service access point (SAP) address of the remote host PU. The default is 4.
lsap *local-sap*	(Optional) local SAP (LSAP) address used by the SNA Service Point to establish connection with the remote host. The default is 12.
interface *slot/port*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with the remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between attempts to retry establishing connection with the remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Host link to be used for the focal point support.

Defaults

The default remote SAP is 4.
The default local SAP is 12.
The default window size is 7.
The default maximum I-frame size is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes Global configuration

Command History

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

Examples The following example defines a link to a Systems Network Architecture (SNA) host:

```
sna host CNM01 xid-snd 05d00001 rmac 4001.3745.1088 rsap 4 lsap 4 focalpoint
```

Related Commands

Command	Description
sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI)	Enables SNA on the interface.
sna rsrb enable-host	Enables an RSRB service access point (SAP) for use by the SNA Service Point feature.
sna rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by the host name through the RSRB.
sna start	Initiates a connection to a remote resource.
sna vdlc enable-host	Enables a SAP for use by the SNA Service Point feature.
sna vdlc start	Specifies that an attempt will be made to connect to the remote resource defined by the host name through virtual data-link control (VDLC).

sna host (Frame Relay)

To define a link to a Systems Network Architecture (SNA) host over a Frame Relay connection, use the **sna host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna host *host-name* **xid-snd** *xid* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no sna host *host-name* **xid-snd** *xid* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	Specified SNA host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
dlci *dlci-number*	Data-link connection identifier (DLCI) number.
rsap *remote-sap*	(Optional) Service access point (SAP) address of the remote host physical unit (PU). The default is 4.
lsap *local-sap*	(Optional) local SAP (LSAP) address used by the SNA Service Point to establish connection with the remote host. The default is 12.
interface *slot/port*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with the remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between attempts to retry establishing connection with the remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Host link to be used for the focal point support.

Defaults

The default remote SAP is 4.
The default local SAP is 12.
The default window size is 7.
The default maximum I-frame size is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes Global configuration

Command History

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

Examples The following example defines a link to a Systems Network Architecture (SNA) host:

```
sna host CNM01 xid-snd 05d00001 dlci 200 rsap 4 lsap 4
```

Related Commands

Command	Description
sna enable-host (Token Ring, Ethernet, Frame Relay, FDDI)	Enables SNA on the interface.
sna start	Initiates a connection to a remote resource.

sna host (QLLC)

To define a link to a Systems Network Architecture (SNA) host over an X.25 or Qualified Logical Link Control (QLLC) connection, use the **sna host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna host *host-name* **xid-snd** *xid* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**interface** *slot/port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no sna host *host-name* **xid-snd** *xid* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**interface** *slot/port]* [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	SNA host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
x25 *remote-x121-addr*	Synchronous Data Link Control (SDLC) address.
qllc *local-x121-subaddr*	(Optional) Service access point (SAP) address of the remote host physical unit (PU). The default is 4.
interface *slot/port*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with the remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between attempts to retry establishing connection with the remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Host link to be used for the focal point support.

Defaults

The default remote SAP is 4.
The default window size is 7.
The default maximum I-frame size is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

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

Examples

The following example defines a link to a Systems Network Architecture (SNA) host:

```
sna host MLM1 xid-snd 05d00001 x25 320108 qllc 08
```

Related Commands

Command	Description
sna enable-host (QLLC)	Enables an X.121 subaddress for use by the SNA Service Point feature on the interface.
sna start	Initiates a connection to a remote resource.

sna host (SDLC)

To define a link to a Systems Network Architecture (SNA) host over an Synchronous Data Link Control (SDLC) connection, use the **sna host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna host *host-name* **xid-snd** *xid* **sdlc** *sdlc-addr* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot*/*port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no sna host *host-name* **xid-snd** *xid* **rmac** *remote-mac* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**interface** *slot*/*port*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	SNA host.
xid-snd *xid*	Exchange identification (XID) that will be sent to the host during connection establishment. The XID value is eight hexadecimal digits that include both block and ID numbers. For example, if the XID value is 05D00001, the block number is 05D and the ID number is 00001.
sdlc *sdlc-addr*	SDLC address.
rsap *remote-sap*	(Optional) Service access point (SAP) address of the remote host physical unit (PU). The default is 4.
lsap *local-sap*	(Optional) local SAP (LSAP) address used by the SNA Service Point to establish connection with the remote host. The default is 12.
interface *slot*/*port*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive window sizes used for the host link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Send and receive maximum I-frame sizes used for the host link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the SNA Service Point attempts to retry establishing connection with the remote host PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 255.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between attempts to retry establishing connection with the remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Host link to be used for the focal point support.

Defaults

The default remote SAP is 4.
The default local SAP is 12.
The default window size is 7.
The default maximum I-frame size is 1472.
The default retry count is 255.
The default retry timeout is 30 seconds.

Command Modes Global configuration

Command History

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

Examples The following example defines a link to a Systems Network Architecture (SNA) host:

```
sna host CNM01 xid-snd 05d00001 sdlc c1 rsap 4 lsap 4 focalpoint
```

Related Commands

Command	Description
sna enable-host (SDLC)	Enables an Synchronous Data Link Control (SDLC) address for use by host connections.
sna start	Initiates a connection to a remote resource.

sna rsrb

To specify the entities that the Systems Network Architecture (SNA) feature will simulate at the remote source-route bridge (RSRB), use the **sna rsrb** command in interface configuration mode. To cancel the specification, use the **no** form of this command.

sna rsrb *local-virtual-ring bridge-number target-virtual-ring virtual-macaddr*

no sna rsrb *local-virtual-ring bridge-number target-virtual-ring virtual-macaddr*

Syntax Description

local-virtual-ring	Local virtual ring number.
bridge-number	Virtual bridge number. The valid range is from 1 to 15.
target-virtual-ring	Target virtual ring number.
virtual-macaddr	Virtual MAC address.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can specify the bridge number no more than once in any configuration.

Examples

The following example identifies a LAN:

```
sna rsrb 88 1 99 4000.FFFF.0001
```

Related Commands

Command	Description
sna rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by the host name through the remote source-route bridging (RSRB).

sna rsrb enable-host

To enable an remote source-route bridging (RSRB) service access point (SAP) for use by the Systems Network Architecture (SNA) Service Point feature, use the **sna rsrb enable-host** command in global configuration mode. To disable the RSRB SAP, use the **no** form of this command.

sna rsrb enable-host [**lsap** *local-sap*]

no sna rsrb enable-host [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP (LSAP) address will be activated as an upstream SAP for both receiving incoming connections attempts and for starting outgoing connection attempts. The default is 12.

Defaults

The default local SAP address is 12.

Command Modes

Global configuration

Command History

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

Examples

In the following example, the local SAP address 10 of the RSRB is enabled for use by the ibm3745 host physical unit (PU):

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

sna rsrb 88 1 99 4000.FFFF.0001
sna rsrb enable-host lsap 10

sna host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections.

sna rsrb start

To specify that an attempt will be made to connect to the remote resource defined by the host name through the remote source-route bridging (RSRB), use the **sna rsrb start** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna rsrb start *host-name*

no sna rsrb start *host-name*

Syntax Description

host-name	The name of a host defined in an **sna host** or equivalent command.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Usage Guidelines

Before issuing this command, you must enable the correct local service access point (SAP) with the appropriate enable command (**sna rsrb enable-host**).

Examples

In the following example, the Systems Network Architecture (SNA) Service Point will initiate a connection with the ibm3745 host physical unit (PU) across the RSRB link:

```
source-bridge ring-group 99
source-bridge remote-peer 99 tcp 10.10.13.1
source-bridge remote-peer 99 tcp 10.10.13.2

sna rsrb 88 1 99 4000.FFFF.0001
sna rsrb enable-host lsap 10

sna host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10
sna rsrb start ibm3745

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
sna rsrb	Specifies the entities that the SNA feature will simulate at the RSRB.

sna start

To initiate a connection to a remote resource, use the **sna start** command in interface configuration mode. To cancel the connection attempt, use the **no** form of this command.

sna start [*resource-name*]

no sna start [*resource-name*]

Syntax Description

resource-name	(Optional) Name of a host defined in an **sna host** command.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Before issuing this command, you must enable the correct address using the **sna enable-host** command.

Examples

The following example initiates a connection to CNM01:

```
sna start CNM01
```

Related Commands

Command	Description
sna host (Frame Relay)	Defines a link to a Systems Network Architecture (SNA) host over a Frame Relay connection.
sna host (QLLC)	Defines a link to an SNA host over an X.25 or Qualified Logical Link Control (QLLC) connection.
sna host (SDLC)	Defines a link to an SNA host over an Synchronous Data Link Control (SDLC) connection.
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.

sna vdlc

To identify the local virtual ring and virtual MAC address that will be used to establish Systems Network Architecture (SNA) host connections over data-link switching plus (DLSw+) using virtual data-link control, use the **sna vdlc** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna vdlc *ring-group virtual-mac-address*

no sna vdlc *ring-group virtual-mac-address*

Syntax Description

ring-group	Local virtual ring number identifying the source-route bridging (SRB) ring group.
virtual-mac-address	Virtual MAC address that represents the SNA virtual data-link control.

Defaults

No default behavior or values

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

The virtual data-link control local virtual ring must have been previously configured using the **source-bridge ring-group** command.

The virtual data-link control virtual MAC address must be unique within the DLSw+ network.

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

Examples

The following is an example of an SNA Service Point configuration that uses virtual data-link control over DLSw+:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

sna vdlc 99 4000.4500.01f0
sna vdlc enable-host lsap 12

sna host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint
```

```
sna vdlc start HOST-B

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
dlsw local-peer	Defines the parameters of the DLSw+ local peer.
dlsw remote-peer tcp	Identifies the IP address of a peer with which to exchange traffic using TCP.
sna vdlc start	Specifies that an attempt will be made to connect to the remote resource defined by the host name through virtual data-link control (VDLC).
source-bridge ring-group	Defines or removes a ring group from the configuration.

sna vdlc enable-host

To enable a service access point (SAP) for use by the Systems Network Architecture (SNA) Service Point feature, use the **sna vdlc enable-host** command in global configuration mode. To disable the SAP, use the **no** form of this command.

sna vdlc enable-host [**lsap** *local-sap*]

no sna vdlc enable-host [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP (LSAP) address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts. The default is 12.

Defaults

The default local SAP address is 12.

Command Modes

Global configuration

Command History

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

Examples

In the following example, the local SAP address 12 is enabled for use by the host physical unit (PU) HOST-B:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

sna vdlc 99 4000.4500.01f0
sna vdlc enable-host lsap 12

sna host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint

sna vdlc start HOST-B

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
sna host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a link to an SNA host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.

sna vdlc start

To specify that an attempt will be made to connect to the remote resource defined by the host name through virtual data-link control (VDLC), use the **sna vdlc start** command in global configuration mode. To cancel the definition, use the **no** form of this command.

sna vdlc start *host-name*

no sna vdlc start *host-name*

Syntax Description

host-name	The name of a host defined in an **sna host** or equivalent command.

Defaults

No default behavior or values

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

Before issuing this command, you must enable the correct local service access point (SAP) with the **sna vdlc enable-host** command.

Examples

In the following example, the Systems Network Architecture (SNA) Service Point feature uses virtual data-link control to initiate a connection with the host physical unit (PU) HOST-B:

```
source-bridge ring-group 99
dlsw local-peer peer-id 10.10.16.2
dlsw remote-peer 0 tcp 10.10.16.1

sna vdlc 99 4000.4500.01f0
sna vdlc enable-host lsap 12

sna host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint

sna vdlc start HOST-B

interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
sna vdlc	Identifies the local virtual ring and virtual MAC address that will be used to establish SNA host connections over data-link switching plus (DLSw+) using VDLC.

snasw cpname

To define a control point (CP) name for SNASw, use the **snasw cpname** command in global configuration mode. To deactivate SNASw and remove the CP definition, use the **no** form of this command.

snasw cpname {*netid.cpname* | *netid* [*hostname* | **ip-address** *interface-name*]} [**hung-pu-awareness** *timer-value*] [**hung-session-awareness** *timer-value*] [**locate-timeout** *timeout-value*] [**max-pacing-window** *max-value*] [**remove-rscvs**] [**station-segmentation**]

no snasw cpname

Syntax Description

netid.cpname	Fully qualified CP name for this node, consisting of both network ID and CP name.
netid	Partial CP name, which consists of only a network ID. If this option is selected, you must also configure the hostname or IP address operands to complete the fully qualified CP name.
hostname	(Optional) Indicates a CP name that is defined by using the hostname which is configured on the router. When configuring this operand, code a *netid* only. The last eight characters of the hostname are used to complete the CP name.
ip-address *interface-name*	(Optional) Indicates the CP name that is defined by deriving the CP name from the IP address on the interface that is indicated in the *interface-name*. When configured, this operand requires a *netid* operand. In addition, a portion of the CP name can be configured. The remaining characters of the CP name that are not configured are generated from the IP address that is indicated. The generated characters are derived from a hexadecimal format of the IP address for the interface that is specified.
hung-pu-awareness *timer-value*	(Optional) Indicates the interval at which Dependent Logical Unit Requestor (DLUR) supported physical units (PUs) are checked to see if they are hung in a pending activate PU state. If a PU is in this state for two consecutive iterations of this timer, then the PU is considered hung. No attempt is made to recover the hung PU, but for diagnostic purposes message DLUR_LOG_23 (A REQACTPU RSP has not been received. Possible hung PU problem) is written to the problem determination log. If the PU later becomes activated, message DLUR_LOG_24 (A PU previously logged as possibly hung is no longer possibly hung) is issued. The valid range is from 5 to 65535 seconds. If this keyword is not specified, the default timer-value is 300 seconds.
hung-session-awareness *timer-value*	(Optional) Indicates the length of time when a new intermediate session that is still in a non-active state is considered hung. No attempt is made to clean up the hung session, but for diagnostic purposes message SCM_LOG_16 (Slow session activation detected) is issued. The valid range is from 5 to 65535 seconds. If this keyword is not specified, the default timer-value is 180 seconds.

locate-timeout *timeout-value*	(Optional) Indicates the time when an Advanced Peer to Peer Networking (APPN) Locate Search message is considered lost and is cleaned up. This will likely result in the failure of the session for which the Locate Search message was sent. When this condition occurs message DS_LOG_18 (Locate search timed out) is issued. The valid range is from 0 to 65535 seconds. A value of 0 indicates that no timeout occurs. A value from 1 to 29 seconds is rounded up to 30 seconds. If this keyword is not specified the default timeout-value is 540 seconds.
max-pacing-window *max-value*	(Optional) Indicates the upper limit of the Receive Pacing window size for intermediate sessions. When variable pacing is used, the Receive Pacing window size will not exceed this value. It may be necessary to configure a small Receive Pacing window size (such as 7) to improve performance when both batch and interactive traffic share the same network. The valid range is from 7 to 65535. If a value is not specified, the default is 64.
remove-rscvs	(Optional) Indicates that Route Selection Control Vectors (RSCVs) will be removed from incoming BINDs that are received from an upstream node before forwarding the BINDs downstream. Removing RSCVs from BINDs enables a downstream network node (NN) that is connected over a low entry networking (LEN) link to receive the BINDs and forward them to the destination node.
station-segmentation	(Optional) Sends all segments (for example, FIS, MIS, and LIS) to a particular LU before sending segments to another LU, which prevents PU 2.0 devices (that do not support segment interleaving) from generating sense code 80070000. Use this keyword for XID0 devices.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.1	The **station-segmentation** and **max-pacing-window** keywords were added.
12.2	The **remove-rscvs** keyword was added.
12.3	The **hung-pu-awareness**, **hung-session-awareness**, and **locate-timeout** keywords were added.
12.4	Support was added to **hung-pu-awareness**, **hung-session-awareness**, and **locate-timeout** keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can also deactivate SNASw without removing the **snasw cpname** definition by using the **snasw stop** privileged EXEC command which enables you to stop and restart SNASw without losing the SNASw configuration. If you use **no snasw cpname**, all SNASw configuration commands that were entered will be lost.

Coding a CP name is required for SNASw. Only one **snasw cpname** command is allowed at a time. You cannot change the **snasw cpname** command without first deleting the previous definition by using the **no** form of the command. If SNASw is active, the **no** form deactivates it. If SNASw is inactive, using **snasw cpname** activates it.

Examples

The following are examples of how to configure the **snasw cpname** command:

```
snasw cpname NETA.BRANCH5
snasw cpname NETBANK2.DLUR0005
snasw cpname NETWORKA hostname
snasw cpname NETA.CP ip-address Loopback0
```

snasw dlcfilter

To filter the frames that arrive and leave System Network Architecture Switching Services (SNASw), use the **snasw dlcfilter** command in global configuration mode. To disable the filtering of frames, use the **no** form of this command.

snasw dlcfilter [**link** *link-name* [**session** *session-address*]] [**port** *port-name*] [**rmac** *mac-address-value* [**session** *session-address*]] [**rtp** *rtp-name* [**session** *session-address*]] [**type** [**cls**] [**hpr-cntl**] [**hpr-data**] [**isr**] [**xid**]]

no snasw dlcfilter

Syntax Description

link *link-name*	(Optional) Specifies the link name upon which the data-link control (DLC) trace is filtered (one to eight characters). All incoming and outgoing frames that match this link are traced.
session *session-address*	(Optional) Specifies the session address that needs to be filtered. The *session-address* argument must be in the 3-byte hexadecimal format (0-FFFFFFFF).
port *port-name*	(Optional) Specifies the port name upon which the port is filtered (one to eight characters). All incoming and outgoing frames that match this port are traced.
rmac *mac-address-value*	(Optional) Specifies the MAC address, in non-canonical format, upon which the DLC trace is filtered. All incoming and outgoing frames that match this MAC address are traced.
rtp *rtp-name*	(Optional) Specifies the RealTime Transport Protocol (RTP) name upon which RTP is filtered (one to eight characters). All incoming and outgoing frames that match this RTP connection name are traced.
type	(Optional) Indicates that one or more frame type filters follow.
cls	(Optional) Indicates that commands to the local DLC are traced.
hpr-cntl	(Optional) Indicates that the High-Performance Routing (HPR) format identifier 5 (FID5), which does not carry a Systems Network Architecture (SNA) data payload, is traced.
hpr-data	(Optional) Indicates that the HPR format identifier 5 (FID5), which carries an SNA data payload, is traced.
isr	(Optional) Indicates that the SNA and Advanced Peer-to-Peer Networking (APPN) format identifier 2 (FID2) is traced.
xid	(Optional) Indicates that the exchange identification (XID) frames are traced.

Command Default

This command defaults to no filtering, and all frames are traced.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **snasw dlcfilter** command is used to limit the output of the **snasw dlctrace** command to a manageable amount of trace data. Running the **snasw dlctrace** command consumes CPU and memory. Using the **snasw dlcfilter** command limits the CPU and memory consumption to only the frames that are targeted for tracing.

Up to four different types of filters can be in place at once. If the type filter is coded, the frame will pass the type filter and any of the matching filters, that are coded to be included in the trace.

Examples

The following example shows how to configure the **snasw dlcfilter** command by adding a link to the dlcfilter list, adding a remote MAC address to the dlcfilter list, and filtering the dlctrace on frames of type XID:

```
Router(config)# snasw dlcfilter link cmc1link
Router(config)# snasw dlcfilter rmac 4001.1234.1001
Router(config)# snasw dlcfilter type xid
```

Related Commands

Command	Description
debug snasw dlc	Displays real-time DLC trace data to the console.
snasw dlctrace	Traces the frames arriving and leaving SNASw.
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.
snasw start	Starts SNASw.
snasw stop	Shuts down SNASw.

snasw dlctrace

To trace frames arriving and leaving Switching Services (SNASw), use the **snasw dlctrace** command in global configuration mode. To deactivate the capture of frame data and free the storage buffer used to capture the data, use the **no** form of this command.

snasw dlctrace [**buffer-size** *buffer-size-value*] [**file** *filename* [**timestamp**]] [**frame-size** *frame-size-value* | **auto-terse**] [**format** [**brief** | **detail** | **analyzer**]] [**nostart**]

no snasw dlctrace

Syntax Description

buffer-size *buffer-size-value*	(Optional) Specifies the size (in kilobytes) of the data-link control (DLC) trace buffer requested. The minimum buffer size is 100, and the maximum is 64000.
file *filename*	(Optional) Specifies the filename for the DLC trace buffer file when this file is written to the file server. Use the following format: protocol://host/path/filename. If the output file size exceeds 32MB, the first 32MB will be in the file with the name *filename*, the next 32MB will be in the file with the name *filename*.01, and so on. Note that with formatting, the output may be of different size than the buffer-size.
timestamp	(Optional) Appends the current date and time to the end of the file when it is dumped.
frame-size *frame-size-value*	(Optional) Indicates the size of the frame that is traced within the DLC trace. All data beyond the size value is truncated and is not included in the trace. The default is that the entire frame is traced.
auto-terse	(Optional) Indicates that logical unit (LU)-LU and system services control points (SSCP)-LU session data frames should be truncated after the Systems Network Architecture (SNA) request/response (RH). Also truncates NMVTs on the SSCP-physical unit (PU) session. Control frames (for example, exchange identification [XID], BIND, Activate Physical Unit [ACTPU]) are traced in their entirety.
format	(Optional) Indicates the format the DLC trace is written to when writing to a file server. Valid values are **brief**, **detail**, and **analyzer**:
brief	(Optional) Indicates that a text file is written with a one-line-per-frame summary for each frame.
detail	(Optional) Indicates that a text file is written with a frame summary line followed by a complete hexadecimal dump of the frame.
analyzer	(Optional) Indicates a binary file is generated that is readable by several popular network analyzer products. This format uses the Network Associates Sniffer file format.
nostart	(Optional) Indicates that the specified trace is not to be started when the subsystem is started.

Defaults

Tracing is off.
If a value for the *buffer-size-value* argument is not specified, then the default is 500, creating a 500-KB buffer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.3	The maximum allowed value of the *buffer-size-value* argument was increased to 6400.
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 **snasw dlctrace** command when directed by service personnel or when analysis of frame data entering and leaving SNASw is necessary.

The **snasw dlctrace** command copies frames into a memory buffer, which can degrade router performance. Therefore, care should be taken when using this command. When issued on a highly used system, the **snasw dlcfilter** command should be used in conjunction with the **snasw dlctrace** command to limit the output of the trace.

Use the **snasw dump** command to dump the trace data to a file server or the **show snasw dlctrace** command to display captured frames on the console.

When the analyzer format is used, portions of the frame are reconstructed from their actual representation on the data link. Because of this format, portions of the data in the header portion of the frame are modified. Specifically, if Routing Information Field (RIF) data was present on the actual data-link frame, that information is omitted in the dlctrace. In addition, information in the Logical Link Control (LLC) header (for example, Nr, Ns counts) is not reliably transferred to the traced frame. However, the remainder of the frame, including all Systems Network Architecture (SNA) content, is a reliable representation of the frame as it appeared on the actual upstream or downstream link.

Examples

The following are examples of how to configure the **snasw dlctrace** command:

```
snasw dlctrace
snasw dlctrace buffer-size 5000 file tftp://10.69.120.21/dlcfiles/dlc/trc
```

Related Commands

Command	Description
show snasw dlctrace	Displays the captured DLC trace information on the console.
snasw dlcfilter	Filters frames being captured.
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.

snasw dlus

To specify parameters related to Dependent Logical Unit Requestor (DLUR) or Dependent Logical Unit Server (DLUS) functionality, use the **snasw dlus** command in global configuration mode. To remove the data specified in a previous **snasw dlus** command, use the **no** form of this command.

snasw dlus *primary-dlus-name* [**backup** *backup-dlus-name*] [**prefer-active**] [**retry** *interval count*] [**once**]

no snasw dlus

Syntax Description

primary-dlus-name	Specifies the fully qualified name of the primary DLUS (3 to 17 characters).
backup *backup-dlus-name*	(Optional) Indicates configuration of a backup DLUS. A backup DLUS is used when the primary DLUS is unreachable or cannot service a specific downstream device. The fully qualified name of the backup DLUS is 3 to 17 characters in length.
prefer-active	(Optional) Indicates that if an active DLUR or DLUS connection was established, an incoming physical unit (PU) will retry exclusively on the active DLUS connection and will not attempt to connect to a different DLUS.
retry *interval count*	(Optional) Indicates that the DLUR retry parameters follow this statement. The *interval* argument indicates the time period between attempts to connect a DLUS if one is not serving a specific PU. The *count* argument indicates the number of times the current or primary DLUS is retried before an attempt is made to connect to a backup or inactive DLUS.
once	(Optional) Instructs the DLUR to attempt only one retry cycle (with primary and backup (if configured) DLUS, according to either the default retry values or to the retry values specified by the **retry** keyword) to request DLUS services. If the service requests are not answered, the downstream link will be disconnected.

Defaults

If the **prefer-active** keyword is not specified, each connected downstream station will attempt to connect to the primary DLUS or backup DLUS until the device receives DLUS services.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

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

Only one **snasw dlus** command is allowed at a time. The **snasw dlus** command cannot be changed without first deleting the previous definition using the **no** form of the command.

The **prefer-active** keyword supersedes the **once** keyword, which means that if the **prefer-active** keyword is configured and there is an active DLUS, then all DLUS services requests will be negotiated only with the active DLUS. The DLUR will not send DLUS service requests to other DLUSs. In this situation, the **once** keyword has no effect.

Examples

The following are examples of how to configure the **snasw dlus** command:

```
snasw dlus NETA.HOST1 backup NETA.HOST2
```

snasw dlus NETBANK2.CDERM34 prefer-active retry 30 3

snasw dump

To copy problem determination logs and traces from internal buffers to an external file server, use the **snasw dump** command in privileged EXEC mode.

snasw dump {**all** | **dlctrace** | **ipstrace** | **summary-ipstrace** | **pdlog**}

Syntax Description

all	Indicates that all configured trace and problem determination buffers should be transferred. The **file** keyword must be configured on the enabling configuration command for the buffers to be dumped. Traces that run but do not have the (See the "Usage Guidelines Section.) **file** keyword coded are not transferred.
dlctrace	Indicates that the data-link control (DLC) trace buffer is transferred to a file server. If **file** keyword is configured on the **snasw dlctrace** command, the URL specified is used for transferring the DLC trace file. If **file** keyword is not configured on the **snasw dlctrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and filename for the transferred file.
ipstrace	Indicates that the InterProcess Signal (IPS) trace buffer is transferred to a file server. If the **file** is configured on the **snasw ipstrace** command, the URL specified is used for transferring the ipstrace file. If **file** keyword is not configured on the **snasw ipstrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and filename for the transferred file.
summary-ipstrace	Indicates that the summary IPS trace buffer is transferred to a file server. If the **file** keyword is coded on the **snasw summary-ipstrace** command, the URL specified is used for transferring the summary ipstrace file. If the **file** keyword is not coded on the **snasw ipstrace** command, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and filename for the transferred file.
pdlog	Indicates that the problem determination log buffer is transferred to a file server. If the **file** keyword is coded on the **snasw pdlog** command, the URL specified is used for transferring the pdlog file. If the **file** keyword is not coded, the transfer protocol defaults to TFTP, and the user is prompted for the remote host and filename for the transferred file.

Command Modes

Privileged EXEC

Defaults

No default behavior or values

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.

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

Usage Guidelines

The **snasw dump** command is used for gathering trace files for diagnosis by Cisco personnel or onsite trace analysis.

TFTP can handle files up to 16 Mb in size. If you are transferring a file larger than 16 Mb, do not use TFTP. Instead, use FTP or some other file transfer method. To change the transmission protocol, use the **file** keyword with the **snasw trace** or **snasw dlctrace** global configuration command.

Before you use FTP, make sure you configure the **ip ftp username** and **ip ftp password** command to a valid user and password on the system to which the file is being sent.

Examples

The following are examples of how to enter the **snasw dump** command:

```
Router# snasw dump all
Router# snasw dump dlctrace
```

Related Commands

Command	Description
snasw dlctrace	Traces frames arriving and leaving Switching Services (SNASw).
snasw ipstrace	Sets up a trace buffer and begins tracing IPS trace elements.
snasw pdlog	Controls message logging to the console and the Systems Network Architecture (SNA) problem determination log cyclic buffer.

snasw event

To indicate which normal events are logged to the console, use the **snasw event** command in global configuration mode. To return the events to their default state, use the **no** form of this command.

snasw event [**cpcp**] [**dlc**] [**implicit-ls**] [**port**]

no snasw event

Syntax Description

cpcp	(Optional) Indicates that an event is issued for control point (CP). The CP session state changes.
dlc	(Optional) Indicates data-link control (DLC) state changes.
implicit-ls	(Optional) Indicates state change on implicit links, including connection network links.
port	(Optional) Indicates that an event is issued for port state changes.

Defaults

By default, only defined links and Dependent Logical Unit Server (DLUS) events are sent to the pdlog or console.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.1(6)	The **defined-ls** keyword was deleted.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to configure the **snasw event** command:

```
snasw event implicit-ls
```

snasw ip-precedence

To define IP type of service (ToS) precedence settings to be mapped to Advanced Peer-to-Peer Networking (APPN) priorities, use the **snasw ip-precedence** command in global configuration mode. To remove the precedence settings, use the **no** form of this command.

snasw ip-precedence link *link-setting* **network** *network-setting* **high** *high-setting* **medium** *medium-setting* **low** *low-setting*

no snasw ip-precedence link *link-setting* **network** *network-setting* **high** *high-setting* **medium** *medium-setting* **low** *low-setting*

Syntax Description

link *link-setting*	ToS precedence setting (0–7) mapped to link control (LDLC) priority.
network *network-setting*	ToS precedence setting (0–7) mapped to network priority.
high *high-setting*	ToS precedence setting (0–7) mapped to high priority.
medium *medium-setting*	ToS precedence setting (0–7) mapped to medium priority.
low *low-setting*	ToS precedence setting (0–7) mapped to low priority.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Examples

The following is an example of how to configure the **snasw ip-precedence** command:

```
snasw ip-precedence link 7 network 7 high 7 medium 7 low 7
```

snasw ipsfilter

To filter interprocess signal trace elements being traced using the **snasw ipstrace** or **debug snasw ips** command, use the **snasw ipsfilter** command in global configuration mode. To remove all filtering, use the **no** form of this command.

snasw ipsfilter [**as**] [**asm**] [**bm**] [**ch**] [**cpc**] [**cs**] [**di**] [**dlc**] [**dma**] [**dr**] [**ds**] [**es**] [**ha**] [**hpr**] [**hs**] [**lm**] [**mds**] [**ms**] [**nof**] [**pc**] [**ps**] [**pu**] [**px**] [**rm**] [**rtp**] [**ru**] [**scm**] [**sco**] [**sm**] [**spc**] [**ss**] [**trs**]

no snasw ipsfilter

Syntax Description

as	(Optional) Specifies a filter on the Address Space component.
asm	(Optional) Specifies a filter on the Address Space Manager component.
bm	(Optional) Specifies a filter on the Buffer Management component.
ch	(Optional) Specifies a filter on the Channel component.
cpc	(Optional) Specifies a filter on the CPI-C component.
cs	(Optional) Specifies a filter on the Configuration Services component.
di	(Optional) Specifies a filter on the Defect Indication component.
dlc	(Optional) Specifies a filter on the Data Link Control component.
dma	(Optional) Specifies a filter on the Direct Memory Access component.
dr	(Optional) Specifies a filter on the Dependent logical unit (LU) Requester component.
ds	(Optional) Specifies a filter on the Directory Services component.
es	(Optional) Specifies a filter on the End System component.
ha	(Optional) Specifies a filter on the High Availability component.
hpr	(Optional) Specifies a filter on the High-Performance Routing component.
hs	(Optional) Specifies a filter on the Half Session component.
lm	(Optional) Specifies a filter on the LU Manager component.
mds	(Optional) Specifies a filter on the Management Data Stream component.
ms	(Optional) Specifies a filter on the Management Services component.
nof	(Optional) Specifies a filter on the Node Operator Facility component.
pc	(Optional) Specifies a filter on the Path Control component.
ps	(Optional) Specifies a filter on the Presentation Services component.
pu	(Optional) Specifies a filter on the physical unit (PU) Manager component.
px	(Optional) Specifies a filter on the PU Concentration component.
rm	(Optional) Specifies a filter on the Resource Manager component.
rtp	(Optional) Specifies a filter on the Rapid Transport Protocol component
ru	(Optional) Specifies a filter on the Request Unit Interface component.
scm	(Optional) Specifies a filter on the Session Connect Manager component.
sco	(Optional) Specifies a filter on the Session Connector component.
sm	(Optional) Specifies a filter on the Session Manager component.
spc	(Optional) Specifies a filter on the Serial Protocol Channel component.
ss	(Optional) Specifies a filter on the Session Services component.
trs	(Optional) Specifies a filter on the Topology Routing Services component.

Defaults No default behavior or values

Command Modes Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 command defaults to no InterProcess Signal (IPS) trace filtering.

Examples The following is an example of how to configure the **snasw ipsfilter** command:

```
snasw ipsfilter ds ss
```

Related Commands

Command	Description
show snasw ipstrace	Displays the interprocess signal trace on the router console.
snasw ipstrace	Sets up a trace buffer and begins tracing IPS trace elements.
debug snasw ips	Displays realtime ipstrace information to the console.

snasw ipstrace

To set up a trace buffer and begin tracing InterProcess Signal (IPS) trace elements, use the **snasw ipstrace** command in global configuration mode. To turn off the capture of trace elements and to free the trace buffer, use the **no** form of this command.

snasw ipstrace [**buffer-size** *buffer-size-value*] [**file** *filename* **timestamp**]

no snasw ipstrace

Syntax Description

buffer-size *buffer-size-value*	(Optional) Indicates that this trace command controls the size of the buffer used for storing ipstrace elements (in kilobytes). The default is 500 KB. The minimum buffer size is 10 KB; the maximum size is 64000 KB.
file *filename*	(Optional) Specifies the filename for the IPS trace buffer file when this file is written to the server. If the output file size exceeds 32MB, the first 32MB will be in the file with the name *filename*, the next 32MB will be in the file with the name *filename*.01, and so on. Note that with formatting, the output may be of different size than the buffer-size.
timestamp	(Optional) Appends the current date and time to the end of the file when it is dumped.

Defaults

This command defaults to no tracing with no cyclic buffer allocated.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.3	The maximum allowed value of the *buffer-size-value* argument was increased to 6400.
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 **snasw ipstrace** command when directed by Switching Services (SNASw) personnel.

The **snasw ipstrace** command copies frames into a memory buffer, which can affect router performance. Therefore, care should be taken when using this command.

The ipstrace information is stored in a cyclic buffer allocated out of main processor memory. Use the **snasw dump** command to dump the binary trace information to a file server or the **show snasw ipstrace** command to display captured IPS trace information to the console. The IPS trace is a low-level internal trace.

Examples

The following is an example of how to configure the **snasw ipstrace** command:

```
snasw ipstrace buffer-size 1000 file tftp://myhost/path/file
```

Related Commands

Command	Description
show snasw ipstrace	Displays interprocess signal trace on the router console.
snasw ipsfilter	Filters interprocess signal trace elements being traced using the **snasw ipstrace** or **debug snasw ips** commands.
debug snasw ips	Displays realtime IPS trace information to the console.

snasw link

To configure upstream links, use the **snasw link** command in global configuration mode. To remove the configuration of upstream links, use the **no** form of this command.

snasw link *linkname* **port** *portname* **rmac** *mac-address* | **host-dest** *v4-or-v6-hostname* | **ip-dest** *ip-address* [**rsap** *sap-value*] [**nns**] [**tgp** [**high** | **low** | **medium** | **secure**]] [**nostart**]

no snasw link *linkname*

Syntax Description

linkname	Indicates the one-to-eight character local name for this link. This name is used to identify the link in **show** and privileged EXEC commands.
port *portname*	Specifies the Switching Services (SNASw) port from which this link will connect.
rmac *mac-address*	Specifies the 48-bit MAC address of the destination station. Either this keyword or the **ip-dest** keyword is required. remote MAC (RMAC) is required for all links associated with ports that are not High-Performance Routing (HPR) or IP ports.
host-dest *v4-or-v6-hostname*	Specifies the hostname that resolves to the IPv4 or IPv6 address of the destination station. Either the **host-dest** or **ip-dest** keyword is required for all links that are associated with HPR over IP ports. The *v4-or-v6-hostname* keyword can be between 1 and 64 characters in length.
ip-dest *ip-address*	Indicates the IP address or Domain Name System (DNS) name of the destination stations. Either this keyword or the **rmac** keyword is required. For all links associated with HPR or IP ports, the **ip-dest** keyword is required.
rsap *sap-value*	(Optional) Indicates the destination service access point (SAP) value, which defaults to 4.
nns	(Optional) Configures the adjacent Control Point (CP) as a preferred Network Node Server (NNS). You can specify the **nns** keyword on more than one link to identify multiple preferred NNSs.
tgp	(Optional) Configures a Transmission Group (TG) characteristic profile for route calculation. All SNASw TGs have the following characteristics in common: • Capacity = 16 megabits per second • Propagation delay = 384 microseconds • User parameter 1 = 128 • User parameter 2 = 128 • User parameter 3 = 128 However, you can adjust the connect cost, byte cost, and security TG characteristics. Valid values are **high**, **low**, **medium**, and **secure**.
high	(Optional) Prefers this link over links with a TG profile of **medium** or **low**. With this TG profile you can have the following TG characteristics: • Connect cost = 0 • Byte cost = 0 Security = Nonsecure

low	(Optional) Prefers this link when links with a TG profile of **high** or **medium** are not available. With this TG profile you can have the following TG characteristics: • Connect cost = 255 • Byte cost = 255 Security = Nonsecure
medium	(Optional) Prefers this link when links with a TG profile of **high** are not available. With this TG profile you can have the following TG characteristics: • Connect cost = 196 • Byte cost = 196 Security = Nonsecure
secure	(Optional) Prefers this link when a secure TG is required by the APPN class-of-service in use. With this TG profile you can have the following TG characteristics: • Connect cost = 196 • Byte cost = 196 Security = Secure public switched network
nostart	(Optional) Indicates that the link will not start automatically when defined.

Defaults

The destination SAP value defaults to 4.

The default TG characteristic profile is medium and nonsecure.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.3(14)T	The **host-dest** keyword 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 **snasw link** command to configure upstream connections to SNA data hosts, services, and DLUS nodes. Do not use this command to establish downstream connections to client workstations and devices that are serviced by the SNA switch. Configure client workstations and devices to connect into the SNA switch by configuring an outbound connection on these devices that specifies the MAC address of a port that is active on SNASw. SNASw then creates the downstream link dynamically when the workstation or device connects to SNASw.

If using the **ip-dest** keyword and using a DNS name instead of an IP address, the DNS name is resolved to an IP address at the time the definition is entered (or the time SNASw is started) and will remain resolved to that same address for the duration that SNASw is active. The DNS name is not resolved to an IP address each time the link is restarted.

If the link fails and SNASw switches to a non-preferred NNS (one without the **nns** keyword configured), SNASw will return CP-CP sessions to the preferred NNS when the NNS link becomes active again. Also, when the **nns** keyword is configured on a link, that link can be automatically restarted, even after the **snasw stop link** command is issued. See the **snasw stop link** command for details.

When using the **host-dest** keyword, the hostname must be resolved locally by either ip **ip host** or **ipv6 host** commands or by a Domain Name Server before the SNASw port is configured.

Examples

The following are examples of how to configure the **snasw link** command:

```
snasw link LINKCMC1 port TOKENO rmac 4000.333.4444 rsap 8
snasw link HOSTIP port HPRIP ip-dest 172.18.3.44
snasw link HOSTEE port HPRIP host-dest MVSOSA1
```

Related Commands

Command	Description
show snasw link	Shows the SNASw link objects.
snasw port	Specifies the DLCs used by SNASw.

snasw location

To configure the location of a resource, use the **snasw location** command in global configuration mode. To disable the location of a resource, use the **no** form of this command.

snasw location *resource-name* {**owning-cp** *cp-name* | **xid** *node-id*}

no snasw location *resource-name*

Syntax Description

resource-name	Indicates the fully qualified name of the resource for which location information is being configured. For name, 3 to 17 characters length is allowed.
owning-cp *cp-name*	Indicates the fully qualified control point (CP) name where the resource resides.
xid *node-id*	Specifies the Exchange identification (XID) of the node, where the specified resource resides. The *node-id* is specified in eight hexadecimal characters.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.2	Support for wildcards was added in the *cpname* argument.
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 **snasw location** command is typically used when a low-entry networking node (LEN) node link is established with a destination logical unit (LU). The **snasw location** command allows Switching Services (SNASw) to route session requests over the LEN node link to the resources named.

If the LEN node has a unique CP name configured, use the **owning-cp** keyword. Use the **xid** keyword when there is no CP name for the LEN node or conntype dyncplen is configured on the snasw port. The XID node-id of the LEN node must be unique for the location statement.

When a LEN node connects into an SNASw node, SNASw dynamically learns the CP name of the LEN and places it in its directory. In addition, SNASw dynamically learns the LU names of all LUs on the LEN that initiate independent sessions. Only define the location when an independent logical unit (ILU) on a LEN device is not sharing the node's CP name and does not initiate the first session. In all other cases, the LU's location will be learned dynamically.

The directory entry is created the next time the LEN node connects. If there is already a link to the LEN node active and you add a new SNASw location statement, it will not take effect until the next time the LEN CP connects.

Note Do not use the **snasw location** command to predefine the location of any resource that can be found dynamically using Advanced Peer-to-Peer Networking (APPN) searches (for example, resources on upstream APPN nodes or upstream or downstream ENs).

It is permissible to use the wildcard character "*" in location definitions to allow a definition to generate name associations for multiple devices. When the wildcard character is used for this purpose, the * symbol must be coded in both the *resource-name* and the *cpname* argument. If any real device attaches with a CP name that matches the non-wildcard portion of the **owning-cp** *cpname* keyword—argument pair specified, a location association will be made that replaces the wildcard characters of the CPname in the position of the *resource-name* argument. For example, if a definition **snasw location NETA.LU*01 owning-cp NETA.CP*** is coded and CP with the name NETA.CPABCD connects, then the resource name NETA.LUABCD01 will be defined to SNASw with owning-cp NETA.CPABCD.

You can also use the wildcard character "*" in location definitions to allow a specific device to connect under different CP names, but a single device cannot connect under multiple CP names at the same time. In this case, the * symbol must be used in only the *cpname* argument and not the *resource-name* argument. When the device connects with a CP name that matches the nonwildcard portion of the *cpname* argument, a corresponding location association will be made for the *resource-name* argument with that CP name.

Examples

The following example shows how to configure the location of a resource when the LEN node has CP name configured:

```
snasw location NETA.INDEPLU owning-cp NETA.LENHOSTA
```

Related Commands

Command	Description
show snasw directory	Displays the SNASw directory entries.

snasw lu62-security

To define a session-key or password with a partner logical unit (LU) or control point (CP), use the **snasw lu62-security** command in global configuration mode. To it, use the **no** form of this command.

snasw lu62-security *NETID.NAME* {**ascii** *char-string* | **hex** *hex-string*}

no snasw lu62-security *NETID.NAME*

Syntax Description

NETID.NAME	Fully qualified partner LU name.
ascii	Password/Session-key entered in ASCII string.
char-string	Character string (8 characters).
hex	Password/Session-key entered in hex string.
hex-string	Hexadecimal string (even length - 16 digits).

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

In the following example, “pvc1” within the PVC range called “range1” is deactivated:

```
Router(config)# snasw lu62-security NETA.HOSTB ascii pass1234
Router(config)# snasw lu62-security NETA.HOSTC hex 023f4bc56a
Router#show snasw session detail
1>
Partner LU nameNETA.HOSTB FMH-12 exchanged Yes
```

Related Commands

Command	Description
show snasw session detail	Displays detailed snasw session information.

snasw mode

To define a new mode and associate it with an existing Class of Service (COS), use the **snasw mode** command in global configuration mode. To delete the mode, use the **no** form of this command.

snasw mode *mode* **cos** *cos*

no snasw mode *mode* **cos** *cos*

Syntax Description

mode	Name of the new mode.
cos *cos*	Name of an existing COS, such as #INTER.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Examples

The following is an example of how to configure the **snasw mode** command:

```
snasw mode abcmode cos #INTER
```

snasw msgdump

To enable automatic dumping of the data-link control (DLC) trace, InterProcess Signal (IPS) trace, and problem determination log when a specified Systems Network Architecture (SNA) Switching Services (SNASw) message is displayed, use the **snasw msgdump** command in global configuration mode. To disable automatic dumping, use the **no** form of this command.

snasw msgdump *message* [**writecore**]

no snasw msgdump *message* [**writecore**]

Syntax Description

message	SNASw message to trigger the automatic dump.
writecore	(Optional) Message to trigger a write core.

Defaults

When the **writecore** keyword is used, the write core operation is attempted using Trivial File Transfer Protocol (TFTP).

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.
12.3(15)T	The **writecore** 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

The **snasw msgdump** command is only invoked the first time the target message is encountered. To trigger automatic dumping after this first instance of the target message, remove the configuration and configure again the command by entering the **no snasw msgdump** command followed by the **snasw msgdump** command.

When the message dump is invoked, an SNA Alert is sent to the local node's Alert focal point. To verify the existence of an Alert focal point, use the **show snasw node** command and look at the value of the "Alert focal point" entry.

Usually, SNASw will have an Alert focal point when the router's has an active upstream link to a network node server.

If that link is active and there is still no focal point, enter the following command in the NetView mainframe application:

```
FOCALPT CHANGE,FPCAT=ALERT,TARGET=cpname
```

where *cpname* is either the CP name of the NN server for SNASw or the CP name of SNASw itself.

The Alert ID of the SNA Alert sent is x'DAED5B0B'.

Caution Use the **writecore** keyword only under the direction of a technical support representative. Use of the **writecore** keyword puts a large load on the router and may cause momentary network disruption.

To use the **writecore** keyword successfully with the **snasw msgdump** command, you must configure the **exception dump** command to specify a destination server. By default, the write core operation is attempted using TFTP; the core file is written under the /tftpboot directory. If you want to specify the File Transfer Protocol (FTP) for exception instead, use the **ip ftp user**, the **ip ftp password**, and the **exception protocol ftp** commands to configure user name and password information.

Because the **writecore** keyword creates a large file, it is recommended that you compress this file to save server space. Use the exception core-file compress command to compress the file.

Examples

The following example shows how to use the **snasw msgdump** command:

```
snasw msgdump %SNASW-6-CS_LOG_60
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception dump	Configures the router to dump a core file to a particular server when the router crashes.
exception protocol	Configures the protocol used for core dumps.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

snasw pathswitch

To force an High-Performance Routing (HPR) pathswitch for an Realtime Transport Protocol (RTP) connection, use the **snasw pathswitch** command in privileged EXEC mode.

snasw pathswitch [*rtp-connection-name* | **all**]

Syntax Description

rtp-connection-name	(Optional) Specifies the RTP connection to pathswitch. This is an 8-byte string. You can obtain the value for the *rtp-connection-name* argument from the **show snasw rtp** command.
all	(Optional) Specifies that a pathswitch operation will be initiated for every RTP connection managed by the local node.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 a specific connection name is coded, and no such connection is known to Switching Services (SNASw), the **snasw pathswitch** command is ignored, and a message is issued. Use the **snasw pathswitch** command to force an HPR pathswitch for sessions that use this node as an RTP endpoint.

Use the **snasw pathswitch** command if you want to force a switch back to a primary route when it recovers, and the session seems to be hung.

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

Examples

The following is an example of how to execute the **snasw pathswitch** command:

```
Router# snasw pathswitch @R000006
```

Related Commands

Command	Description
show snasw rtp	Displays the SNASw RTP connections.

snasw pdlog

To control message logging to the console and the Systems Network Architecture (SNA) problem determination log cyclic buffer, use the **snasw pdlog** command in global configuration mode. To remove previous pdlog configurations, use the **no** form of this command.

snasw pdlog [**problem** | **exception** | **info**] [**buffer-size** *buffer-size-value*] [**file** *filename* [**timestamp**]]

no snasw pdlog

Syntax Description

problem	(Optional) Indicates that only problem records are sent to the console. This is the default.
exception	(Optional) Indicates that both problems and exceptions are sent to the console.
info	(Optional) Indicates that informational messages and problems and exceptions are sent to the console.
buffer-size *buffer-size-value*	(Optional) Indicates the size of the pdlog buffer requested (in kilobytes). The default is 500 KB. The minimum size is 10 KB, and the maximum size is 64000 KB.
file *filename*	(Optional) Indicates the URL for writing the pdlog file to a server. Use the following format: protocol://host/path/filename. If the output file size exceeds 32MB, the first 32MB will be in the file with the name *filename*, the next 32MB will be in the file with the name *filename*.01, and so on. Note that with formatting, the output may be of different size than the buffer-size.
timestamp	(Optional) Appends the current date and time to the end of the file when it is dumped.

Defaults

If not coded, the **snasw pdlog** command defaults to an active 500 KB cyclic buffer. Problems, exceptions, and informational messages are always sent to the buffer. By default, only problems go to the console.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
12.3	The maximum allowed value of the *buffer-size-value* argument was increased to 6400.
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 **snasw pdlog** command to customize the type of information you prefer to see on the router console from the Switching Services (SNASw) feature.

Examples

The following is an example of how to configure the **snasw pdlog** command:

```
snasw pdlog exception buffer-size 200 file tftp://my host/files/trace.pdlog
```

Related Commands

Command	Description
show snasw pdlog	Displays entries in the cyclical problem determination log to the console.
snasw dump	Copies problem determination logs and traces from internal buffers to an external file server.

snasw port

To specify the data-link controls (DLCs) used by System Network Architecture Switching Services (SNASw), use the **snasw port** command in global configuration mode. To delete a previously configured port, use the **no** form of this command.

HPR-IP Ports

snasw port *port-name* **hpr-ip** *interface-name* [**hostname** *v4-or-v6-hostname* [**ipv4 | ipv6**]] [**ldlc** [*liveness-time t1-retry-time t1-retry-count*]] [**maxbtu** *max-btu-size*] [**qsize** *qsize-value*] [**vnname** *virtual-node-name* [**no-limres**]] [**nostart**]

no snasw port *port-name*

VDLC and Virtual Token Ring Ports

snasw port *port-name* {**vdlc** *ring-group* **mac** *mac-address* | *virtual-TokenRing-interface-name*} [**conntype nohpr | len | dyncplen | dialoutlen**] [**hpr-sap** *hpr-sap-value*] [**max-links** *link-limit-value*] [**maxbtu** *max-btu-size*] [**nns-required**] [**sap** *sap-value*] [**vnname** *virtual-node-name* [**no-limres**]] [**nostart**]

no snasw port *port-name*

All Other Types of Ports

snasw port *port-name interface-name* [**conntype nohpr | len | dyncplen | dialoutlen**] [**hpr-sap** *hpr-sap-value*] [**max-links** *link-limit-value*] [**maxbtu** *max-btu-size*] [**sap** *sap-value*] [**vnname** *virtual-node-name* [**no-limres**]] [**nostart**]

no snasw port *port-name*

Syntax Description

hpr-ip	Indicates that the port is HPR or IP types.
port-name	The one- to- eight character name for the port. This argument is used to refer to this port in informational messages and the **show snasw port** command.
interface-name	The name of the interface over which the port communicates. Allowable interfaces are Token Ring, Ethernet, VLAN, or loopback.
hostname *v4-or-v6-hostname*	(Optional) Specifies a hostname that resolves to an IPv4 or IPv6 address associated with the interface and over which the port will communicate. The *v4-or-v6-hostname* argument can be between 1 and 64 characters in length.
ipv4	(Optional) Specifies that the preceding hostname is resolved to an IPv4 address only.
ipv6	(Optional) Specifies that the preceding hostname is resolved to an IPv6 address only.
ldlc	(Optional) Overrides the default Logical Data Link Control (LDLC) parameters for all links which use the port. This keyword allows the LDLC parameters for SNASw links to be configured to match those at the other Rapid Transport Protocol (RTP) endpoint, which is often a host z/OS or CS/390.

liveness-time	(Optional) Number of seconds for the liveness timer. This parameter matches the z/OS or CS/390 LIVTIME keyword. The allowed range is from 5 to 25 seconds. Prior to Cisco IOS Release 12.3(8)T, the default was 2 seconds. For Cisco IOS Release 12.3(8)T and later releases, the default is 10 seconds.
t1-retry-time	(Optional) Number of seconds between T1 retry attempts. This parameter matches the z/OS or CS/390 SRQTIME keyword. The allowed range is from 3 to 20 seconds. Prior to Cisco IOS Release 12.3(8)T, the default was 2 seconds. For Cisco IOS Release 12.3(8)T and later releases, the default is 15 seconds.
t1-retry-count	(Optional) Number of times to retry before the HPR-IP TG becomes inoperative. This parameter matches the z/OS or CS/390 SRQRETRY keyword. The allowed range is from 3 to 9 retries. Prior to Cisco IOS Release 12.3(8)T, the default was 10 retries. For Cisco IOS Release 12.3(8)T and later, the default is 3 retries.
maxbtu *max-btu-size*	(Optional) Indicates the maximum basic transmission unit (BTU) size for the remote end (both inbound and outbound). This value is used in XID3 negotiation. The valid range is from 1 to 17800.
qsize *qsize-value*	Number of packets allowed on the IP/ User Datagram Protocol (UDP) inbound queue. • Set the number of packets allowed to a higher value if **show ip socket detail** for one of the SNASw sockets (1200-12004) are showing drops and a highwater equal to the queue limit. • Consider adjusting the interface input hold queues and IP Selective Packet Discard (SPD) queue thresholds at the same time. The allowed range is 50 to 10000, and the default is 50. This keyword applies to HRP/IP interfaces only.
vnname *virtual-node-name*	(Optional) Indicates the network qualified virtual node name (3 to 17 characters) of the connection network being defined.
no-limres	(Optional) Indicates that sessions established on the links over this port are presented as non-limited resources.
nostart	(Optional) Indicates that the port will not open automatically when defined.
vdlc *ring-group*	Indicates that the port is virtual data-link control (VDLC). No *interface-name* argument is required. The *ring-group* argument indicates the source-bridge ring group of which this VDLC port is a member.
mac *mac-address*	Indicates the virtual source MAC address used for the VDLC port.
virtual-TokenRing-interface-name	Name of the virtual token ring interface.
conntype	(Optional) Indicates the connection type for the port. If this keyword is not configured, HPR-capable links are established.
nohpr	(Optional) Indicates that the HPR is not supported but Advanced Peer-to-Peer Networking (APPN) connections with control point (CP)-CP sessions are permitted.
len	(Optional) Indicates that APPN connections are not allowed; only low-entry networking node (LEN) node-level connectivity is negotiated.
dyncplen	(Optional) Specifies the connection type and ends CP names configured on devices that have not been configured uniquely across the XID3-capable devices.
dialoutlen	(Optional) Specifies the connection type when logical unit (LU) 6.2 communications are used.
hpr-sap *hpr-sap-value*	(Optional) Indicates the local HPR-service access point (SAP) value.

max-links *link-limit-value*	(Optional) Indicates the number of links permitted on this port.
maxbtu *max-btu-size*	(Optional) Indicates the maximum BTU size for the remote end (both inbound and outbound). This value is used in XID3 negotiation. The valid range is from 1 to 17800.
nns-required	(Optional) Enables configurations with redundant downstream MAC addresses to only allow SNASw nodes that have appropriate upstream connectivity to accept and retain connections from downstream devices.
sap *sap-value*	(Optional) Indicates the local SAP (LSAP) value.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7) T.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. The **no-limres** keyword was added.
12.3	This command was integrated into Cisco IOS Release 12.3. The **dialoutlen** keyword was added.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T. The default values for the *liveness-time*, *t1-retry-time*, and *t1-retry-count* arguments were changed.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T. The **hostname** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(16)	This command was integrated into Cisco IOS Release 12.4(16). The **qsize** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M. The **ipv4** and **ipv6** keywords were added.

Usage Guidelines

More than one port can be configured (with different port names). A configured port cannot be redefined without first deleting the port using the **no** form of the **port** command.

Note Two ports cannot be defined on the same interface unless different values are configured for the **sap** and **hrp-sap** keywords on the ports.

- SNASw ports do not dynamically adjust to interface configuration changes that are made when SNASw is active. For example, if you change an interface MAC address or maximum transmission unit (MTU), SNASw may not recognize the new value. If you want to make changes to an interface and want SNASw to adjust to the new interface changes, you may need to either delete and redefine

the port that is using that interface or stop and restart SNASw.

The interface must be defined before the ports that use them are defined and activated.

SNASw does not support EtherChannel interfaces (neither port-channel interfaces nor Fast Ethernet interfaces configured with the **channel-group** command). Do not try to configure a SNASw port with either of these EtherChannel interface types.

- When using the **hostname** keyword, the hostname must be defined on the interface and be resolved locally by either **ip host** or **ipv6 host** commands or by a Domain Name Server (DNS) before the SNASw port is configured.
- When using the **vnname** keyword to define a connection network, Cisco recommends that you do not define any links to this port. Configure one port for your defined links to use, without the **vnname** keyword, and another port with the **vnname** keyword. No links should use the port with the **vnname** keyword. This means you may need to also configure a loopback interface for the **vnname** port.
- When the **dyncplen** keyword is used, a unique cpname must be generated and used locally by SNASw to have a properly functioning APPN connection management and directory function.
- When LU 6.2 communications are used on this link, the **dialoutlen** keyword is needed. A unique cpname must be generated and used locally by SNASw to have a properly functioning APPN connection management and directory function. The keyword is used when link activation to a downstream device is driven by the mainframe dial command.
- When the max-links limit is reached, the port does not respond to inbound connection requests from stations attempting to connect to this port. Outbound connections are still permitted. The **max-links** can be coded only on VDLC and Virtual Token Ring port types.
- When the connection network is treated by default as limited resource, the **no-limres** keyword prevents the remote end from dropping the sessions prematurely (provided that appropriate definitions are also coded on the remote end, such as DISCNT=NO for Physical Unit (PU) or Model in VTAM).
- When a port is configured with the **nns-required** keyword, the port does not respond to downstream connection requests unless this SNASw node has active CP-CP sessions to an upstream network management system (NNS). If a connection has already been made through this SNASw node and then upstream NNS CP-CP connectivity is lost, this SNASw node deactivates all non-HPR links using this port that do not have active LU-LU or Intermediate Session Routing (ISR) sessions.

Note The **nns-required** keyword is relevant only for ports that will be accepting downstream connections from devices. It is not relevant for upstream ports. This keyword is only valid for Virtual Token Ring and VDLC ports.

Examples

The following examples show how to configure the **snasw port** command:

```
Router(config)# snasw port SRBG Virtual-TokenRing0 conntype nohpr
Router(config)# snasw port UPSTREAM TokenRing1/1
Router(config)# snasw port dlswport vdlc 30 mac 4000.33333.4444
Router(config)# snasw port HPRIP hpr-ip Loopback0
Router(config)# snasw port TRVLAN Vlan1/1 vnname NETA.CONNET
Router(config)# snasw port HOSTEE hpr-ip Loopback0 vnname NETA.CONNET hostname Loop0ip
```

Related Commands

Command	Description
show snasw port	Displays the SNASw port objects.
snasw link	Configures upstream links.

snasw rtp pathswitch-timers

To tune the RealTime Transport Protocol (RTP) pathswitch timers for an SNASwitch, use the **snasw rtp pathswitch-timers** command in global configuration mode. To restore the default settings for the RTP pathswitch timers, use the **no** form of this command.

snasw rtp pathswitch-timers *low-priority medium-priority high-priority network-priority*

no snasw rtp pathswitch-timers

Syntax Description

low-priority	Number of seconds to attempt pathswitch for low-priority RTPs. Allowed values are from 5 to 65535 seconds. The default is 480.
medium-priority	Number of seconds to attempt pathswitch for medium-priority RTPs. Allowed values are from 5 to 65535 seconds. The default is 240 seconds.
high-priority	Number of seconds to attempt pathswitch for high-priority RTPs. Allowed values are from 5 to 65535 seconds. The default is 120 seconds.
network-priority	Number of seconds to attempt pathswitch for network-priority RTPs. Allowed values are from 5 to 120 seconds. The default is 60 seconds.

Defaults

low-priority: 480 seconds
medium-priority: 240 seconds
high-priority: 120 seconds
network-priority: 60 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

The arguments for this command should be tuned to match the values specified at the other end of the RTP connection. This endpoint could be another SNA switch router or any other High-Performance Routing (HPR)-capable control point, which will most often be an IBM z/OStm mainframe. In this case, you should match the settings of the HPRPST start option.

The value for each pathswitch timer value must be greater than or equal to the value for the next highest priority timer argument. In other words, the *low-priority* argument >= *medium-priority* argument >= *high-priority* argument >= *network-priority* argument.

Examples

The following example tunes the RTP pathswitch timers:

```
router(config)# snasw rtp pathswitch-timers 160 80 40 20
```

snasw start

To start Switching Services (SNASw), use the **snasw start** command in privileged EXEC mode.

snasw start

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 not enough memory exists to start SNASw, a message indicating lack of memory is issued. A control point (CP) name must be configured with the **snasw cpname** command before SNASw will start.

Examples

The following is an example of the **snasw start** command:

```
Router# snasw start
```

Related Commands

Command	Description
show snasw node	Displays details and statistics of the SNASw operation.
snasw stop	Shuts down SNASw.

snasw start cp-cp

To initiate a request to start control point (CP)-CP sessions with a partner CP, use the **snasw start cp-cp** command in privileged EXEC mode.

snasw start cp-cp *cpname*

Syntax Description

cpname	Indicates the fully qualified CP name of the adjacent node with which CP-CP sessions should be started.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 **snasw start cp-cp** command if CP-CP sessions fail permanently or temporarily, but beyond the time frame for automatic CP-CP session retry. If the current state of the node mandates that CP-CP sessions cannot be started to the partner (for example, CP-CP sessions already exist on a different upstream link) or no active adjacent CP matches the cpname named, the command fails.

Typically, Switching Services (SNASw) automatically activates CP-CP sessions as necessary and the **snasw start cp-cp** command is rarely needed. Frequent CP-CP session failure beyond the time frame for automatic session retry indicates a problem, and should be reported.

Examples

The following is an example of the **snasw start cp-cp** command:

```
Router# snasw start cp-cp NETA.CMCHOST
```

Related Commands

Command	Description
snasw stop cp-cp	Terminates CP-CP sessions with a partner CP.

snasw start link

To start an inactive defined link, use the **snasw start link** command in privileged EXEC mode.

snasw start link *linkname*

Syntax Description

linkname	Indicates the name of the link as configured or shown in **show snasw link** command.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 **snasw start link** command to initiate a connection sequence for a link that is defined but not active. Unless the **nostart** command is configured on the link definition, a link is started automatically. Use this command to start links that have **nostart** configured or links that have been stopped using the **snasw stop link** privileged EXEC command.

Examples

The following is an example of the **snasw start link** command:

```
Router# snasw start link CMCHOST1
```

Related Commands

Command	Description
show snasw link	Displays the Switching Services (SNASw) link objects.
snasw stop link	Stops an active link.

snasw start port

To start an inactive port, use the **snasw start port** command in privileged EXEC mode.

snasw start port *portname*

Syntax Description

portname	Indicates the name of the port as configured or shown in the **show snasw port** command.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 **snasw start port** command to enable a port that is defined to the configuration but is not active. Unless the **nostart** command is configured on the port definition, a port is started automatically. Use this command to start ports that have **nostart** configured or ports that have been stopped using the **snasw stop port** privileged EXEC command.

Examples

The following is an example of the **snasw start port** command:

```
Router# snasw start port TOKEN0
```

Related Commands

Command	Description
show snasw port	Displays the Switching Services (SNASw) port objects.
snasw stop port	Stops an active port.

snasw stop

To shut down Switching Services (SNASw), use the **snasw stop** command in privileged EXEC mode.

snasw stop

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 **snasw stop** command to terminate all sessions, stop all ports and links, and shut down SNASw. When you enter this command, you are prompted for confirmation.

Examples

The following is an example of the **snasw stop** command:

```
Router# snasw stop
```

Related Commands

Command	Description
snasw start	Starts SNASw.

snasw stop cp-cp

To terminate control point (CP)-CP sessions with a partner CP, use the **snasw stop cp-cp** command in privileged EXEC mode.

snasw stop cp-cp *cpname*

Syntax Description

cpname	Indicates the fully qualified CP name of the adjacent node with which CP-CP sessions should be stopped.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 primary National Number (NN) server (uplink) fails, CP-CP sessions are established with a backup, if one is available. When the link to the primary recovers, Switching Services (SNASw) retains the CP-CP sessions established with the backup and does not automatically switch back to the primary. To force SNASw to switch back to the primary, use the **snasw stop cp-cp** command. (If the link to the backup fails, SNASw does switch back to the primary automatically.)

You can also use the **snasw stop cp-cp** command to clear some fault scenarios, such as hung or nonresponsive CP sessions, allowing the Systems Network Architecture (SNA) switch to potentially restart sessions with the same or alternate destination logical unit (LU).

Examples

The following is an example of the **snasw stop cp-cp** command:

```
Router# snasw stop cp-cp NETA.CMCHOST
```

Related Commands

Command	Description
snasw start cp-cp	Initiates a request to start CP-CP sessions with a partner CP.

snasw stop link

To stop an active link, use the **snasw stop link** command in privileged EXEC mode.

snasw stop link *linkname*

Syntax Description

linkname	Indicates the name of the link as configured or shown in the **show snasw link** command.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 **snasw stop link** command to deactivate a link to a specified partner control point (CP). All High-Performance Routing (HPR) sessions established using the link are disconnected. HPR sessions are disrupted only if no alternate route is available.

Normally a link stopped with the **snasw stop link** command must be restarted by issuing the **snasw start link** command. However, it will be automatically restarted under the following conditions:

- The **nns** keyword is specified on the **snasw link** command, and
- The SNASw CP did not already re-establish CP-CP sessions with a network node server over another upstream link.

Examples

The following is an example of the **snasw stop link** command:

```
Router# snasw stop link CMCHOST1
```

Related Commands

Command	Description
show snasw link	Displays the Switching Services (SNASw) link objects.

snasw stop port

To stop an active port, use the **snasw stop port** command in privileged EXEC mode.

snasw stop port *portname*

Syntax Description

portname	Indicates the name of the port as configured or shown in the **show snasw port** command.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 **snasw stop port** command to disable a specified port without removing it from the configuration. All High-Performance Routing (HPR) sessions established using the port and all links are shut down on the port. HPR sessions are disrupted only if no alternate route is available.

Examples

The following is an example of the **snasw stop port** command:

```
Router# snasw stop port TOKEN0
```

Related Commands

Command	Description
snasw start port	Starts an inactive port.

snasw stop session

To terminate an active session, use the **snasw stop session** command in privileged EXEC mode.

snasw stop session *pcid*

Syntax Description

pcid	Procedure correlator ID in 16-digit hexadecimal form.

Defaults

No default behaviors or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0 T.
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 **snasw stop session** command is used to clear sessions that are active but in an indeterminate or hung state or if the session partner is not responsive.

You can also use the **snasw stop session** command to free a small amount of memory if the session is no longer being used to transport data and you do not expect to use the session later.

Examples

The following is an example of the **snasw stop session** command:

```
Router# snasw stop session C3BBD36EA9CBA1AF
```

Related Commands

Command	Description
show snasw session	Displays the Switching Services (SNASw) session objects.

source-bridge

To configure an interface for source-route bridging (SRB), use the **source-bridge** command in interface configuration mode. To disable source-route bridging on an interface, use the **no** form of this command.

source-bridge *source-ring-number bridge-number target-ring-number* [**conserve-ring**]

no source-bridge *source-ring-number bridge-number target-ring-number* [**conserve-ring**]

Syntax Description

source-ring-number	Ring number for the interface's Token Ring or FDDI ring. It must be a decimal number in the range from 1 to 4095 that uniquely identifies a network segment or ring within the bridged Token Ring or FDDI network
bridge-number	Number that uniquely identifies the bridge connecting the source and target rings. It must be a decimal number in the range from 1 to 15.
target-ring-number	Ring number of the destination ring on this router. It must be unique within the bridged Token Ring or FDDI network. The target ring can also be a ring group. Must be a decimal number.
conserve-ring	(Optional) Keyword to enable SRB over Frame Relay. When this option is configured, the SRB software does not add the ring number associated with the Frame Relay PVC (the partner's virtual ring) to outbound explorer frames. This option is permitted for Frame Relay subinterfaces only.

Defaults

SRB is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was revised to enable SRB over Frame Relay.
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 parser automatically displays the word "active" in the **source-bridge** command in configurations that have SRB enabled. You need not enter the **source-bridge** command with the **active** keyword.

Examples

In the following example, Token Rings 129 and 130 are connected via a router:

```
interface tokenring 0
```

```
 source-bridge 129 1 130
!
interface tokenring 1
 source-bridge active 130 1 129
```

In the following example, an FDDI ring on one router is connected to a Token Ring on a second router across a data-link switching plus (DLSw+) link:

```
dlsw local-peer peer-id 132.11.11.2
dlsw remote-peer 0 tcp 132.11.11.3
!
interface fddi 0
 no ip address
 multiring all
 source-bridge active 26 1 10
!
dlsw local-peer peer-id 132.11.11.3
dlsw remote-peer 0 tcp 132.11.11.2
!
interface tokenring 0
 no ip address
 multiring all
 source-bridge active 25 1 10
```

In the following example, a router forwards frames from a locally attached Token Ring over the Frame Relay using SRB:

```
source-bridge ring-group 200
!
interface Serial0
 encapsulation frame-relay
!
interface Serial0.30 point-to-point
 frame-relay interface-dlci 30 ietf
 source-bridge 100 1 200 conserve-ring
 source-bridge spanning
!
interface TokenRing0
 source-bridge 600 1 200
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
source-bridge ring-group	Defines or removes a ring group from the configuration.
source-bridge transparent	Establishes bridging between transparent bridging and SRB.

source-bridge connection-timeout

To establish the interval of time between first attempt to open a connection until a timeout is declared, use the **source-bridge connection-timeout** command in global configuration mode. To disable this feature, use the **no** form of this command.

source-bridge connection-timeout *seconds*

no source-bridge connection-timeout *seconds*

Syntax Description

seconds	Interval of time, in seconds, before a connection attempt to a remote peer is aborted. The default is 10 seconds.

Defaults

The default connection-timeout interval is 10 seconds.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **source-bridge connection-timeout** command is used for setting timeout intervals in a complex topology such as a large multihop WAN with virtual rings or satellite links. The timeout interval is used when a connection to a remote peer is attempted. If the timeout interval expires before a response is received, the connection attempt is aborted.

Examples

The following example sets the connection timeout interval to 60 seconds:

```
source-bridge connection-timeout 60
```

Related Commands

Command	Description
source-bridge ring-group	Defines or removes a ring group from the configuration.

source-bridge cos-enable

To force the Cisco IOS software to read the contents of the format identification (FID) frames to prioritize traffic when using TCP, use the **source-bridge cos-enable** command in global configuration mode. To disable prioritizing, use the **no** form of this command.

source-bridge cos-enable

no source-bridge cos-enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(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 prioritize your Systems Network Architecture (SNA) traffic across the backbone network. All your important front-end processor (FEP) traffic can flow on high-priority queues. This is useful only between FEP-to-FEP (physical unit [PU] 4-to-PU 4) communications (across the non-SNA backbone).

Note Logical Link Control, type 2 (LLC2) local acknowledgment must be turned on for the Class of Service (CoS) feature to take effect, and the **source-bridge remote-peer tcp** command with the **priority** keyword must be issued.

Examples

The following example enables CoS for prioritization of SNA traffic across a network:

```
source-bridge cos-enable
```

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 enable-80d5

To change the router's Token Ring to Ethernet translation behavior, use the **source-bridge enable-80d5** command in global configuration mode. To disable this function, use the **no** form of this command.

source-bridge enable-80d5

no source-bridge enable-80d5

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

The Cisco IOS software supports two types of Token Ring LLC2 to Ethernet conversion:

- Token Ring LLC2 to Ethernet 802.3 LLC2
- Token Ring LLC2 to Ethernet 0x80d5

Use this global configuration command to change the translation behavior. By default, the Cisco IOS software translates Token Ring LLC2 to Ethernet 802.3 LLC2. This command allows you to configure the software to translate Token Ring LLC2 frames into Ethernet 0x80d5 format frames.

This command is useful when you have a non-IBM device attached to an IBM network with devices that are using the nonstandard Token Ring LLC2 to Ethernet 80d5 translation. If you do not configure your router to enable 80d5 processing, the non-IBM and IBM devices will not be able to communicate.

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** command to verify that 80d5 processing is enabled. If it is, the following line is displayed in the output:

```
Translation between LLC2 and Ethernet Type II 80d5 is enabled
```

Examples

The following example enables 0x80d5 processing, removes the translation for service access point (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 sap-80d5	Allows 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, and allows the translation to be set on a per-DSAP basis.

source-bridge explorer-dup-ARE-filter

To filter out duplicate explorers in networks with redundant topologies, use the **source-bridge explorer-dup-ARE-filter** command in global configuration mode. To disable this feature, use the **no** form of this command.

source-bridge explorer-dup-ARE-filter

no source-bridge explorer-dup-ARE-filter

Syntax Description

This command has no arguments or keywords.

Defaults

Duplicate explorer filtering is disabled.

Command Modes

Global configuration

Command History

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

Examples

The following example enables duplicate explorer filtering:

```
source-bridge explorer-dup-ARE-filter
```

source-bridge explorer-fastswitch

To enable explorer fast switching, use the **source-bridge explorer-fastswitch** command in global configuration mode. To disable explorer fast switching, use the **no** form of this command.

source-bridge explorer-fastswitch

no source-bridge explorer-fastswitch

Syntax Description

This command has no arguments or keywords.

Defaults

Fast switching is enabled.

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

Use the **no** form of this command in conjunction with the **source-bridge explorerq-depth** and the **source-bridge explorer-maxrate** commands to optimize explorer processing.

Examples

The following example enables explorer fast switching after it has been previously disabled:

```
source-bridge explorer-fastswitch
```

Related Commands

Command	Description
source-bridge explorer-maxrate	Sets the maximum byte rate of explorers per ring.
source-bridge explorerq-depth	Sets the maximum explorer queue depth.

source-bridge explorer-maxrate

To set the maximum byte rate of explorers per ring, use the **source-bridge explorer-maxrate** command in global configuration mode. To reset the default rate, use the **no** form of this command.

source-bridge explorer-maxrate *maxrate*

no source-bridge explorer-maxrate *maxrate*

Syntax Description

maxrate	Number in the range from 100 to 1000000000 (in bytes per second). The default maximum byte rate is 38400 bytes per second.

Defaults

The default maximum byte rate is 38400 bytes per second.

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

Given the number of different explorer packet types and sizes and the bandwidth limits of the various interfaces, the bus data rate (as opposed to the packet rate) is the common denominator used to decide when to flush incoming explorers. The packets are dropped by the interface before any other processing.

Examples

The following command sets the maximum byte rate of explorers on a ring:

```
source-bridge explorer-maxrate 100000
```

source-bridge explorerq-depth

To set the maximum explorer queue depth, use the **source-bridge explorerq-depth** command in global configuration mode. To reset the default value, use the **no** form of this command.

source-bridge explorerq-depth *depth*

no source-bridge explorerq-depth *depth*

Syntax Description

depth	The maximum number of incoming packets. The valid range is from 1 to 500. The default is 30 packets.

Defaults

The default maximum depth is 30.

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

In this implementation, the maximum depth is set on a per-interface basis (default maximum depth is 30) therefore, each interface can have up to the maximum outstanding packets on the queue before explorers from that particular interface are dropped.

The **source-bridge explorerq-depth** command is used in a Token Ring and source-route bridging environment.

Examples

The following example sets the maximum explorer queue depth:

```
source-bridge explorerq-depth 100
```

Related Commands

Command	Description
dlsw explorerq-depth	Establishes queue depth for multiple queues that handle various types of explorer traffic.

source-bridge fst-peername

To set up a Fast-Sequenced Transport (FST) peer name, use the **source-bridge fst-peername** command in global configuration mode. To disable the IP address assignment, use the **no** form of this command.

source-bridge fst-peername *local-interface-address*

no source-bridge fst-peername *local-interface-address*

Syntax Description

local-interface-address	IP address to assign to the local router.

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 is the first step to configuring a remote source-route bridge to use FST.

Examples

The following example sets up an FST peer name:

```
source-bridge fst-peername 10.136.64.98
```

Related Commands

Command	Description
source-bridge remote-peer fst	Specifies an FST encapsulation connection.

source-bridge input-address-list

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

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

no source-bridge input-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
10.3	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 command filters source-routed packets received from the router interface based upon the source MAC address.

Examples

The following example assigns access list 700 to Token Ring 0:

```
access-list 700 deny 1000.5A00.0000  8000.00FF.FFFF
access-list 700 permit 0000.0000.0000  FFFF.FFFF.FFFF
!
interface tokenring 0
 source-bridge input-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 output-address-list	Applies an access list to an interface configured for SRB, and filters source-routed packets sent to the router interface based on the destination MAC address.

source-bridge input-lsap-list

To filter, on input, FDDI and IEEE 802-encapsulated packets that include the destination service access point (DSAP) and source service access point (SSAP) fields in their frame formats, use the **source-bridge input-lsap-list** command in interface configuration mode. To restore the default value, use the **no** form of this command.

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

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

Syntax Description

access-list-number	Number of the access list. This access list is applied to all IEEE 802 or FDDI frames received on that interface prior to the source-routing process. Specify zero (0) to disable the filter. The value must be in the range from 200 to 299.

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 access list specifying the type codes to be filtered is given by this variation of the **source-bridge** command in interface configuration mode.

Examples

The following example specifies access list 203:

```
interface tokenring 0
 source-bridge input-lsap-list 203
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
source-bridge output-lsap-list	Filters, on output, FDDI and IEEE 802-encapsulated packets that have DSAP and SSAP fields in their frame formats.

source-bridge input-type-list

To filter Subnetwork Access Protocol (SNAP)-encapsulated packets on input, use the **source-bridge input-type-list** command in interface configuration mode.

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

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

Syntax Description

access-list-number	Number of the access list. This access list is applied to all SNAP frames received on that interface prior to the source-routing process. 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

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

Use the **access list** command to specify type code when using the **source-bridge input-type-list** command.

Examples

The following example specifies access list 202:

```
access-list 202 deny 0x6000 0x0007
access-list 202 permit 0x0000 0xFFFF
!
interface tokenring 0
 source-bridge input-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 output-type-list	Filters SNAP-encapsulated frames by type code on output.

source-bridge keepalive

To assign the keepalive interval of the remote source-bridging peer, use the **source-bridge keepalive** command in interface configuration mode. To cancel previous assignments, use the **no** form of this command.

source-bridge keepalive *seconds*

no source-bridge keepalive

Syntax Description

seconds	Keepalive interval in seconds. The valid range is from 10 to 300. The default value is 30 seconds.

Defaults

30 seconds

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 sets the keepalive interval to 60 seconds:

```
source-bridge keepalive 60
```

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 largest-frame

To configure the largest frame size that is used to communicate with any peers in the ring group, use the **source-bridge largest-frame** command in global configuration mode. To cancel previous assignments, use the **no** form of this command.

source-bridge largest-frame *ring-group size*

no source-bridge largest-frame *ring-group*

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.
size	Maximum frame size. The default is that no frame size is assigned. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

Defaults

No frame size is assigned.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The Cisco IOS software negotiates all transit routes down to the specified size or lower. Use the *size* argument with this command to prevent timeouts in end hosts by reducing the amount of data they must send in a fixed interval. For example, in some networks containing slow links, it would be impossible to send an 8-KB frame and receive a response within a few seconds. These are standard defaults for an application on a 16-Mb Token Ring. If the frame size is lowered to 516 bytes, then only 516 bytes must be sent and a response received in 2 seconds. This feature is most effective in a network with slow links. The legal values for this argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800 bytes.

Examples

The following example sets the largest frame that can be sent through a ring group to 1500 bytes:

```
source-bridge largest-frame 8 1500
```

Related Commands

Command	Description
source-bridge ring-group	Defines or removes a ring group from the configuration.

source-bridge max-hops

To control the forwarding or blocking of all-route explorer frames received on an interface, use the **source-bridge max-hops** command in interface configuration mode. To reset the count to the maximum value, use the **no** form of this command.

source-bridge max-hops *count*

no source-bridge max-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 input frame plus hops appended by the router is fewer than or equal to the specified count. If the interface is connected to a destination interface, the router appends one hop. If the interface is tied to a virtual ring, the router appends two hops. This applies only to all-routes explorer frames on input to this interface.

Examples

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

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

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.
source-bridge max-in-hops	Controls the forwarding or blocking of spanning-tree explorer frames received on an interface.
source-bridge max-out-hops	Controls the forwarding or blocking of spanning-tree explorer frames sent from this interface.

source-bridge max-in-hops

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

source-bridge max-in-hops *count*

no source-bridge max-in-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 input frame is fewer than or equal to the specified count. This applies only to spanning-tree explorer frames input to the specified interface.

Examples

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

```
source-bridge max-in-hops 3
```

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-out-hops	Controls the forwarding or blocking of spanning-tree explorer frames sent from this interface.