default-profile

To specify the name of the profile to be applied as a default to all the listen points, use the **default-profile** command in security configuration mode. To disable the default profile specification, use the **no** form of this command.

default-profile *profilename*

no default-profile *profilename*

Syntax Description

profilename	A profile name that has already been configured.

Defaults

No default profile.

Command Modes

Security configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is configured, this profile name and all of its attributes will be associated with all listen points that do not specify an individual profile with the **sec-profile** command.

Profile names cannot be duplicated.

Entering the **no** form of this command removes the default specification and any listen points that do not have the **sec-profile** command specified will revert to a nonsecure mode.

This command has no retroactive effect. If a listen point is specified using the **listen-point** command, and the **sec-profile** command was already configured for that listen point, then all client connections to that listen point will be secure.

If a listen point is specified using the listen-point command, and the **default-profile** command is not configured, then all client connections to that listen point will not be secure. However, if the **default-profile** command is later configured, then all now connections to that listen point will be secure using the specified **default-profile** command. This will not affect the nonsecure connections.

Examples

The following example specifies DOMESTIC as the default profile name for all clients connecting to listen point 10.10.10.1 until the **default-profile LAM** command is configured. Once the **default-profile LAM** command is configured, all new client connections will use LAM as the default profile.

```
tn3270
 security
```

```
 profile NOSECURITY none
 default-profile DOMESTIC
pu DIRECT 012ABCDE tok 0 04
 default-profile LAM
listen-point 10.10.10.1
```

Related Commands

Command	Description
profile	Specifies a name and a security protocol for a security profile and enters profile configuration mode.
sec-profile	Specifies the security profile to be associated with a listen point.

disable (TN3270)

To turn off security in the TN3270 server, use the **disable** (TN3270) command in security configuration mode.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Security configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring the **disable** command does not terminate any active secure or nonsecure connections. This command specifies that all new connections established with the TN3270 server will be nonsecure. If a client initiates a change cipher specification for an existing secure connection, then the TN3270 server will process the request.

There is not a **no** form for this command. The **enable** command is equivalent to the **no** form of this command.

Examples

The following example turns off security in the TN3270 server so that all new connections established with the TN3270 server will be nonsecure:

```
disable
```

Related Commands

Command	Description
enable (TN3270)	Turns on security in the TN3270 server.

dlsw allroute-netbios

To change the single-route explorer to an all-route broadcast for NetBIOS, use the **dlsw allroute-netbios** command in global configuration mode. To return to the default single-route explorer, use the **no** form of this command.

dlsw allroute-netbios

no dlsw allroute-netbios

Syntax Description

This command has no arguments or keywords.

Defaults

Single-route explorer.

Command Modes

Global configuration

Command History

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

Examples

The following example specifies all-route broadcasts for NetBIOS:

```
dlsw allroute-netbios
```

dlsw allroute-sna

To change the single-route explorer to an all-route broadcast for Systems Network Architecture (SNA), use the **dlsw allroute-sna** command in global configuration mode. To return to the default single-route explorer, use the **no** form of this command.

dlsw allroute-sna

no dlsw allroute-sna

Syntax Description

This command has no arguments or keywords.

Defaults

Single-route explorer.

Command Modes

Global configuration

Command History

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

Examples

The following example specifies all-route broadcasts for SNA:

```
dlsw allroute-sna
```

dlsw bgroup-list

To map traffic on the local Ethernet bridge group interface to remote peers, use the **dlsw bgroup-list** command in global configuration mode. To cancel the map, use the **no** form of this command.

dlsw bgroup-list *list-number* **bgroups** *number*

no dlsw bgroup-list

Syntax Description

list-number	The ring list number. This number is subsequently used in the **dlsw remote-peer** command to define the segment to which the bridge group should be applied. The valid range is from 1 to 255.
bgroups *number*	The transparent bridge group list number. The valid range is from 1 to 63.

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

Traffic received from a remote peer is forwarded only to the bridge group specified in the bridge group list. Traffic received from a local interface is forwarded to peers if the input bridge group number appears in the bridge group list applied to the remote peer definition. The definition of a bridge group list is optional. Each remote peer has a single list number associated with it; therefore, if you want traffic to go to a bridge group and to either a ring list or port list, you should specify the same list number in each definition.

Examples

The following example configures bridge group list 1:

```
dlsw bgroup-list 1 bgroups 33
```

Related Commands

Command	Description
dlsw bridge-group	Links data-link switching plus (DLSw+) to the bridge group of the Ethernet LANs.
dlsw ring-list	Configures a ring list, mapping traffic on a local interface to remote peers.

dlsw bridge-group

To link data-link switching plus (DLSw+) to the bridge group of the Ethernet LANs, use the **dlsw bridge-group** command in global configuration mode. To disable the link, use the **no** form of this command.

dlsw bridge-group *group-number* [**llc2** [**N2** *number*] [**ack-delay-time** *milliseconds*] [**ack-max** *number*] [**idle-time** *milliseconds*] [**local-window** *number*] [**t1-time** *milliseconds*] [**tbusy-time** *milliseconds*] [**tpf-time** *milliseconds*] [**trej-time** *milliseconds*] [**txq-max** *number*] [**xid-neg-val-time** *milliseconds*] [**xid-retry-time** *milliseconds*]] [**locaddr-priority** *lu address priority list number*] [**sap-priority** *priority list number*]

no dlsw bridge-group *group-number* [**llc2** [**N2** *number*] [**ack-delay-time** *milliseconds*] [**ack-max** *number*] [**idle-time** *milliseconds*] [**local-window** *number*] [**t1-time** *milliseconds*] [**tbusy-time** *milliseconds*] [**tpf-time** *milliseconds*] [**trej-time** *milliseconds*] [**txq-max** *number*] [**xid-neg-val-time** *milliseconds*] [**xid-retry-time** *milliseconds*]] [**locaddr-priority** *lu address priority list number*] [**sap-priority** *priority list number*]

Syntax Description

group-number	Transparent bridge group to which DLSw+ will be attached. The valid range is from 1 to 63.
llc2	(Optional) Logical Link Control, type 2 (LLC2) interface subcommands.
N2 *number*	(Optional) Number of times router should retry various operations. The valid range is from 1 to 255.
ack-delay-time *milliseconds*	(Optional) Maximum time the router allows incoming I-frames to stay unacknowledged. The valid range is from 1 to 60000.
ack-max *number*	(Optional) Maximum number of I-frames received before an acknowledgment must be sent. The valid range is from 1 to 255.
idle-time *milliseconds*	(Optional) Frequency of polls during periods of idle traffic. The valid range is from 1 to 60000.
local-window *number*	(Optional) Maximum number of I-frames to send before waiting for an acknowledgment. The valid range is from 1 to 127.
t1-time *milliseconds*	(Optional) Amount of time the router waits for an acknowledgment to sent I-frames. The valid range is from 1 to 60000.
tbusy-time *milliseconds*	(Optional) Amount of time the router waits while the other LLC2 station is in a busy state before attempting to poll the remote station. The valid range is from 1 to 60000.
tpf-time *milliseconds*	(Optional) Amount of time the router waits for a final response to a poll frame before resending the original poll frame. The valid range is from 1 to 60000.
trej-time *milliseconds*	(Optional) Amount of time the router waits for a resend of a rejected frame before sending the reject command. The valid range is from 1 to 60000.
txq-max *number*	(Optional) Queue for holding LLC2 information frames. The valid range is from 20 to 200.
xid-neg-val-time *milliseconds*]	(Optional) Frequency of exchange of identification (XID). The valid range is from 1 to 60000.

xid-retry-time *milliseconds*	(Optional) Amount of time the router waits for reply to XID. The valid range is from 1 to 60000.
locaddr-priority *lu address priority list number*	(Optional) Assigns an input Systems Network Architecture (SNA) logical unit (LU) address priority list to this bridge group. The valid range is from 1 to 10.
sap-priority *priority list number*	(Optional) Assigns an input service access point (SAP) priority list to this bridge group. The valid range is from 1 to 10.

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 Guideliness

More than one bridge group can be attached to DLSw+ by using this command multiple times. Multiple bridge group support is available in Cisco IOS Release 11.3.

Examples

The following example links DLSw+ to bridge groups 1, 2, and 3:

```
dlsw local-peer peer-id 1.1.1.1
dlsw remote-peer 0 tcp 2.2.2.2
dlsw bridge-group 1
dlsw bridge-group 2
dlsw bridge-group 3

interface Ethernet0
 bridge-group 1

interface Ethernet1
 bridge-group 2

interface Ethernet2
 bridge-group 3

bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
```

Related Commands

Command	Description
dlsw bgroup-list	Maps traffic on the local Ethernet bridge group interface to remote peers.

dlsw cache-ignore-netbios-datagram

To prevent data-link switching (DLSw) from caching NetBIOS names when a datagram (0x08) NetBIOS command is received, use the **dlsw cache-ignore-netbios-datagram** command in global configuration mode. To remove the filter, use the **no** form of this command.

dlsw cache-ignore-netbios-datagram

no dlsw cache-ignore-netbios-datagram

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Examples

The following example helps maintain a smaller name cache:

```
dlsw cache-ignore-netbios-datagram
```

dlsw disable

To disable data-link switching plus (DLSw+) without altering the configuration, use the **dlsw disable** command in global configuration mode. To reenable DLSw+, use the **no** form of this command.

dlsw disable

no dlsw disable

Syntax Description

This command has no arguments or keywords.

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.

Examples

The following example reenables DLSw+:

```
no dlsw disable
```

dlsw duplicate-path-bias

To specify how data-link switching plus (DLSw+) handles duplicate paths to the same MAC address or NetBIOS name, use the **dlsw duplicate-path-bias** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw duplicate-path-bias [**load-balance**]

no dlsw duplicate-path-bias [**load-balance**]

Syntax Description

load-balance	(Optional) Specifies that sessions are load-balanced across duplicate paths.

Defaults

Fault tolerance is the default logic used to handle duplicate paths.

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

A path is either a remote peer or a local port.

In full-tolerance mode, the preferred path is always used unless it is unavailable. The preferred path is either the path over which the first response to an explorer was received, or, in the case of remote peers, the peer with the least cost.

Examples

The following example specifies load balancing to resolve duplicate paths:

```
dlsw duplicate-path-bias load-balance
```

dlsw explorerq-depth

To establish queue depth for multiple queues that handle various types of explorer traffic, including Systems Network Architecture (SNA) and NetBIOS frames, use the **dlsw explorerq-depth** command in global configuration mode. To remove the queues, use the **no** form of this command.

dlsw explorerq-depth {**sna** *value* | **netbios** *value* | **other** *value*}

no dlsw explorerq-depth {**sna** *value* | **netbios** ***value*** | **other** *value*}

Syntax Description

sna *value*	Establishes queue depth for SNA frames. The valid range is from 10 to 1000. The default is unlimited.
netbios *value*	Establishes queue depth for NetBIOS frames. The valid range is from 10 to 1000. The default is unlimited.
other *value*	Establishes queue depth for unnumbered information (UI) frames. The valid range is from 10 to 1000. The default is 100.

Defaults

The default value for the **sna** queue and **netbios** queue is unlimited (that is, if no value is specified, there is no threshold for these queues). The default for the **other** queue is 100.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3 (1)	This command was removed from Cisco IOS software.
12.1 (3)T	This command was reintroduced to Cisco IOS software.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **dlsw explorererq-depth** command allows data-link switching plus (DLSw+) to establish queue depth for multiple queues that handle different types of traffic, including SNA and NetBIOS frames. UI frames are handled by the **other** queue. Using multiple queues, the SNA and NetBIOS frames will take priority over the UI frames. The UI frames will be dropped when the **other** queue reaches its threshold.

The **dlsw explorererq-depth** command is used in an Ethernet and transparent-bridging environment.

Examples

The following example specifies the maximum number of explorers allowed in the SNA queue:

```
dlsw explorerq-depth sna 100
```

Related Commands

Command	Description
source-bridge explorerq-depth	Sets the maximum explorer queue depth.

dlsw group-cache disable

To disable the border peer caching feature, use the **dlsw group-cache disable** command in global configuration mode. To return to the default peer caching feature, use the **no** form of this command.

dlsw group-cache disable

no dlsw group-cache disable

Syntax Description

This command has no arguments or keywords.

Defaults

Border peer caching is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

If a border peer becomes a nonborder peer, then the group cache is automatically deleted.

This command prevents a border peer from learning reachability information from relay responses. This command also prevents a border peer from using local or remote caches to make forwarding decisions.

Examples

The following example disables the group cache:

```
dlsw group-cache disable
```

Related Commands

Command	Description
dlsw group-cache max-entries	Limits the number of entries in the group cache.

dlsw group-cache max-entries

To limit the number of entries in the group cache, use the **dlsw group-cache max entries** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw group-cache max-entries *number*

no dlsw group-cache max entries

Syntax Description

number	Maximum number of entries allowed in the group cache. The valid range is from 0 through 12000. If the value is set to 0, then there is no limit to the number of entries. The default is 2000.

Defaults

The default setting is 2000.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Once the number of entries has reached the maximum number specified, if a new entry needs to be added an entry will be removed to make room.

The value set for the *number* argument applies to both the NetBIOS and Systems Network Architecture (SNA) group cache.

Examples

The following configuration defines the maximum number of entries allowed in the NetBIOS or SNA group cache as 1800:

```
dlsw group-cache max-entries 1800
```

Related Commands

Command	Description
dlsw group-cache disable	Disables the border peer caching feature.

dlsw history-log

To enable the data-link switching (DLSw) history log, use the **dlsw history-log** command in global configuration mode. To disable the DLSw history log, use the **no** form of this command.

dlsw history-log *size* [**connected-only**] [**ignore-info-frames**]

no dlsw history-log

Syntax Description

size	Specifies the number of circuits for which to retain history. The history size per circuit is fixed at the last 16 events. The *size* argument can range from 16 to 65536. The default value is 32.
connected-only	(Optional) Specifies that history will be recorded only for circuits that reach the CONNECTED state, and only finite state machines (FSM) events following the move to the CONNECTED state will be retained.
ignore-info-frames	(Optional) Specifies that the following FSM events will not be recorded in the history: • WAN infoframe • WAN dgmframe • Data-link control (DLC) udata.ind • DLC data.ind

Defaults

The DLSw history log is enabled with a value of 32 for the *size* argument.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The command was enabled by default with a value of 32 for the *size* 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.

Examples

The following example configures the DLSw history log size to 2000 circuits and specifies that history be recorded only for circuits that reach the CONNECTED state:

```
router(config)# dlsw history-log 2000 connected-only
```

dlsw icannotreach saps

To configure a list of service access points (SAPs) not locally reachable by the router, use the **dlsw icannotreach saps** command in global configuration mode. To remove the list, use the **no** form of this command.

dlsw icannotreach saps *sap*

no dlsw icannotreach saps *sap*

Syntax Description

sap	One or more SAPs, separated by spaces.

Defaults

No lists are configured.

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 **dlsw icannotreach saps** command causes the local router to send a control vector to its peers during the capabilities exchange, which tells the peers not to send canureach messages to the local router for sessions using those destination service access point (DSAP)s. (They are DSAPs from the peer's perspective, and source service access point (SSAP)s from the perspective of the devices attached to the local router.) The effect is that devices attached to the peer will not be able to initiate sessions to devices attached to the local router using the listed DSAPs. Devices attached to the local router, however, will still be able to start sessions with devices on its peers using the listed SAP as SSAPs. The reason is that the local router can still send canureach requests to its peers,because no filtering is actually done on the local router. The filtering done by the peers does not prohibit the peers from responding to canureach requests from the local router sending the control vector, only sending canureach requests to the local router.

Examples

The following example specifies that NetBIOS traffic will be denied:

```
dlsw icannotreach saps F0
```

dlsw icanreach

To configure a resource that is locally reachable by this router, use the **dlsw icanreach** command in global configuration mode. To remove the resource, use the **no** form of this command.

dlsw icanreach {**mac-exclusive** [**remote**] | **netbios-exclusive** [**remote**] | **mac-address** *mac-addr* [**mask** *mask*] | **netbios-name** *name* | **saps** *sap-value*}

no dlsw icanreach {**mac-exclusive** [**remote**] | **netbios-exclusive** [**remote**] | **mac-address** *mac-add* [**mask** *mask*] | **netbios-name** *name* | **saps** *sap-value*}

Syntax Description

mac-exclusive	Router can reach only the MAC addresses that are user configured.
remote	(Optional) Gives the MACs (that are local to the router and that are not already defined in the **dlsw icanreach mac-address** *mac-addr* command) access to remote MAC addresses.
netbios-exclusive	Router can reach only the NetBIOS names that are user configured.
remote	(Optional) Gives the NetBIOS workstations (that are local to the router and that are not already defined in the **dlsw icanreach netbios-name** *name* command) access to remote servers.
mac-address *mac-addr*	Configures a MAC address that this router can locally reach.
mask *mask*	(Optional) MAC address mask in hexadecimal *h.h.h*. The “f” value represents the “care” bit and the “0” value represents the “don’t care” bit. The mask indicates which bits in the MAC address are relevant.
netbios-name *name*	Configures a NetBIOS name that this router can locally reach. Wildcards (*) are allowed at the end of the name. Trailing white spaces are ignored when comparing against an actual name in a NetBIOS frame.
saps	Configures a list of SAPs that are locally reachable by this router.
sap-value	Even SAP value, in hex.

Defaults

No resources are configured.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
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 can be entered at any time. It causes a capabilities exchange to relay the information to all active peers. By specifying resource names or MAC addresses in this command, you can avoid broadcasts from remote peers that are looking for this resource. By specifying “exclusive” you can avoid

broadcasts to this router or any resources. For example, you could configure the front-end processor (FEP) MAC address or corporate site LAN servers in central site routers to avoid any broadcasts over the WAN for these resources.

Configuring the **remote** keyword gives the NetBIOS workstations and MACs that are local to the router and that are not already defined in the **dlsw icanreach netbios-name** *name* and **dlsw icanreach mac-address** *mac-addr* commands access to remote NetBIOS servers and remote MAC addresses. The connection must be from the local Netbios workstation or MAC address to the remote Netbios Server or MAC address.

In the default case (where the **remote** keyword is not specified), a local NetBIOS station that is not configured in the **icanreach netbios-name** list will not be able to make a connection in this router over data-link switching plus (DLSw+), whether incoming or outgoing.

Note Because the configuration of the **mac-address** and **netbios-name** keywords prevents the DLSw+ peer from exploring, an incorrect configuration could prevent DLSw+ from being able to find a resource actually available elsewhere in the network.

Examples

The following example indicates that this peer has information only has information about a single NetBIOS server, and that no peers should send this peer explorers searching for other NetBIOS names. Because the **remote** option is also configured, NetBIOS workstations that are connected to the NetBIOS server named lanserv will be able to establish a DLSw+ connection:

```
dlsw icanreach netbios-exclusive
dlsw icanreach netbios-name lanserv
```

Related Commands

Command	Description
show dlsw capabilities	Displays the configuration of a specific peer or all peers.

dlsw llc2 nornr

To prevent the receiver not ready (RNR) message from being sent while establishing a Logical Link Control, type 2 (LLC2) connection, use the **dlsw llc2 nornr** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw llc2 nornr

no dlsw llc2 nornr

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled by default.

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

This command is used when any device does not handle the LLC2 RNR frames.

Examples

The following example keeps the receiver not ready (RNR) message from being sent when establishing an LLC2 connection:

```
dlsw llc2 nornr
```

The following is output from a Sniffer trace showing when use of the **dlsw llc2 nornr** command would be appropriate because the RNR message is being rejected from the front-end processor (FEP) when the router is trying to establish an LLC2 connection:

```
SUMMARY  Delta T    From 400020401003               From 400023491026
8     0.173                                    LLC C D=00 S=04 TEST P
9     0.003   LLC R D=04 S=00 TEST F
10    0.002                                    SNA XID Fmt 2 T4
11    0.059   SNA XID Fmt 2 T4
12    0.004                                    SNA XID Fmt 2 T4
13    0.065   SNA XID Fmt 2 T4
14    0.005                                    SNA XID Fmt 2 T4
16    0.054   LLC C D=04 S=04 SABME P
17    0.003                                    LLC R D=04 S=04 UA
```

The router sends an RNR message:

```
18    0.001   LLC C D=04 S=04 RNR NR=0
```

From frames 19 to 35, the FEP does not respond:

```
19    0.002   LLC C D=04 S=04 RR NR=0
20    0.048   SNA  C NC  NC-ER-OP
21    0.997   LLC C D=04 S=04 RR NR=0 P
22    1.000   LLC C D=04 S=04 RR NR=0 P
24    1.000   LLC C D=04 S=04 RR NR=0 P
25    1.000   LLC C D=04 S=04 RR NR=0 P
31    1.000   LLC C D=04 S=04 RR NR=0 P
32    1.000   LLC C D=04 S=04 RR NR=0 P
34    1.000   LLC C D=04 S=04 RR NR=0 P
35    1.000   LLC C D=04 S=04 RR NR=0 P
```

The router disconnects the circuit:

```
37    1.000   LLC C D=04 S=04 DISC P
38    0.002                                   LLC R D=04 S=04 UA F
```

The sequence repeats:

```
39    0.179                                   LLC C D=00 S=04 TEST P
41    0.767   SNA XID Fmt 2 T4
42    0.634   SNA XID Fmt 2 T4
43    0.173                                   LLC C D=00 S=04 TEST
44    0.003   LLC R D=04 S=00 TEST F
45    0.002                                   SNA XID Fmt 2 T4
46    0.060   SNA XID Fmt 2 T4
47    0.004                                   SNA XID Fmt 2 T4
48    0.063   SNA XID Fmt 2 T4
49    0.005                                   SNA XID Fmt 2 T4
```

dlsw load-balance

To enable load balancing and to select either round robin or circuit-count-based load balancing, use the **dlsw load-balance** command in global configuration mode. To disable the previous assignments, use the **no** form of this command.

dlsw load-balance [**round-robin** | **circuit-count** *circuit-weight*]

no dlsw load-balance [**round-robin** | **circuit-count** *circuit-weight*]

Syntax Description

round-robin	(Optional) Enables round-robin type of load balancing.
circuit-count *circuit-weight*	(Optional) Enables the data-link switching plus (DLSw+) Enhanced Load Balancing feature. The value represents the default circuit weight to be used for the peers that are not explicitly configured with a circuit-weight value in the **dlsw remote-peer tcp** command. The valid range is from 1 to 100.

Defaults

Fault-tolerant mode is the default setting. The default value for the *circuit weight* argument is 10.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A circuit is never be taken down and reestablished by the code in an attempt to rebalance the load. The DLSw+ Enhanced Load Balancing feature changes the decision-making process only at the time a new circuit is desired.

The **dlsw load-balance** command replaces the **dlsw duplicate-path-bias load balance** command. The latter command continues to be accepted, however, it will be converted to the new command if the configuration is displayed or saved.

Examples

The following example enables the DLSw+ Enhanced Load Balancing feature:

```
dlsw load-balance circuit-count 10
```

dlsw local-peer

To define the parameters of the data-link switching plus (DLSw+) local peer, use the **dlsw local-peer** command in global configuration mode. To cancel the definitions, use the **no** form of this command.

dlsw local-peer [**cluster** *cluster-id*] [**peer-id** *ip-address*] [**group** *group*] [**border**] [**cost** *cost*] [**lf** *size*] [**keepalive** *seconds*] [**passive**] [**promiscuous**] [**biu-segment**] [**init-pacing-window** *size*] [**max-pacing-window** *size*]

no dlsw local-peer [**cluster** *cluster-id*] [**peer-id** *ip-address*] [**group** *group*] [**border**] [**cost** *cost*] [**lf** *size*] [**keepalive** *seconds*] [**passive**] [**promiscuous**] [**biu-segment**] [**init-pacing-window** *size*] [**max-pacing-window** *size*]

Syntax Description

cluster *cluster-id*	(Optional) Implements the DLSw+ Peer Clusters feature and defines the router as part of a particular cluster. The valid range is from 1 to 255.
peer-id *ip-address*	(Optional) Local peer IP address. This address is required when Fast-Sequenced Transport (FST) or TCP is used.
group *group*	(Optional) Peer group number for this router. The valid range is from 1 to 255.
border	(Optional) Enables the router as a border peer. The **group** option must be specified to use the border peer option.
cost *cost*	(Optional) Peer cost advertised to remote peers in the capabilities exchange. The valid range is from 1 to 5.
lf *size*	(Optional) Largest frame size for this local peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
keepalive *seconds*	(Optional) Default remote peer keepalive interval in seconds. The valid range is from 0 to 1200 seconds. The default is 30 seconds. The value 0 means no keepalives.
passive	(Optional) Specifies that this router does not initiate remote peer connections to configured peers.
promiscuous	(Optional) Accept connections from nonconfigured remote peers.
biu-segment	(Optional) DLSw+ spoofs the maximum receivable I-frame size in exchange identification (XID) so that each end station sends its largest frame.
init-pacing-window *size*	(Optional) Size of the initial pacing window as defined in RFC 1795. The valid range is from 1 to 2000.
max-pacing-window *size*	(Optional) Maximum size of the pacing window as defined in RFC 1795. The valid range is from 1 to 2000.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The **cluster** 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

When there are multiple peers to a given destination, use the **cost** keyword to determine which router is preferred and which is capable. The **cost** keyword applies only in fault tolerance mode.

The **biu-segment** option is a performance and utilization improvement. If a frame that arrives from a remote peer is too large for the destination station to handle, DLSw+ segments the frame. If you choose to implement this option, you must add the option to both DLSw peer partners.

Examples

The following command defines the local peer IP address and specifies the peer group number for this router:

```
dlsw local-peer peer-id 10.2.17.1 group 2
```

Related Commands

Command	Description
dlsw duplicate-path-bias	Specifies how DLSw+ handles duplicate paths to the same MAC address or NetBIOS name.
show dlsw capabilities	Displays the configuration of a specific peer or all peers.

dlsw mac-addr

To configure a static MAC address, use the **dlsw mac-addr** command in global configuration mode. To cancel the configuration, use the **no** form of this command.

dlsw mac-addr *mac-addr* {**ring** *ring-number* | **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*}| **rif** *rif-string* | **group** *group*}

no dlsw mac-addr *mac-addr* {**ring** *ring -number*| **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*}| **rif** *rif-string* | **group** *group*}

Syntax Description

mac-addr	Specifies the MAC address.
ring *ring-number*	Maps the MAC address to a ring number or ring group number. The valid range is from 1 to 4095.
remote-peer	Maps the MAC address to a specific remote peer.
interface serial *number*	Specifies the remote peer by direct serial interface.
ip-address *ip-address*	Specifies the remote peer by IP address.
rif *rif-string*	Maps the MAC address to a local interface using a Routing Information Field (RIF) string. The RIF string describes a source-routed path from the router to the MAC address. It starts at the router's ring group and ends on the ring where the MAC address is located. The direction is from the router toward the MAC address. See the IEEE 802.5 standard for details.
group *group*	Maps the MAC address to a specified peer group. Valid numbers are in the range from 1 to 255.

Defaults

No static MAC address is configured.

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

You can statically define resources to prevent the Cisco IOS software from sending explorer frames for the specified resource. For example, you can include the MAC address of a front-end processor (FEP) in the configuration for each remote router to eliminate any broadcasts that are searching for a FEP.

Alternately, you can specify a single **dlsw icanreach** statement in the router attached to the FEP indicating the MAC address of the FEP. This information is sent to all remote routers as part of the capabilities exchange.

Note Because the configuration of this command prevents the data-link switching plus (DLSw+) peer from exploring, an incorrect configuration could prevent DLSw+ from being able to find a resource actually available elsewhere in the network.

Examples

The following example maps the static MAC address 1000.5A12.3456 to the remote peer at IP address 10.17.3.2:

```
dlsw mac-addr 1000.5A12.3456 remote-peer ip-address 10.17.3.2
```

Related Commands

Command	Description
show dlsw reachability	Displays DLSw+ reachability information.

dlsw max-multiple-rifs

To enable caching of multiple Routing Information Field (RIF)s per interface, use the **dlsw max-multiple-rifs** command in global configuration mode. To turn off the feature, use the **no** form of this command.

dlsw max-multiple-rifs *multiple-rifs-per-port*

no dlsw max-multiple-rifs *multiple-rifs-per-port*

Syntax Description

multiple-rifs-per-port	Number of multiple RIF entries per interface. The valid range is from 1 to 4. The default value is 1.

Defaults

The default value is 1.

Command Modes

Global configuration

Command History

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

Usage Guidelines

A MAC address or NetBIOS name can have several RIF entries. Prior to this command, data-link switching plus (DLSw+) could cache only one of these RIF entries per local Token Ring port. With the **dlsw max-multiple-rifs** command configured, however, DLSw+ can cache multiple RIF entries (up to four) for a specific MAC address or NetBIOS name on one Token Ring port.

If the value 1 is specified, multiple RIF caching is not enabled.

Examples

The following example enables the router to cache up to two RIFs per interface:

```
dlsw max-multiple-rifs 2
```

dlsw multicast

To enable a DLSw router to participate in a multicast group, use the **dlsw multicast** command in global configuration mode. To remove the router from the multicast group, use the **no** form of this command.

dlsw multicast [*multicast-ip-address*]

no dlsw multicast [*multicast-ip-address*]

Syntax Description

multicast-ip-address	(Optional) The IP address used by the multicast group. The default is 224.0.10.0.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.0	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 order for routers to be able to receive multicast traffic through DLSw, they must be properly configured to receive multicasts. The appropriate multicast configuration will depend on the specific topologies used.

The **dlsw multicast** command is implemented together with the DLSw version 2 support (RFC2166). It allows anybody-to-anybody communication without configuring a full mesh of the DLSw peers.

Examples

The following example configures a router to be part of the multicast group using 224.0.11.0 as the multicast address:

```
dlsw local-peer peer-id 172.18.62.11 promiscuous
dlsw multicast 224.0.11.0
```

dlsw netbios-cache-length

To customize the number of characters of a NetBIOS name that are retained in the cache, use the **dlsw netbios-cache-length** command in global configuration mode. To restore the default cache length, use the **no** form of this command.

dlsw netbios-cache-length [**15** | **16**]

no dlsw netbios-cache-length

Syntax Description

15	The first 15 characters of NetBIOS names are cached.
16	The full 16 characters of NetBIOS names are cached.

Defaults

The first 15 characters of NetBIOS names are cached.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)	This command was introduced.
12.3(4)T	This command is no longer supported in Cisco_IOS Mainline or Technology-based (T) releases. It may continue to appear in Cisco_IOS 12.2S-family releases.
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

Configure the cache length to 16 characters only if the router will be dealing with NetBIOS names that differ only in the 16th byte.

Examples

The following example configures the cache to retain the full 16 characters of the NetBIOS name:

```
router(config)# dlsw netbios-cache-length 16
```

The following command restores the default behavior of caching only the first 15 characters of the NetBIOS name:

```
router(config)# no dlsw netbios-cache-length
```

dlsw netbios-keepalive-filter

To enable the NetBIOS dial-on-demand routing (DDR) feature, use the **dlsw netbios-keepalive-filter** command in global configuration mode. To turn off the feature, use the **no** form of this command.

dlsw netbios-keepalive-filter

no dlsw netbios-keepalive-filter

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelines

Refer to the "Cisco IOS Bridging and IBM Networking Overview" chapter of the *Cisco IOS Bridging and IBM Networking Configuration Guide* for more details on the NetBIOS DDR feature.

Examples

The following example enables NetBIOS DDR:

```
dlsw netbios-keepalive-filter
```

dlsw netbios-name

To configure a static NetBIOS name, use the **dlsw netbios-name** command in global configuration mode. To cancel the configuration, use the **no** form of this command.

dlsw netbios-name *netbios-name* {**ring** *ring-number* | **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*}| **rif** *rif-string* | **group** *group*}

no dlsw netbios-name *netbios-name* {**ring** *ring-number* | **remote-peer** {**interface serial** *number* | **ip-address** *ip-address*}| **rif** *rif-string* | **group** *group*}

Syntax Description

netbios-name	Specifies the NetBIOS name. Wildcards are allowed.
ring *ring number*	Maps the NetBIOS name to a ring number or ring group number. Test frames for this name will be sent only to LAN ports in this ring group.
remote-peer	Maps the NetBIOS name to a specific remote peer.
interface serial *number*	Specifies the remote peer by direct interface.
ip-address *ip-address*	Specifies the remote peer by IP address.
rif *rif- string*	Maps the MAC address to a local interface using a Routing Information Field (RIF) string. The RIF string describes a source-routed path from the router to the MAC address, starting at the router's ring-group and ending on the ring where the MAC address is located. The direction is from the router toward the MAC address. See the IEEE 802.5 standard for details.
group *group*	Maps the NetBIOS name to a specified peer group. Valid numbers are in the range from 1 to 255.

Defaults

No static NetBIOS name is configured.

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

Because the configuration of this command prevents the data-link switching plus (DLSw+) peer from exploring, an incorrect configuration could prevent DLSw+ from being able to find a resource actually available elsewhere in the network.

Examples

```
dlsw netbios-name netbios-1 remote-peer ip-address 10.132.248.5
```

Related Commands

Command	Description
show dlsw reachability	Displays DLSw+ reachability information.

dlsw peer-log-changes

To enable the logging of Syslog messages related to DLSw peer state changes, use the **dlsw peer-log-changes** global configuration command. To disable the logging of Syslog messages related to DLSw peer state changes, use the **no** form of this command.

dlsw peer-log-changes [**extend**]

no dlsw peer-log-changes

Syntax Description

extend	(Optional) Enables more verbose logging of messages, beyond the basic connection and disconnection messages.

Defaults

Disabled

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

When the **dlsw peer-log-changes** command is enabled, Syslog messages are generated for the following events:

- Connection attempt to a DLSw peer.
- Successful connection to a DLSw peer.
- Disconnection from a DLSw peer

When the **extended** keyword is enabled, Syslog messages are also generated for the following events:

- DLSw peer keepalive failure.
- DLSw TCP peer receives a TCP FINI.
- The configuration contains a promiscuous mismatch.
- Error when opening a priority peer.
- Explanation of why a backup peer was closed (such as linger timer expired or last circuit gone).

Examples

The following example enables verbose logging of Syslog messages related to DLSw peer state changes:

```
Router(config)# dlsw peer-log-changes extended
```

dlsw peer-on-demand-defaults

To configure defaults for peer-on-demand transport, use the **dlsw peer-on-demand-defaults** command in global configuration mode. To disable the previous assignment, use the **no** form of this command.

dlsw peer-on-demand-defaults [**fst**] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *destination-mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**inactivity** *minutes*] [**keepalive** *seconds*] [**lf** size] [**lsap-output-list** *list*] [**port-list** *port-list-number*] [**priority**] [**rsvp** {**global** | *average-bit-rate maximum burst*}] [**tcp-queue-max**]

no dlsw peer-on-demand-defaults [**fst**] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *destination-mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**inactivity** *minutes*] [**keepalive** *seconds*] [**lf** size] [**lsap-output-list** *list*] [**port-list** *port-list-number*] [**priority**] [**rsvp** {**global** | *average-bit-rate maximum burst*}] [**tcp-queue-max**]

Syntax Description

fst	(Optional) Use Fast Sequenced Transport (FST) encapsulation for all peers-on-demand established by this router.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for peer-on-demand peers. The *bytes-list-name* value is the name of the previously defined NetBIOS bytes access list filter.
cost *cost*	(Optional) Specifies the cost to reach peer-on-demand peer. The valid range is from 1 to 5. The default cost is 3.
dest-mac *destination-mac-address*	(Optional) Specifies the exclusive destination MAC address for peer-on-demand peers.
dmac-output-list *access-list-number*	(Optional) Specifies the filter output destination MAC addresses.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for peer-on-demand peers. The *host-list-name* value is the name of the previously defined NetBIOS host access list filter.
inactivity *minutes*	(Optional) Configures the length of time after the peer's circuit count is 0 that the peer-on-demand is disconnected. The valid range is from 0 to 1440 seconds. The default is 600 seconds.
keepalive *seconds*	(Optional) Configures the peer-on-demand keepalive interval. The valid range is from 0 to 1200 seconds. The default is 30 seconds.
lf *size*	(Optional) Largest frame size for this remote peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
lsap-output-list *list*	(Optional) Configures local service access point (LSAP) output filtering for peer-on-demand peers. Valid numbers are in the range from 200 to 299.
port-list *port-list-number*	(Optional) Configures a port list for peer-on-demand peers. Valid numbers are in the range from 0 to 4095.

priority	(Optional) Configures prioritization for peer-on-demand peers. The default state is off.
rsvp global	(Optional) Sets the Resource Reservation Protocol (RSVP) parameters to the global values specified in the **dlsw rsvp** command.
rsvp *average-bit-rate*	(Optional) Average bit rate (kilobits per second) to reserve up to 75 percent of total bits on the interface. The valid range is from 0 to 4294967.
maximum-burst	(Optional) Maximum burst size (kilobytes of data in queue). The valid range is from 0 to 4294967.
tcp-queue-max	(Optional) Configures the maximum output TCP queue size for peer-on-demand peers.

Defaults

The default peer-on-demand transport is TCP. The default **cost** is 3.
The default **inactivity** is 600 seconds.
The default **keepalive** is 30 seconds.
The default **priority** state is off.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(3)T	The **rsvp** 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

A peer-on-demand peer is a nonconfigured remote peer that was connected because of a Logical Link Control, type 2 (LLC2) session established through a border peer data-link switching plus (DLSw+) network.

Setting the *average-bit-rate* and *maximum burst* values to 0 disables the RSVP bandwidth reservation for the peer connections.

Examples

The following example configures FST for peer-on-demand transport:

```
dlsw peer-on-demand-defaults fst
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw port-list

To map traffic on a local interface (Token Ring or serial) to remote peers, use the **dlsw port-list** command in global configuration mode. To disable the previous map assignment, use the **no** form of this command.

dlsw port-list *list-number type number*

no dlsw port-list *list-number type number*

Syntax Description

list-number	Port list number. The valid range is from 1 to 255.
type	Interface type.
number	Interface number.

Defaults

No port list is configured.

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

Traffic received from a remote peer is forwarded only to the ports specified in the port list. Traffic received from a local interface is forwarded to peers if the input port number appears in the port list applied to the remote peer definition. The definition of a port list is optional.

Examples

The following example configures a data-link switching (DLSw) peer port list for Token Ring interface 1:

```
dlsw port-list 3 token ring 1
```

Related Commands

Command	Description
dlsw bgroup-list	Maps traffic on the local Ethernet bridge group interface to remote peers.
dlsw ring-list	Configures a ring list, mapping traffic on a local interface to remote peers.

dlsw prom-peer-defaults

To configure defaults for promiscuous transport, use the **dlsw prom-peer-defaults** command in global configuration mode. To disable the previous assignment, use the **no** form of this command.

dlsw prom-peer-defaults [**fst**] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *destination-mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**lsap-output-list** *list*] [**rsvp** {**global** | **learn** | [*average-bit-rate maximum burst*]}] [**tcp-queue-max** *size*]

no dlsw prom-peer-defaults [**fst**] [**bytes-netbios-out** *bytes-list-name*] [**cost** *cost*] [**dest-mac** *destination-mac-address*] [**dmac-output-list** ***access-list-number***] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**lsap-output-list** *list*] [**rsvp** {**global** | **learn** | [*average-bit-rate maximum burst*]}] [**tcp-queue-max** *size*]

Syntax Description

fst	(Optional) Use Fast Sequenced Transport (FST) encapsulation for all promiscuous peers established by this router.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for promiscuous peers. The *bytes-list-name* value is the name of the previously defined NetBIOS bytes access list filter.
cost *cost*	(Optional) Specifies the cost to reach promiscuous peers. The valid range is from 1 to 5. The default cost is 3.
dest-mac *destination-mac-address*	(Optional) Specifies the exclusive destination MAC address for promiscuous peers.
dmac-output-list *access-list-number*	(Optional) Specifies the filter output destination MAC addresses.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for promiscuous peers. The *host-list-name* value is the name of the previously defined NetBIOS host access list filter.
keepalive *seconds*	(Optional) Configures the promiscuous keepalive interval. The valid range is from 0 to 1200 seconds. The default is 30 seconds.
lf *size*	(Optional) Largest frame size for this promiscuous peer. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
lsap-output-list *list*	(Optional) Configures Link Service Access Point (LSAP) output filtering for promiscuous peers. Valid numbers are 200 to 299.
rsvp global	(Optional) Sets the Resource Reservation Protocol (RSVP) parameters to the global values.
rsvp learn	(Optional) Configures RSVP parameters (*average-bit-rate* and *maximum burst* rate) to be those of the remote peer to which the promiscuous peer is connecting.

average-bit-rate	(Optional) Configures RSVP parameters for this peer connection, which are different from the global values. Average bit rate (kilobits per second) to reserve up to 75 percent of the total bits on the interface. The valid range is from 0 to 4294967.
maximum-burst	(Optional) Maximum burst size (kilobytes of data in queue). The valid range is from 0 to 4294967.
tcp-queue-max *size*	(Optional) Configures the maximum output TCP queue size for promiscuous peers.

Defaults

The default promiscuous-peer transport is TCP.
The default cost is 3.
The default keepalive value is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.0(3)T	The **rsvp** 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-

A prom peer is a peer not configured as a remote peer on this data-link switching plus (DLSw+) device, but that initiated a peer connection that was accepted because promiscuous peering was enabled.

Setting the *average-bit-rate* and *maximum burst* values to 0 disables the RSVP bandwidth reservation for non configured remote peers.

Examples

The following example configures cost for promiscuous peers:

```
dlsw prom-peer-defaults cost 4
```

Related Commands

Command	Description
show dlsw capabilities	Displays the configuration of a specific peer or all peers.

dlsw redundant-rings

To eliminate caching problems and explorer looping when multiple data-link switching plus (DLSw+) peers are connected to a single Token Ring LAN where the virtual ring numbers configured in those DLSw+ routers are different, use the **dlsw redundant-rings** command in global configuration mode. To disable the previous settings, use the **no** form of this command.

dlsw redundant-rings [*ring***]**

no dlsw redundant-rings [*ring***]**

Syntax Description

ring	(Optional) Virtual ring number. You can configure up to 10 redundant rings, separated by spaces.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Examples

The following example configures router remote-router-1 so that the redundant virtual ring 300 should drop any explorer that is sourced from ring number 300. Similarly, router remote-router-2 knows that 300 is a redundant ring and any explorer sourced from ring 300 should be dropped.

```
remote-router-1# dlsw redundant-rings 300
remote-router-2# dlsw redundant-rings 300
```

dlsw remote-peer frame-relay

To specify the remote peer with which the router will connect, use the **dlsw remote-peer frame-relay** command in global configuration mode. To disable the previous assignments, use the **no** form of this command.

dlsw remote-peer *list-number* **frame-relay interface serial** *number dlci-number* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | **circuit-inactivity** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**] **pass-thru**

no dlsw remote-peer *list-number* **frame-relay interface serial** *number dlci-number* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | ***circuit-inactivity*** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**] **pass-thru**

Syntax Description

list-number	Ring list number. The valid range is from 1 to 255. The default is 0, which means data-link switching plus (DLSw+) forwards explorers over all ports or bridge groups on which DLSw+ is enabled.
interface serial *number*	Serial interface number of the remote peer with which the router is to communicate.
dlci-number	data-link connection identifier (DLCI) number of the remote peer.
backup-peer *ip-address*	(Optional) IP address of the existing TCP or Fast Sequenced Transport (FST) peer for which this peer is the backup peer.
backup-peer frame-relay interface serial *number dlci-number*	(Optional) Serial interface and DLCI number of the existing DirectLogical Link Control, type 2 (LLC2) Frame Relay peer for which this peer is the backup peer.
backup-peer interface *name*	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
backup-peer circuit-inactivity *minutes*	(Optional) Configures the length of time a circuit is inactive before terminating the circuit. May be used with the linger option. The valid range is from 1 to 1440 minutes.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The *bytes-list-name* argument is the name of the previously defined NetBIOS bytes access list filter.
circuit-weight *weight*	(Optional) Configures circuit weight for this remote peer.
cost *cost*	(Optional) Cost to reach this remote peer. The valid range is from 1 to 5. This cost takes precedence over the cost learned as part of the capabilities exchange with the remote peer. The **cost** keyword is relevant only in fault-tolerance mode.

dest-mac *mac-address*	(Optional) Permits the connection to be established only when an explorer frame is destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
dmac-output-list *access-list-number*	(Optional) Permits the connection to be established only when the explorer frame passes the specified access list. The *access-list-number* is the list number specified in the **access-list** command.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is from 0 to 1200 seconds.
lf *size*	(Optional) Largest frame size, in bytes, this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger *minutes*	(Optional) Configures the length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is from 1 to 300 minutes. The default is 5 minutes.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range from 200 to 299.
passive	(Optional) Designates this remote peer as passive.
pass-thru	(Optional) Selects pass-through mode. The default is local acknowledgment mode.

Defaults

No remote peers are specified.
The **linger** default is 5 minutes.
The **pass-thru** default is local acknowledgment mode.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.2	The following keywords and arguments were added: • **cost** *cost* • **dest-mac** *mac-address* • **dmac-output-list** *access-list-number* • **linger** *minutes* • **pass-thru**
12.0(3)T	The **circuit-weight** keyword was added.
12.2	The **backup peer circuit-inactivity** keyword and *minutes* argument were added.

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

Usage Guidelines

When you need to permit access to only a single MAC address, the **dest-mac** option is a shortcut over the **dmac-output-list** option.

When the **pass-thru** keyword is not specified, traffic will be locally acknowledged and reliably transported in Logical Link Control, type 2 (LLC2) across the WAN.

The following keywords and arguments first appeared in Cisco IOS Release 12.2:

The backup-peer circuit-inactivity is only configurable in tandem with the backup-peer command for TCP or LLC2 peers.

Examples

The following example specifies a DLSw+ Lite peer as a backup to a primary direct peer:

```
dlsw remote-peer 0 frame-relay interface serial 1 40 pass-thru
dlsw remote-peer 0 frame-relay interface serial 0 30 backup-peer frame-relay interface
serial 1 40
```

The following example specifies Frame Relay encapsulation connection for remote peer transport:

```
dlsw remote-peer 0 frame-relay interface serial 0 30
```

The following example specifies Remote Peer Backup Peer circuit-inactivity linger before termination:

```
dlsw local-peer peer-id 10.1.1.3
dlsw remote-peer 0 frame-relay 10.1.1.1
dlsw remote-peer 0 frame-relay 10.1.1.2 backup-peer 10.1.1.1 linger 20
circuit-inactivity 3
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw remote-peer fst

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

dlsw remote-peer *list-number* **fst** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**]

no dlsw remote-peer *list-number* **fst** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**]

Syntax Description

list-number	Ring list number. The valid range is from 1 to 255. The default is 0, which means DLSw+ forwards explorers over all ports or bridge groups on which data-link switching plus (DLSw+) is enabled.
ip-address	IP address of the remote peer with which the router is to communicate.
backup-peer *ip-address*	(Optional) IP address of the existing TCP or FST peer for which this peer is the backup peer.
backup-peer frame-relay-interface serial *number dlci-number*	(Optional) Serial interface and data-link connection identifier (DLCI) number of the existing direct or LLC2 Frame Relay peer for which this peer is the backup peer.
backup-peer interface *name*	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The *bytes-list-name* argument is the name of the previously defined NetBIOS bytes access list filter.
circuit-weight *weight*	(Optional) Configures circuit weight for this remote peer.
cost *cost*	(Optional) Cost to reach this remote peer. The valid range is from 1 to 5. This cost takes precedence over the cost learned as part of the capabilities exchange with the remote peer. The **cost** keyword is relevant only in fault-tolerance mode.
dest-mac *mac-address*	(Optional) Permits the connection to be established only when an explorer frame is destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
dmac-output-list *access-list-number*	(Optional) Permits the connection to be established only when the explorer frame passes the specified access list. The *access-list-number* is the list number specified in the **access-list** command.

host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is from 0 to 1200 seconds.
lf *size*	(Optional) Largest frame size this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger *minutes*	(Optional) Configures the length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is from 1 to 300 minutes. The default is 5 minutes.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range from 200 to 299.
passive	(Optional) Designates this remote peer as passive.

Defaults

No FST encapsulation connection is specified.

The **linger** default is 5 minutes.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2	The following keywords and arguments were added: • **dest-mac** *mac-address* • **dmac-output-list** *access-list-number* • **linger** *minutes*
12.0(3)T	The **circuit-weight** 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

When you need to permit access to a single MAC address, the **dest-mac** option is a shortcut over the **dmac-output-list** option.

Examples

The following example specifies an FST peer as backup to a primary TCP peer:

```
dlsw remote-peer 0 tcp 10.2.18.1
dlsw remote-peer 1 fst 10.2.17.8 backup-peer 10.2.18.1
```

The following example specifies an FST encapsulation connection for remote peer transport:

```
dlsw remote-peer 1 fst 10.2.17.8
```

The following example specifies Remote Peer Backup Peer circuit inactivity and lingering before termination:

```
dlsw local-peer peer-id 10.1.1.3
dlsw remote-peer 0 tcp 10.1.1.1
dlsw remote-peer 0 tcp 10.1.1.2 backup-peer 10.1.1.1 linger 20
circuit-inactivity 3
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw remote-peer interface

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

dlsw remote-peer *list-number* **interface serial** *number* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | **circuit-inactivity** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**] [**pass-thru**]

no dlsw remote-peer *list-number* **interface serial** *number* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | ***circuit-inactivity*** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**circuit-weight** *weight*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**host-netbios-out** *host-list-name*] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**passive**] [**pass-thru**]

Syntax Description

list-number	Ring list number. The valid range is from 1 to 255. The default is 0, which means all.
serial *number*	Specifies the remote peer by direct serial interface.
backup-peer *ip-address*	(Optional) IP address of the existing TCP or FST peer for which this peer is the backup peer.
backup-peer frame-relay interface serial *number dlci-number*	(Optional) Serial interface and data-link connection identifier (DLCI) number of the existing direct or Logical Link Control, type 2 (LLC2) Frame Relay peer for which this peer is the backup peer.
backup-peer interface *name*	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
backup-peer circuit-inactivity *minutes*	(Optional) Configures the length of time a circuit is inactive before being terminated. May be used with the linger option. The valid range is from 1 to 1440 minutes.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The *bytes-list-name* argument is the name of the previously defined NetBIOS bytes access list filter.
circuit-weight *weight*	(Optional) Configures circuit weight for this remote peer.
cost *cost*	(Optional) Cost to reach this remote peer. The valid range is from 1 to 5.
dest-mac *mac-address*	(Optional) Permits the connection to be established only when an explorer frame is destined for the specified 48-bit MAC address written as a dotted triple of four-digit hexadecimal numbers.
dmac-output-list *access-list-number*	(Optional) Permits the connection to be established only when the explorer frame passes the specified access list. The *access-list-number* is the list number specified in the **access-list** command.

host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is from 0 to 1200 seconds.
lf *size*	(Optional) Largest frame size, in bytes, this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger *minutes*	(Optional) Configures the length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is from 1 to 300 minutes. The default is 5 minutes.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range from 200 to 299.
passive	(Optional) Designates this remote peer as passive.
pass-thru	(Optional) Selects pass-through mode. The default is local acknowledgment mode.

Defaults

No point-to-point direct encapsulation connection is specified.
The **linger** default is 5 minutes.
The **pass-thru** default is local acknowledgment mode.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.2	The following keywords and arguments were added: • **dest-mac** *mac-address* • **dmac-output-list** *access-list-number* • **linger** *minutes*
12.0(3)T	The **circuit-weight** keyword was added.
12.2	The **backup peer circuit-inactivity** keyword *minutes* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **cost** keyword specified in a remote peer statement takes precedence over the cost learned as part of the capabilities exchange with the remote peer. The **cost** keyword is relevant only in fault-tolerance mode.

When you need to permit access to a single MAC address only, the **dest-mac** option is a shortcut over the **dmac-output-list** option.

Examples

The following example specifies a point-to-point direct peer backup to a primary direct peer:

```
dlsw remote-peer 0 interface serial 1 pass-thru
dlsw remote-peer 1 interface serial 2 backup-peer interface serial 1 pass-thru
```

The following example specifies a point-to-point direct encapsulation connection for remote peer transport:

```
dlsw remote-peer 1 interface serial 2 pass-thru
```

The following example specifies Remote Peer Backup Peer circuit inactivity and lingering before termination:

```
dlsw local-peer peer-id 10.1.1.3
dlsw remote-peer 0 tcp 10.1.1.1
dlsw remote-peer 0 tcp 10.1.1.2 backup-peer 10.1.1.1 linger 20
circuit-inactivity 3
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw remote-peer tcp

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

dlsw remote-peer *list-number* **tcp** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | **circuit-inactivity** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**cluster** *cluster-id*] [**circuit-weight** *value*] [**cost** *cost*] [**dest-mac** *mac-address*] **dmac-output-list** *access-list-number*] [**dynamic**] [**host-netbios-out** *host-list-name*] [**inactivity** *minutes*] [**dynamic**] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] [**lsap-output-list** *list*] [**no-llc** *minutes*] [**passive**] [**priority**] [**rif-passthru** *virtual-ring-number*] [**rsvp** {**global** | *average-bit-rate maximum burst*}] [**tcp-queue-max** *size*] [**timeout** *seconds*]

no dlsw remote-peer *list-number* **tcp** *ip-address* [**backup-peer** [*ip-address* | **frame-relay interface serial** *number dlci-number* | **interface** *name* | **circuit-inactivity** *minutes*]] [**bytes-netbios-out** *bytes-list-name*] [**cluster** *cluster-id*] [**circuit-weight** *value*] [**cost** *cost*] [**dest-mac** *mac-address*] [**dmac-output-list** *access-list-number*] [**dynamic**] [**host-netbios-out** *host-list-name*] [**inactivity** *minutes*] [**dynamic**] [**keepalive** *seconds*] [**lf** *size*] [**linger** *minutes*] **lsap-output-list** *list*] [**no-llc** *minutes*] [**passive**] [**priority**] [**rif-passthru** *virtual-ring-number*] [**rsvp** {**global** | *average-bit-rate maximum burst*}] [**tcp-queue-max** *size*] [**timeout** *seconds*]

Syntax Description

list-number	Remote peer ring group list number. This ring group list number default is 0. Otherwise, this value must match the number you specify with the **dlsw ring-list**, **dlsw port-list**, or **dlsw bgroup-list** command.
ip-address	IP address of the remote peer with which the router is to communicate.
backup-peer *ip-address*	(Optional) IP address of the existing TCP or FST peer for which this peer is the backup peer.
backup-peer frame-relay interface serial *number dlci-number*	(Optional) Serial interface and data-link connection identifier (DLCI) number of the existing direct or Logical Link Control, type 2 (LLC2) Frame Relay peer for which this peer is the backup peer.
backup-peer interface *name*	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
backup-peer circuit-inactivity *minutes*	(Optional) Configures the length of time a circuit is inactive before terminating the circuit. The valid range is from 1 to 1440.
bytes-netbios-out *bytes-list-name*	(Optional) Configures NetBIOS bytes output filtering for this peer. The *bytes-list-name* argument is the name of the previously defined NetBIOS bytes access list filter.
cluster *cluster-id*	(Optional) Used to indicate to a border peer that a particular remote peer should be treated as part of a specific peer cluster. The valid range is from 1 to 255.
circuit-weight *value*	(Optional) Configures the target state that data-link switching plus (DLSw+) tries to maintain. The valid range is from 1 to 100.
cost *cost*	(Optional) Cost to reach this remote peer. The valid range is from 1 to 5.

dest-mac *mac-address*	(Optional) Specifies the exclusive 48-bit destination MAC address, written as a dotted triple of four-digit hexadecimal numbers, for peer-on-demand peers. If the **dynamic** keyword is also specified, the TCP connection is established only when there is an explorer frame destined for the specified MAC address.
dmac-output-list *access-list-number*	(Optional) Specifies the filter output destination MAC addresses. The *access-list-number* is the list number specified in an **access-list** command. If the **dynamic** keyword is also specified, the TCP connection is established only when the explorer frame passes the specified access list.
dynamic	(Optional) Establishes the TCP connection only when there is DLSw+ data to send.
host-netbios-out *host-list-name*	(Optional) Configures NetBIOS host output filtering for this peer. The *host-list-name* is the name of the previously defined NetBIOS host access list filter.
inactivity *minutes*	(Optional) Configures the length of time a connection is inactive before closing the dynamic remote peer connection. The valid range is from 1 to 300 minutes. The default is 5 minutes.
keepalive *seconds*	(Optional) Sets the keepalive interval for this remote peer. The range is from 0 to 1200 seconds.
lf *size*	(Optional) Largest frame size, in bytes, this local peer uses on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger *minutes*	(Optional) Configures the length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is from 0 to 1440 minutes.
lsap-output-list *list*	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range from 200 to 299.
no-llc *minutes*	(Optional) Configures the length of time a remote peer remains connected after all Logical Link Control, type 2 (LLC2) connections are gone. The valid range is from 1 to 300 minutes. The default is 5 minutes.
passive	(Optional) Designates this remote peer as passive.
priority	(Optional) Enables prioritization features for this remote peer. Valid TCP port numbers are the following: • High—2065 • Medium—1981 • Normal—1982 • Low—1983

rif-passthru *virtual-ring-number*	(Optional) Configures the remote peer as RIF-Passthru. The *virtual-ring-number* value is the same number as the *ring number* value assigned in the **source-bridge ring-group** commands of the DLSw+ Passthru peers.
rsvp global	(Optional) Configures the RSVP parameters for this specific peer back to the global values.
rsvp *average-bit-rate*	(Optional) Configures Resource Reservation Protocol (RSVP) parameters for this peer, which are different from the global values. Average bit rate (kilobits per second) reserves up to 75 percent of the total bits on the interface. range is from 0 to 4294967.
maximum burst	(Optional) Maximum burst size (kilobytes of data in queue). range is from 0 to 4294967.
tcp-queue-max *size*	(Optional) Maximum output TCP queue size for this remote peer. The valid maximum TCP queue size is a number in the range from 10 to 2000.
timeout *seconds*	(Optional) Resend time limit for TCP. The valid range is from 5 to 1200 seconds. The default is 90 seconds.

Defaults

No peer IP address is identified.

The **dynamic** option is not on by default. If the dynamic option is added without either the **inactivity** or **no-llc** argument specified, the default is to terminate the TCP connection to the remote peer after 5 minutes of no active LLC2 connection.

The **inactivity** default is 5 minutes.

The **no-llc** default is 5 minutes.

The **timeout** default is 90 seconds.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
11.1	The following keywords and arguments were added: • **dynamic** • **inactivity** *minutes* • **linger** *minutes* • **no-llc** *minutes* • **timeout** *seconds*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
11.2	The following keywords and arguments were added: • **dest-mac** *mac-address* • **dmac-output-list** *access-list-number* • **linger** *minutes*
12.0(3)T	The following keywords and arguments were added: • **circuit-weight** *value* • **rsvp** *maximum burst*
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

Systems Network Architecture (SNA) dial-on-demand routing (DDR) technology allows switched links to be closed during idle periods. To enable this feature, set the **keepalive** keyword *seconds* argument to 0 and configure the **timeout** keyword *seconds* argument. When the **dynamic** keyword is configured, the **keepalive** keyword *seconds* argument is automatically set to 0.

To enhance DDR cost savings, you can configure the TCP connection to a remote peer to be dynamically established (that is, established only when there is DLSw data to send). You can further configure the TCP connection to terminate after a specified period of idle time on the peer or after a specified period of no active LLC sessions on the peer.

You cannot use both **no-llc** and **inactivity** in a command specifying a dynamic peer.

When you need to permit access to a single MAC address, the **dest-mac** keyword *mac-address* argument is a shortcut over the **dmac-output-list** keyword *access-list-number* argument.

Use the **linger** keyword *minutes* argument to specify that a backup peer will remain connected for a specified period of time after the primary connection is reestablished. Setting the **linger** keyword *minutes* argument to 0 causes sessions connected to the backup peer to drop immediately when the primary peer recovers. If the **linger** keyword is omitted, all sessions connected to the backup peer remain active until they terminate on their own.

When the **priority** keyword on the **dlsw remote-peer** command is configured, DLSw+ automatically activates four TCP ports to that remote peer (ports 2065, 1981, 1982 and 1983) and assigns traffic to specific ports. Furthermore, if Advanced Peer-to-Peer Networking (APPN) is running with DLSw+ and you specify the **priority** keyword option on the **dlsw remote-peer** command, then the SNA type of service (ToS) will map APPN class of service (COS) to TCP ToS and will preserve the APPN COS characteristics throughout the network.

The **rif passthru** keyword works only on Token Ring LANs via source-route bridging (SRB). Other LAN types, such as Synchronous Data Link Control (SDLC) and Qualified Logical Link Control (QLLC), are not supported. The RIF Passthru feature is supported with TCP encapsulation and it disables local acknowledgment.

The following features are not supported with the DLSw+ RIF Passthru feature:

- Border peers
- Peer-on-demand peers
- Dynamic peers
- Backup peers

The **cluster** keyword is available only on border peers. This option enables the DLSw+ Peer Clusters feature without forcing every DLSw+ router in the network to upgrade its software.

Setting the *average-bit-rate* or *maximum burst* value to 0 turns off RSVP for this peer.

Examples

The following example specifies a TCP encapsulation connection for remote peer transport:

```
dlsw remote-peer 0 tcp 10.2.17.8
```

The following example specifies a TCP peer as backup to a primary Fast Sequenced Transport (FST) peer:

```
dlsw remote-peer 0 fst 10.2.18.9
dlsw remote-peer 0 tcp 10.2.17.8 backup-peer 10.2.18.9
```

Related Commands

Command	Description
show dlsw peers	Displays DLSw peer information.

dlsw ring-list

To configure a ring list, mapping traffic on a local interface to remote peers, use the **dlsw ring-list** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dlsw ring-list *list-number* **rings** *ring-number*

no dlsw ring-list *list-number* **rings** *ring-number*

Syntax Description

list-number	Ring list number. The valid range is from 1 to 255.
rings	Specify one or more physical or virtual rings.
ring-number	Physical or virtual ring numbers. Multiple values are allowed. The valid range is from 1 to 4095.

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

Traffic received from a remote peer is forwarded only to the rings specified in the ring list. Traffic received from a local interface is forwarded to peers if the input ring number appears in the ring list applied to the remote peer definition. The definition of a ring list is optional.

Examples

The following example configures a data-link switching (DLSw) ring list, assigning rings 1, 2, and 3 to ring list 3:

```
dlsw ring-list 3 rings 1 2 3
```

Related Commands

Command	Description
dlsw port-list	Maps traffic on a local interface (Token Ring or serial) to remote peers.
dlsw remote-peer frame-relay	Specifies the remote peer with which the router will connect.
show dlsw capabilities	Displays the configuration of a specific peer or all peers.

dlsw rsvp

To enable the data-link switching plus (DLSw+) RSVP Bandwidth Reservation feature on the local peer, use the **dlsw rsvp** command in global configuration mode. To disable the DLSw+ RSVP Bandwidth Reservation feature for all peers in the router, use the **no** form of this command.

dlsw rsvp {**default** | *average-bit-rate maximum-burst*]}

no dlsw rsvp {**default** | *average-bit-rate maximum-burst*}

Syntax Description

default	Sets the average bit rate to 10 kbps and the maximum burst rate to 28 kbps.
average-bit-rate	Average bit rate (kilo*bits* per second) to reserve up to 75 percent of the total bits on the interface. The valid range is from 1 to 4294967 kbps.
maximum-burst	Maximum burst size (kilo*bytes* of data in queue). The valid range is from 1 to 4294967 kbps.

Defaults

The default values for the *average-bit-rate* and *maximum-burst* are 10 kbps and 28 kbps, respectively.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The DLSw+ RSVP Bandwidth Reservation feature does not require that all peers in a network have Resource Reservation Protocol (RSVP) configured. However, the feature does require that the end peer devices are configured with RSVP and that all devices in the middle are IP RSVP-capable.

The **default** keyword assumes that the DLSw+ peer is connected via a 56-kbps link. If this is not the case, then the default values will likely not produce optimal results. Even if the line speed is 56 kbps, the default values (10 kbps *average-bit-rate* and 28 kBps *maximum-burst*) may not be optimal in a particular network environment and should be changed accordingly.

Setting the *average-bit-rate* or *maximum-burst* value to 0 turns off RSVP for this peer.

Examples

The following example configures the DLSw+ RSVP Bandwidth Reservation feature with an *average bit rate* of 10 kbps and a *maximum-burst* value of 28 kbps:

```
dlsw rsvp default
```

Related Commands

Command	Description
dlsw peer-on-demand-defaults	Configures defaults for peer-on-demand transport.
dlsw prom-peer-defaults	Configures defaults for promiscuous transport
dlsw remote-peer tcp	Identifies the IP address of a peer with which to exchange traffic using TCP.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.
show ip rsvp request	Displays RSVP-related request information being requested upstream.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.

dlsw timer

To tune an existing configuration parameter, use the **dlsw timer** command in global configuration mode. To restore the default parameters, use the **no** form of this command.

dlsw timer {**icannotreach-block-time** | **netbios-cache-timeout** | **netbios-explorer-timeout** | **netbios-group-cache** | **netbios-retry-interval** | **netbios-verify-interval** | **sna-cache-timeout** | **explorer-delay-time** | **sna-explorer-timeout** | **explorer-wait-time** | **sna-group-cache** | **sna-retry-interval** | **sna-verify-interval**} *time*

no dlsw timer {**icannotreach-block-time** | **netbios-cache-timeout** | **netbios-explorer-timeout** | **netbios-group-cache** | **netbios-retry-interval** | **netbios-verify-interval** | **sna-cache-timeout** | **explorer-delay-time** | **sna-explorer-timeout** | **explorer-wait-time** | **sna-group-cache** | **sna-retry-interval** | **sna-verify-interval**} *time*

Syntax Description

icannotreach-block-time	Cache life of unreachable resource; during this time searches for the resource are blocked. The valid range is from 1 to 86400 seconds. The default is 0 (disabled).
netbios-cache-timeout	Cache life of NetBIOS name location for the local and remote reachability caches. The valid range is from 1 to 86400 seconds. The default is 960 seconds (16 minutes).
netbios-explorer-timeout	Length of time that the Cisco IOS software waits for an explorer response before marking a resource unreachable (on both a LAN and a WAN). The valid range is from 1 to 86400 seconds. The default is 6 seconds.
netbios-group-cache	Cache life of NetBIOS entries in the group cache. The valid range is from 1 to 86000 seconds. The default is 240 seconds (4 minutes).
netbios-retry-interval	NetBIOS explorer retry interval (on a LAN only). The valid range is from 1 to 86400 seconds. The default is 1 second.
netbios-verify-interval	Number of seconds between a cache entry's creation and its marking as stale. If a search request comes in for a stale cache entry, a directed verify query is sent to ensure that the cache still exists. The valid range is from 1 to 86400 seconds. The default is 240 seconds (4 minutes).
sna-cache-timeout	Length of time that anSystems Network Architecture (SNA) MAC or service access point (SAP) location cache entry exists before it is discarded (for local and remote caches). The valid range is from 1 to 86400 seconds. The default is 960 seconds (16 minutes).
explorer-delay-time	Time to wait before sending or accepting explorers. The valid range is from 1 to 5 minutes. The default is 0.
sna-explorer-timeout	Length of time that the Cisco IOS software waits for an explorer response before marking a resource unreachable (on a LAN and WAN). The valid range is from 1 to 86400 seconds. The default is 180 seconds (3 minutes).
explorer-wait-time	Time to wait for all stations to respond to explorers. The valid range is from 1 to 86400 seconds. The default is 0.
sna-group-cache	Cache life of SNA entries in the group cache. The valid range is from 1 to 86000 seconds. The default is 240 seconds (4 minutes).

sna-retry-interval	Interval between SNA explorer retries (on a LAN). The valid range is from 1 to 86400 seconds. The default is 30 seconds.
sna-verify-interval	Number of seconds between a cache entry's creation and its marking as stale. If a search request comes in for a stale cache entry, a directed verify query is sent to ensure that the cache still exists. The valid range is from 1 to 86400 seconds. The default is 240 seconds (4 minutes).
time	Length of time for selected timer, in seconds.

Defaults

The **icannotreach-block-time** default is 0 (disabled).

The **netbios-cache-timeout** default is 960 seconds (16 minutes).

The **netbios-explorer-timeout** default is 6 seconds.

The **netbios-group-cache** default is 240 seconds (4 minutes).

The **netbios-retry-interval** default is 1 second.

The **netbios-verify-interval** default is 240 seconds (4 minutes).

The **sna-cache-timeout** default is 960 seconds (16 minutes).

The **explorer-delay-time** default is 0.

The **sna-explorer-timeout** default is 180 seconds (3 minutes).

The **explorer-wait-time** default is 0.

The **sna-group-cache** default is 240 seconds (4 minutes).

The **sna-retry-interval** default is 30 seconds.

The **sna-verify-interval** default is 240 seconds (4 minutes).

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 **netbios-group-cache** and **sna-group-cache** options were added to this command for the border peer caching feature.

Examples

The following configuration defines the length of time that an entry will stay in the group cache as 120 seconds (2 minutes):

```
dlsw timers sna-group-cache 120
```

The following example configures the length of time that an SNA MAC location cache entry exists before it is discarded:

```
dlsw timer sna-cache-timeout 3
```

dlsw timer connect-timeout

To modify the maximum allowed interval between first exchange identification (XID) and set asynchronous balanced mode extended unnumbered acknowledgment (SABME/UA) frames for circuits, use the **dlsw timer connect-timeout** command in global configuration mode. To disable the modification of XID and SABME/UA frames for circuits, use the **no** form of this command.

dlsw timer connect-timeout *time*

no dlsw timer connect-timeout *time*

Syntax Description

time	The time interval between XID and SABME/UA frames for circuits, in seconds. The complete XID negotiation has to be finished within this time interval. The range is 1 to 86400. The default is 60 seconds.

Command Default

Modification of XID and SABME/UA frames for circuits is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3T	This command was introduced.

Usage Guidelines

Use the **dlsw timer connect-timeout** command to override the value of the timer value default.

Examples

The following example sets the interval to 30 seconds for the modification of XID and SABME/UA frames for circuits:

```
Router(config)# dlsw timer connect-timeout 30
```

Related Commands

Command	Description
dlsw timer	Tunes an existing configuration parameter.
dlsw timer local-connect-timeout	Modifies the maximum allowed interval between local-switched circuits.

dlsw timer local-connect-timeout

To modify the maximum allowed interval between local-switched circuits, use the **dlsw timer local-connect-timeout** command in global configuration mode. To disable the modification of time intervals between local-switched circuits, use the **no** form of this command.

dlsw timer local-connect-timeout *time*

no dlsw timer local-connect-timeout *time*

Syntax Description

time	The time interval between local-switched circuits, in seconds. The range is 1 to 86400. The default is 30 seconds.

Command Default

Modification of the maximum allowed interval between local-switched circuits is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3T	This command was introduced.

Usage Guidelines

Use the **dlsw timer local-connect-timeout** command for the following reasons:

- This command overrides the value of the timer value default.
- This command enables you to link between local-switched circuits, such as Synchronous Data Link Control (SDLC) protocol to Logical Link Control, type 2 (LLC2) protocol and Qualified Logical Link Control (QLLC) protocol LLC2 protocol.

Examples

The following example sets the interval between local-switched circuits to 60 seconds:

```
Router(config)# dlsw timer local-connect-timeout 60
```

Related Commands

Command	Description
dlsw timer	Tunes an existing configuration parameter.
dlsw timer connect-timeout	Modifies the maximum allowed interval between XID and SABME/UA frames for circuits.

dlsw tos disable

To disable any type of service (ToS) bits in data-link switching plus (DLSw+)-generated packets, use the **dlsw tos disable** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw tos disable

no dlsw tos disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0	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 disables the ToS bits in DLSw+-generated packets:

```
dlsw tos disable
```

dlsw tos map

To associate a type of service (ToS) value for priority peers, use the **dlsw tos map** command in global configuration mode. To return to the default, use the **no** form of this command.

dlsw tos map [**high** *value* [**medium** *value* | **normal** *value* | **low** *value*]]

no dlsw tos map [**high** *value* [**medium** *value* | **normal** *value* | **low** *value*]]

Syntax Description

high *value*	(Optional) Overrides the default values set for the port labeled "high." The value is the ToS bit value. Valid range is from 0 to 7.
medium *value*	(Optional) Overrides the default values set for the port labeled "medium." The value is the ToS bit value. Valid range is from 0 to 7.
normal *value*	(Optional) Overrides the default values set for the port labeled "normal." The value is the ToS bit value. Valid range is from 0 to 7.
low *value*	(Optional) Overrides the default values set for the port labeled "low." The value is the ToS bit value. Valid range is from 0 to 7.

Defaults

The default settings, with priority peers configured, are defined in Table 11.

Command Modes

Global configuration

Command History

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

Usage Guidelines

By default, data-link switching plus (DLSw+) peer traffic is set to Critical-ECP. When the **priority** keyword is specified in the **dlsw remote peer tcp** command, DLSw+ automatically activates four TCP ports to that remote peer (ports 2065, 1981, 1982 and 1983) and associates a priority level. This command enables the user to customize the prioritization of DLSw+ traffic within the network. If priority peers are not configured, high is the only option. See Table 11 for corresponding priority levels and options.

Table 11 Priority Levels and Options

ToS Bit Value	DLSw+ Translation Value	ToS Bit Value Meaning	TCP Port Numbers
0[1]	Routine	—	—
1[1]	Priority	—	—
2	Immediate	Low	1983
3	Flash	Normal	1982
4	Flash Override	Medium	1981
5	Critical ECP	High	2065
6[2]	Internetwork Control	—	—
7[2]	Network Control	—	—

1. Using ToS bit values 0 and 1 does not cause negative impact to the network, but these values do not prioritize the traffic.
2. ToS bit values 6 and 7 are not recommended because of potential interference with critical network infrastructure flows.

Examples

The following example changes the default setting on IP packets generated by DLSw+ from high to low:

```
dlsw tos map low 2
```

The following is an example policy routing configuration that shows how to modify the default setting of TCP port 2065. The configuration changes the default setting on IP packets from network control priority to routine priority.

```
ip local policy route-map test
access-list 101 permit tcp any eq 2065 any
access-list 101 permit tcp any any eq 2065
route-map test permit 20
 match ip address 101
set ip precedence routine
```

dlsw transparent map

To enable MAC address mapping in a switch-based environment, use the **dlsw transparent map** command in interface configuration mode. To disable MAC address mapping, use the **no** form of this command.

dlsw transparent map local mac *mac-address* **remote mac** *mac-address* [**neighbor** *mac-address*]

no dlsw transparent map local mac *mac-address* **remote mac** *mac-address* [**neighbor** *mac-address*]

Syntax Description

local mac *mac-address*	MAC address that is created and given to the remote device. This MAC address is mapped to the actual MAC address that is specified in the **remote mac** *mac-address* option.
remote mac *mac-address*	MAC address of the remote device.
neighbor *mac-address*	(Optional) MAC address of the data-link switching plus (DLSw+) device that takes over mapping if the primary DLSw+ device becomes unavailable.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Only the routers that are connected to the switch are configured for address mapping.

Examples

The following example maps MAC address 4000.1000.1234 to the actual device with the MAC address of 4000.3754.1000 and designates the DLSw+ device with MAC address 0000.0c12.0001 as backup:

```
dlsw transparent map local-mac 4000.1000.1234 remote mac 4000.3754.1000 neighbor
0000.0c12.0001
```

Related Commands

Command	Description
dlsw transparent switch-support	Enables the special support that is required for the interfaces connected to an Ethernet switch with the **dlsw transparent redundancy-enable** command configured.

dlsw transparent redundancy-enable

To configure transparent redundancy, use the **dlsw transparent redundancy-enable** command in interface configuration mode. To disable transparent redundancy, use the **no** form of this command.

dlsw transparent redundancy-enable *multicast-mac-address* [**master-priority** *value*]

no dlsw transparent redundancy-enable *multicast-mac-address* [**master-priority** *value*]

Syntax Description

multicast-mac-address	MAC address to which all data-link switching plus (DLSw+) devices on a transparent bridged domain advertise their presence by sending the master present frame.
master-priority *value*	(Optional) Configures the router as a master device. The valid range is from 0 to 254. The lower the value, higher the priority. The default value is 100.

Defaults

No default behavior or value

The **master-priority** default is 100.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The same *multicast-mac-address* value must be configured on all DLSw+ devices within the same transparent bridged domain. All the DLSw+ devices advertise their presence via frames to this *multicast-mac-address* value.

All routers in the transparent bridged domain compete and elect one master router. The master router is elected based on its **master-priority** value. In the case of equal master priority setting, the router with the lowest MAC address is the elected master router.

Examples

The following example configures Ethernet redundancy with a **master-priority** value of 100:

```
dlsw transparent redundancy-enable 9999.9999.9999 master-priority 100
```

Related Commands

Command	Description
show dlsw transparent cache	Displays the master circuit cache for each transparent bridged domain.
show dlsw transparent neighbor	Displays DLSw neighbors in a transparent bridged domain.

dlsw transparent switch-support

To enable the special support that is required for the interfaces connected to an Ethernet switch with the **dlsw transparent redundancy-enable** command configured, use the **dlsw transparent switch-support** command in global configuration mode. To disable data-link switching (DLSw) transparent switch support, use the **no** form of this command.

dlsw transparent switch-support

no dlsw transparent switch-support

Syntax Description

This command has no arguments or keywords.

Defaults

Switch support is off.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **dlsw transparent switch-support** command must be configured before the **dlsw transparent map** command.

Examples

The following example configures Ethernet switch support:

```
dlsw transparent switch-support
```

Related Commands

Command	Description
dlsw transparent map	Enables MAC address mapping in a switch-based environment.

dlsw transparent timers

To configure the timeout value the master router waits for all requests for a circuit before giving the permission for a router for a circuit, use the **dlsw transparent timers** command in interface configuration mode. To disable the timeout value, use the **no** form of this command.

dlsw transparent timers [**netbios** *value* | **sna** *value*]

no dlsw transparent timers [**netbios** *value* | **sna** *value*]

Syntax Description

netbios *value*	(Optional) Timeout value for the NetBIOS session. The valid range is from 100 to 900 milliseconds (ms). The default value is 400 ms.
sna *value*	(Optional) Timeout value for the Systems Network Architecture (SNA) session. The valid range is from 100 to 5000 ms. The default value is 1000 ms (1 second).

Defaults

The default NetBIOS value is 400 ms.
The default SNA value is 1000 ms (1 second).

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **dlsw transparent redundancy-enable** command must be configured before the **dlsw transparent timers** command.

Examples

The following example configures the master router to wait 500 ms for a NetBIOS session before giving or denying permission to a router to create a circuit:

```
dlsw transparent timers netbios 500
```

Related Commands

Command	Description
dlsw transparent redundancy-enable	Configures transparent redundancy.

dlsw udp-disable

To disable the User Datagram Protocol (UDP) unicast feature, use the **dlsw udp-disable** command in global configuration mode. To return to the default UDP unicast feature, use the **no** form of this command.

dlsw udp-disable

no dlsw udp-disable

Syntax Description

This command has no arguments or keywords.

Defaults

The UDP unicast feature is enabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

If the **dlsw udp-disable** command is configured, then a data-link switching plus data-link switching plus (DLSw+) node will not send packets via UDP unicast and will not advertise UDP Unicast support in its capabilities exchange message.

Refer to the "Bridging and IBM Networking Overview" chapter of the *Bridging and IBM Networking Configuration Guide* for more information on the UDP Unicast feature.

Examples

The following example disables the UDP unicast feature:

```
dlsw udp-disable
```

dlur

To enable the Systems Network Architecture (SNA) session switch function on the Cisco Mainframe Channel Connection (CMCC) adapter and enter dependent logical unit requester (DLUR) configuration mode, use the **dlur** command in TN3270 server configuration mode. To disable the SNA session switch function and discard all parameter values associated with the SNA session switch, use the **no** form of this command.

dlur [*fq-cpname fq-dlusname*]

no dlur

Syntax Description

fq-cpname	(Optional) Fully qualified control point (CP) name used by the SNA session switch and the logical unit (LU) name for the DLUR function. This name must be unique among Advanced Peer-to-Peer Networking (APPN) nodes in the network including other values for the *fq-cpname* argument specified on all other TN3270 servers running under the Cisco IOS software.
fq-dlusname	(Optional) Fully qualified name of the primary choice for the dependent LU server (DLUS). This is the name of an LU, usually a CP, in an APPN host. The value for the *fq-dlusname* argument can be repeated and shared across servers.

Defaults

No DLUR function is enabled.

Command Modes

TN3270 server configuration

Command History

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

Usage Guidelines

This command is valid only on the virtual channel interface. If the SNA session switch function is already enabled, the **dlur** command with no arguments puts you in DLUR configuration mode. The session switch function implements an End Node DLUR.

Several parameters in the DLUR configuration mode consist of fully qualified names, as defined by the APPN architecture. Fully qualified names consist of two case-insensitive alphanumeric strings, separated by a period. However, for compatibility with existing APPN products, including virtual telecommunications access method (VTAM), the characters “#” (pound), “@” (at), and “$” (dollar) are allowed in the fully qualified name strings. Each string is from one to 8 characters long; for example, RA12.NODM1PP. The portion of the name before the period is the network entity title (NET) ID and is shared between entities in the same logical network.

The **no dlur** command hierarchically deletes all resources defined beneath it.

Examples

The following example performs two functions: It enters DLUR configuration mode and it enables the DLUR function and defines the LU name for the DLUR as SYD.TN3020 and the primary choice for DLUS as SYD.VMG. Note that the NET ID portion of both names is the same:

```
dlur SYD.TN3020 SYD.VMG
```

Related Commands

Command	Description
lsap	Creates a SAP in the SNA session switch and enters DLUR SAP configuration mode.
preferred-nnserver	Specifies a preferred NN as server.
pu (DLUR)	Creates a PU entity that has no direct link to a host and enters DLUR PU configuration mode.

dlus-backup

To specify a backup Dependent Logical Unit Server (DLUS) for the Dependent Logical Unit Requestor (DLUR) function, use the **dlus-backup** command in DLUR configuration mode. To remove a backup DLUS name, use the **no** form of this command.

dlus-backup *dlusname*

no dlus-backup

Syntax Description

dlusname	Fully qualified name of the backup DLUS for the DLUR.

Defaults

No backup DLUS is specified.

Command Modes

DLUR 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

This command is valid only on the virtual channel interface. Only one backup DLUS can be specified per Cisco Mainframe Channel Connection (CMCC) adapter. If the backup DLUS specified in the **dlus-backup** command is in use when a **no dlus-backup** command is issued, the connection is not torn down.

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

Examples

The following example specifies SYD.VMX as the backup DLUS:

```
dlus-backup SYD.VMX
```

Related Commands

Command	Description
client pool	Nails clients to pools.

domain-id

To specify a domain name suffix that the TN3270 server appends to a configured machine name to form a fully qualified name when configuring inverse Domain Name System (DNS) nailing, use the **domain-id** command in TN3270 server configuration mode. To disable this specification, use the **no** form of this command.

domain-id *DNS-domain-identifier DNS-domain*

no domain-id *DNS-domain-identifier DNS-domain*

Syntax Description

DNS-domain-identifier	A numeric identifier that specifies the domain name. The valid value range is from 1 to 255. Each domain ID statement can have only one *DNS-domain-identifier* value. This identifier is also used in the **client pool** command.
DNS-domain	An alphanumeric string that specifies a domain name suffix, including all dots (.) but not delimited by dots. The string can contain no more than 80 characters. All dots must be included when the string is appended to a configured DNS name. If the DNS domain starts with a dot, then the dot must be included if it is not already at the end of the DNS name.

Defaults

No default behavior or values

Command Modes

TN3270 server configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The user can configure up to 255 domain names, one per statement. This command must be configured before you configure the **client pool** command with either the **domain-id** keyword or the **name** keyword and the optional *DNS-domain-identifier* argument.

Examples

In the following example, the **domain-id** command specifies 23 as the *DNS domain identifier* for the .cisco.com domain name. All clients nailed to the pool GENERAL will use .cisco.com as the domain name suffix. For example, the client name ally-isdn1 will become ally-isdn1.cisco.com.

```
tn3270-server
 domain-id 23 .cisco.com
  pool GENERAL  cluster layout 4s1p
```

```
 listen-point 172.18.5.168
  pu T240CA   91922363 token-adapter 31 12 rmac 4000.4000.0001
   allocate lu 1 pool GENERAL  clusters 1
client name ally-isdn1 23 pool GENERAL
```

dspu activation-window

To define the number of activation request units (RUs) and response messages (such as activate logical unit (ACTLU)s or Dynamic Definition of Dependent LU (DDDLU) Network Management Vector Transport (NMVT)s that can be sent without waiting for responses from the remote physical unit (PU), use the **dspu activation-window** command in global configuration mode. To restore the default window size, use the **no** form of this command.

dspu activation-window *window-size*

no dspu activation-window

Syntax Description

window-size	Number of outstanding unacknowledged activation RUs. The default is five.

Defaults

The default window size is five outstanding unacknowledged activation RUs.

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

You do not typically need to define the number of activation RUs, but doing so can enhance activation performance in some situations. Increasing the downstream physical unit (DSPU) activation window allows more logical unit (LU)s to become active in a shorter amount of time (assuming the required buffers for activation RUs are available). Conversely, decreasing the DSPU activation window limits the amount of buffers the DSPU can use during PU or LU activation. This command provides pacing to avoid depleting the buffer pool during PU activation.

Examples

In the following example, the DSPU activation window is configured to 10. The DSPU can send up to 10 activation RUs without a response from the remote PU. However, the DSPU cannot send any additional activation RUs until a response is received. The DSPU can only have 10 activation RUs awaiting response at any given time.

```
dspu activation-window 10
```

dspu default-pu

To enable the default PU feature to be used when a downstream physical unit (PU) attempts to connect, but does not match any of the explicit PU definitions, use the **dspu default-pu** command in global configuration mode. To disable the default PU feature, use the **no** form of this command.

dspu default-pu [**window** *window-size*] [**maxiframe** *max-iframe*]

no dspu default-pu [**window** *window-size*] [**maxiframe** *max-iframe*]

Syntax Description

window *window-size*	(Optional) Send and receive window sizes used across the link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum size (in bytes) of an I-frame that can be sent or received across the link. The range is from 64 bytes to 18432 bytes. The default is 1472.

Defaults

The default window size is 7.

The default maximum I-frame size is 1472.

Command Modes

Global configuration

Command History

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

Usage Guidelines

If the downstream physical unit (DSPU) default PU is not defined, a connection attempt by a downstream PU that does not match any explicit PU definition is rejected.

The **dspu default-pu** command must be followed by at least one **dspu lu** command to define which pool the default LUs will be assigned from. Default LUs cannot be defined as dedicated LUs from a host.

The maximum I-frame size includes the Systems Network Architecture (SNA) transmission header (TH), request header (RH), and request unit (RU), but does not include the Data-link control (DLC) header. The DSPU feature segments frames being sent to fit within this frame size. If an exchange identification (XID) is received from a remote PU, which indicates that it supports a different maximum I-frame size, then the lower of the two values is used.

Examples

In the following example, the default PU feature is enabled with a window size of five and a maximum I-frame size of 128. Each default PU can have up to three LUs assigned from the hostpool pool of LUs.

```
dspu pool hostpool host ibm3745 lu 2 254
```

```
dspu default-pu window 5 maxiframe 128
dspu lu 2 4 pool hostpool
```

Related Commands

Command	Description
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.
dspu pool	Defines a range of host LUs in an LU pool.

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

To enable a local service access point (SAP) on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts, use the **dspu enable-host** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

dspu enable-host [**lsap** *local-sap*]

no dspu enable-host [**lsap** *local-sap*]

Syntax Description

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

Defaults

The default local SAP address is 12.

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.

Examples

In the following example, the local SAP address 10 on Token Ring interface 0 is enabled for use by upstream host connections:

```
interface tokenring 0
 dspu enable-host lsap 10
```

Related Commands

Command	Description
dspu host (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.

dspu enable-host (QLLC)

To enable an X.121 subaddress for use by upstream host connections via Qualified Logical Link Control (QLLC), use the **dspu enable-host** command in interface configuration mode. To disable the X.121 subaddress, use the **no** form of this command.

dspu enable-host qllc *x121-subaddress*

no dspu enable-host qllc *x121-subaddress*

Syntax Description

qllc	Specifies that the interface will use QLLC.
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 upstream host connections:

```
interface serial 0
 encapsulation x35
 x25 address 3202
 x25 map qllc 320112
 dspu enable-host qllc 320108
```

Related Commands

Command	Description
dspu host (QLLC)	Defines a DSPU 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.

dspu enable-host (SDLC)

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

dspu enable-host sdlc *sdlc-address*

no dspu enable-host sdlc *sdlc-address*

Syntax Description

sdlc	Specifies that the interface will use SDLC.
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 upstream host connections:

```
interface serial 0
 encapsulation sdlc
 sdlc role secondary
 sdlc address c1
 dspu enable-host sdlc c1
```

Related Commands

Command	Description
dspu host (SDLC)	Defines a DSPU host over an SDLC connection.
sdlc address	Assigns a set of secondary stations attached to the serial link.
sdlc role	Establishes the router to be either a primary or secondary SDLC station.

dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)

To enable an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstreamphysical unit (PU) connections, use the **dspu enable-pu** command in interface configuration mode. To disable the connection, use the **no** form of this command.

dspu enable-pu [**lsap** *local-sap*]

no dspu enable-pu [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Local service access point (SAP) address used by the downstream physical unit (DSPU) to establish connection with the remote host. The default local SAP address is 8.

Defaults

The default local SAP address is 8.

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.

Examples

The following example demonstrates the configuration of a downstream PU via Token Ring and Ethernet:

```
interface tokenring 0
 ring-speed 16
 dspu enable-pu lsap 8

interface ethernet 0
 dspu enable-pu lsap 8
```

Related Commands

Command	Description
dspu pu (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), virtual data-link control (VDLC), or NCIA connections.

dspu enable-pu (QLLC)

To enable an X.121 subaddress for use by downstream physical unit (PU) connections via Qualified Logical Link Control (QLLC), use the **dspu enable-pu** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

dspu enable-pu qllc *x121-subaddress*

no dspu enable-pu qllc *x121-subaddress*

Syntax Description

qllc	Required keyword for Qualified Logical Link Control (QLLC) data-link control.
x121-subaddress	Variable-length X.121 address. It is assigned by the X.25 network service provider.

Defaults

No default address is assigned.

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 an X.121 subaddress for use by downstream PU connections:

```
interface serial 0
 encapsulation x25
 x25 address 3201
 x25 map qllc 320208
 dspu enable-pu qllc 08
```

Related Commands

Command	Description
dspu pu (QLLC)	Defines a downstream PU over an X.25 connection explicitly.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.

dspu enable-pu (SDLC)

To enable an Synchronous Data Link Control (SDLC) address for use by downstream physical unit (PU) connections, use the **dspu enable-pu** command in interface configuration mode. To disable the connection, use the **no** form of this command.

dspu enable-pu sdlc *sdlc-address*

no dspu enable-pu sdlc *sdlc-address*

Syntax Description

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

Defaults

No default 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

The following example enables a downstream physical unit (DSPU) downstream connection:

```
interface serial 0
 encapsulation x25
 sdlc role primary
 sdlc address c1
 dspu enable-pu sdlc c1
```

Related Commands

Command	Description
dspu pu (SDLC)	Defines a DSPU host over an SDLC connection.
sdlc address	Assigns a set of secondary stations attached to the serial link.
sdlc role	Establishes the router to be either a primary or secondary SDLC station.

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

To define a downstream physical unit (DSPU) host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections, use the **dspu host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu 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 dspu 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	The specified DSPU 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) SAP address of the remote host PU. The default is 4.
lsap *local-sap*	(Optional) Local SAP address used by the DSPU to establish connection with the remote host. The default is 12.
interface *slot/port]*	(Optional) Slot and port number of the interface. The slash mark is required.
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 DSPU attempts to retry establishing connection with 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 DSPU attempts to retry establishing connection with remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Specifies that the host link will be used for the focal point support.

Defaults

The default remote SAP address is 4.
The default local SAP address is 12.
The default window size is 7.
The default maximum I-frame is 1472.
The default number of retries 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.

Usage Guidelines

The local SAP address must be enabled by one of the following commands: **dspu enable-host**, **dspu rsrb enable-host**, or **dspu vdlc enable-host**.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the lower of the two values is used.

Alerts from downstream PUs will be forwarded to the focal point host. The **focalpoint** keyword must be included in no more than one **dspu host** command.

Examples

The following example shows the definition for a DSPU host with 252 logical unit (LU)s and a connection to be established across an RSRB link:

```
dspu rsrb 88 1 99 4000.ffff.0001
dspu rsrb enable-host lsap 10
dspu host ibm3745 xid 06500001 rmac 4000.3745.0001 lsap 10
dspu pool hostpool lu 2 253 host ibm3745
```

Related Commands

Command	Description
dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay)	Enables a local SAP on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts.
dspu pool	Defines a range of host LUs in an LU pool.
dspu rsrb enable-host	Enables an RSRB SAP for use by DSPU host connections.
dspu rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name through the RSRB.
dspu start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name.
dspu vdlc enable-host	Enables a SAP for use by DSPU host connections.

dspu host (Frame Relay)

To define a downstream physical unit (DSPU) host over a Frame Relay connection, use the **dspu host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

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

no dspu 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	The specified DSPU 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*	Frame Relay data-link connection identifier (DLCI) number; a decimal number.
rsap *rsap-addr*	(Optional) Remote service access point (SAP) address.
lsap *lsap-addr*	(Optional) Local SAP address.
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 DSPU attempts to retry establishing connection with remote host physical unit (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 DSPU attempts to retry establishing connection with remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Specifies that the host link will 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 is 1472.
The default retry count is 255.
The default retry timeout is 30 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 local SAP address must be enabled by a **dspu enable-host** command.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the lower of the two values is used.

Alerts from downstream PUs will be forwarded to the focal point host. The **focalpoint** keyword must be included in no more than one **dspu host** command.

Examples The following example defines a DSPU host for Frame Relay support:

```
dspu host rosebud xid-snd 06500001 dlci 200 rsap 4 lsap 12
```

Related Commands

Command	Description
dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay)	Enables a local SAP on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts.
dspu pool	Defines a range of host LUs in an LU pool.

dspu host (QLLC)

To define a downstream physical unit (DSPU) host over an X.25 or Qualified Logical Link Control (QLLC) connection, use the **dspu host** command in global configuration mode. To delete the DSPU host definition, use the **no** form of this command.

dspu 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 dspu 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	The specified DSPU 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*	Remote X.121 address.
qllc *local-x121-subaddr*	(Optional) Local X.121 subaddress.
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 DSPU attempts to retry establishing connection with 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 DSPU attempts to retry establishing connection with remote host physical unit (PU). The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Specifies that the host link will be used for the focal point support.

Defaults

The default window size is 7.
The default maximum I-frame 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.

Usage Guidelines

The X.121 subaddress must be enabled by a **dspu enable-host** command.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the lower of the two values is used.

Alerts from downstream PUs will be forwarded to the focal point host. The **focalpoint** keyword must be included in no more than one **dspu host** command.

Examples

The following example defines a DSPU host:

```
dspu host hosta xid-snd 065ffff0 x25 00000123005 qllc 12
```

Related Commands

Command	Description
dspu enable-host (QLLC)	Enables an X.121 subaddress for use by upstream host connections through QLLC.
dspu pool	Defines a range of host LUs in an LU pool.
dspu start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name.

dspu host (SDLC)

To define a downstream physical unit (DSPU) host over an Synchronous Data Link Control (SDLC) connection, use the **dspu host** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu host *host-name* **xid-snd** *xid* **sdlc** *sdlc-addr* [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

no dspu host *host-name* **xid-snd** *xid* **sdlc** *sdlc-addr* [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*] [**focalpoint**]

Syntax Description

host-name	The specified DSPU 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 hexadecimal address.
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 window size is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with remote host physical unit (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 DSPU attempts to retry establishing connection with remote host PU. The range is from 1 to 600 seconds. The default is 30 seconds.
focalpoint	(Optional) Specifies that the host link will be used for the focal point support.

Defaults

The default window size is 7.
The default maximum I-frame is 1472.
The default number of retries is 255.
The default retry timeout is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

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

Usage Guidelines

The SDLC address must be enabled by a **dspu enable-host** command.

If an XID is received from a remote PU that indicates it supports a different maximum I-frame size, then the lower of the two values is used.

Alerts from downstream PUs will be forwarded to the focal point host. The **focalpoint** keyword must be included in no more than one **dspu host** command.

Examples

The following example defines a DSPU host for SDLC:

```
dspu host hosta xid-snd 065ffff0 sdlc c1
```

Related Commands

Command	Description
dspu enable-host (SDLC)	Enables an SDLC address for use by upstream host connections.
dspu pool	Defines a range of host LUs in an LU pool.

dspu lu

To define a dedicated logical unit (LU) or a range of LUs for an upstream host and a downstream physical unit (PU), use the **dspu lu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu lu *lu-start* [*lu-end*] {**host** *host-name host-lu-start* | **pool** *pool-name*} [**pu** *pu-name*]

no dspu lu *lu-start* [*lu-end*] {**host** *host-name host-lu-start* | **pool** *pool-name*} [**pu** *pu-name*]

Syntax Description

lu-start	Starting LU address in the range of LUs to be assigned from a pool or dedicated to a host.
lu-end	(Optional) Ending LU address in the range of LUs to be assigned from a pool or dedicated to a host.
host *host-name host-lu-start*	Specifies that each LU in the range of LUs will be dedicated to a host LU *host-name* value. The range of host LUs starts with the *host-lu-start* address.
pool *pool-name*	Specifies that each LU in the range of LUs will be assigned from the specified pool.
pu *pu-name*	(Optional) Downstream PU for which this range of LUs is being defined.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

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

Usage Guidelines

If the **dspu lu** command immediately follows a **dspu default-pu** or **dspu pu** command, then the **dspu lu** command is applied to that PU**, and the pu** *pu-name* option is not necessary for the **dspu lu** command.

If the keyword and argument are included, the LU defined by the **dspu lu** command will be applied to the named PU.

The **pool** and **host** keywords are mutually exclusive. You can define a range of LUs to be either assigned from a pool or dedicated to a host.

Examples

The following example defines downstream LUs as dedicated LUs. The downstream PU, ciscopu, has three downstream LUs with addresses 2 and 4. When ciscopu establishes a connection with the downstream physical unit (DSPU), the three downstream LUs (2, 3, and 4) are dedicated to LUs 22, 23, and 24, respectively, from the IBM 3745 host.

```
dspu host ibm3745 xid-snd 065000001 rmac 4000.3745.0001
dspu pu ciscopu xid-rcv 05D00001 rmac 1000.5AED.1F53
dspu lu 2 4 host ibm3745 22
```

Related Commands

Command	Description
dspu default-pu	Enables the default PU feature to be used when a downstream PU attempts to connect, but does not match any of the explicit PU definitions.
dspu host (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu host (QLLC)	Defines a DSPU host over an X.25/QLLC connection.
dspu host (SDLC)	Defines a DSPU host over an SDLC connection.
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
dspu pool	Defines a range of host LUs in an LU pool.
dspu pu (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu pu (QLLC)	Defines a downstream PU over an X.25 connection explicitly.
dspu pu (SDLC)	Defines a DSPU host over an SDLC connection.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.

dspu ncia

To configure the native client interface architecture (NCIA) server as the underlying transport, use the **dspu ncia** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu ncia [*server-number*]

no dspu ncia [*server-number*]

Syntax Description

server-number	(Optional) Server number configured in the **ncia server** command. Currently, only one NCIA server is supported.

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

You must use the **ncia server** command to configure an NCIA server on the router before using the **dspu ncia** command to configure the NCIA server as the underlying transport.

Examples

The following example configures the NCIA server as the underlying transport mechanism communicating directly with the downstream physical unit (DSPU):

```
dspu ncia 1
```

Related Commands

Command	Description
dspu ncia enable-pu	Enables a SAP on the NCIA server for use by downstream connections.
ncia server	Configures an NCIA server on a Cisco router.

dspu ncia enable-pu

To enable a destination service access point (DSAP) on the native client interface architecture (NCIA) server for use by downstream connections, use the **dspu ncia enable-pu** command in global configuration mode. To disable the SAP, use the **no** form of this command.

dspu ncia enable-pu [**lsap** *local-sap*]

no dspu ncia enable-pu [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for receiving incoming connection attempts. The default is 8.

Defaults

The default local SAP is 8.

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 8 is enabled for use by the downstream PU CISCOPU-A:

```
dspu ncia 1
dspu ncia enable-pu lsap 8
!
dspu host HOST-9370 xid-snd 11100001 rmac 4000.1060.1000 rsap 4 lsap 4
!
dspu pu CISCOPU-A xid-rcv 01700001
dspu lu 2 6 host HOST-9370 2
!
interface TokenRing 0
 ring-speed 16
 llc2 xid-retry-time 0
 dspu enable-host lsap 4
 dspu start HOST-9370
```

Related Commands

Command	Description
dspu ncia	Configures the NCIA server as the underlying transport.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.

dspu notification-level

To specify the downstream physical unit (DSPU) notifications to send to Simple Network Management Protocol (SNMP) and Systems Network Architecture (SNA) network management, use the **dspu notification-level** command in global configuration mode. To specify the default notification level **low**, use the **no** form of this command.

dspu notification-level {**off** | **low** | **medium** | **high**}

no dspu notification-level

Syntax Description

off	Sends neither SNMP traps nor unsolicited SNA messages for the DSPU.
low	Sends physical unit (PU) and logical unit (LU) activation failures only.
medium	Sends PU state changes and PU and LU activation failures.
high	Sends both PU and LU state changes and activation failures.

Defaults

The default notification level is low.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command applies to both SNMP traps and unsolicited SNA messages to the operator. The upstream PU and LU notification events and the LU state change notification events are not sent as unsolicited SNA messages to the operator. These events are sent as SNMP traps only.

Examples

The following example sets the notification level to enable the DSPU to send notifications to network management for both PU and LU state changes and activation failures:

```
dspu notification-level high
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of SNMP notifications.

dspu pool

To define a range of host logical unit (LU)s in an LU pool, use the **dspu pool** command in global configuration mode. To remove the definition, use the **no** form of this command.

dspu pool *pool-name* **host** *host-name* **lu** *lu-start* [*lu-end*] [**inactivity-timeout** *minutes*]

no dspu pool *pool-name* **host** *host-name* **lu** *lu-start* [*lu-end*] [**inactivity-timeout** *minutes*]

Syntax Description

pool-name	Name identifier of the pool.
host *host-name*	Name of the host that owns the range of host LUs in the pool.
lu *lu-start*	Starting LU address in the range of host LUs in the pool.
lu-end	(Optional) Ending address (inclusive) of the range of host LUs in the pool. If no ending address is specified, only one LU (identified by the *lu-start* argument) will be defined in the pool.
inactivity-timeout *minutes*	(Optional) Interval of inactivity (in minutes) on either the system services control points (SSCP)-LU or LU-LU sessions, which will cause the downstream LU to be disconnected from the upstream LU. The default is disabled.

Defaults

The inactivity-timeout is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You can include multiple **dspu pool** commands that specify the same pool name. In this way, an LU pool can include several LU ranges from the one host physical unit (PU), or it can include LUs from different host PUs. The LUs from the host *host-name* value starting at the *lu-start* value and ending with the *lu-end* value, inclusive, will be included in the pool *pool-name*. For the LUs in this pool, if there is no traffic on either the SSCP-LU or LU-LU sessions for the inactivity timeout number of minutes, the downstream LU will be disconnected from the upstream LU, and the upstream LU will be allocated to any downstream LU waiting for a session. A value of zero for inactivity minutes means no timeouts. (The inactivity timeout applies to all LUs in this pool, not just the LUs defined by this **dspu pool** command. The last value configured will be used.)

Examples

The following example defines a pool of host LUs. A pool of 253 host LUs is defined with all LUs supplied from the ibm3745 host PU:

```
dspu host ibm3745 xid-snd 065000001 rmac 4000.3745.0001
dspu pool hostpool host ibm3745 lu 2 254
```

The following example defines multiple pools and defines a disjoint pool of host LUs. One pool with a total of 205 host LUs and second pool with a total of 48 host LUs are defined with all LUs supplied from the same ibm3745 host PU. Host LUs with addresses 2 to 201 and 250 to 254 are defined in hostpool1. Host LUs with addresses 202 to 249 are defined in hostpool2.

```
dspu host ibm3745 xid-snd 065000001 rmac 4000.3745.0001
dspu pool hostpool1 host ibm3745 lu 2 201
dspu pool hostpool2 host ibm3745 lu 202 249
dspu pool hostpool1 host ibm3745 lu 250 254
```

The following example defines a pool of LUs from multiple hosts. A pool of 506 host LUs is defined with 253 LUs supplied by the ibm3475 host PU and 253 supplied by the ibm3172 host PU.

```
dspu host ibm3745 xid-snd 065000001 rmac 4000.3745.0001
dspu host ibm3172 xid 06500002 rmac 4000.3172.0001
dspu pool hostpool host ibm3745 lu 2 254
dspu pool hostpool host ibm3172 lu 2 254
```

Related Commands

Command	Description
dspu host (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu host (QLLC)	Defines a DSPU host over an X.25/QLLC connection.
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), or virtual data-link control (VDLC) connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)

To define an explicit downstream physical unit (PU) over Token Ring, Ethernet, FDDI, remote source-route bridging (RSRB), virtual data-link control, or NCIA connections, use the **dspu pu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu pu *pu-name* [**rmac** *remote-mac*] [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**interface** *slot | port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

no dspu pu *pu-name* [**rmac** *remote-mac*] [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Syntax Description

pu-name	Name of the downstream PU.
rmac *remote-mac*	(Optional) MAC address of the downstream PU.
rsap *remote-sap*	(Optional) service access point (SAP) address of the downstream PU. The default is 4.
lsap *local-sap*	(Optional) Local SAP address used by the downstream physical unit (DSPU) to establish connection with the downstream PU. The default is 8.
xid-rcv *xid*	(Optional) Specifies a match on exchange identification (XID).
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive sizes used for the downstream PU link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is from 1 to 600 seconds. The default is 30 seconds.

Defaults

The default remote SAP is 4.
The default local SAP is 8.
The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 4.
The default retry timeout is 30 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 local SAP address must be enabled by one of the following commands:

- **dspu enable-pu lsap fo5**
- **dspu ncia enable-pu lsap**
- **dspu rsrb enable-pu lsap**
- **dspu vdlc enable-pu lsap**

The send and receive maximum I-frame size includes the Systems Network Architecture (SNA) transmission header (TH) and request/response (RH), but does not include the data-link control header. The DSPU feature will segment frames being sent to fit within this frame size. If an XID is received from a remote PU, which indicates that it supports a different maximum I-frame size, then the lower of the two values is used.

If you want the DSPU to attempt a ConnectOut to the remote node using the **dspu start** command, you must configure the **rmac** keyword and argument. If you want this PU to match against a ConnectIn attempt, then several combinations of the **rmac**, **rsap**, and **xid-rcv** keywords are possible. The matching algorithms are as follows:

- **rmac**—Match on remote MAC/SAP address of downstream PU.
- **xid-rcv**—Match on XID value received from downstream PU.
- **rmac/rsap, xid-rcv**—Match on remote MAC or SAP address of downstream PU and XID value received from downstream PU.

If an XID is received from a remote PU, which indicates that it supports a different maximum I-frame size, then the lower of the two values is used.

For Cisco IOS Release 11.3 and later releases, the number of DSPU PUs that can be configured is 1024.

Examples

In the following example, a downstream PU is defined with only the MAC address and SAP address specified. A downstream PU that attempts an incoming connection to the DSPU will be accepted only if the remote MAC or SAP address matches the configured values for this downstream PU (and the proper local SAP address is enabled).

```
dspu pu ciscopu rmac 1000.5AED.1F53 rsap 20
dspu lu 2 5 pool hostpool
interface tokenring 0
dspu enable-pu lsap 8
```

In the following example, a downstream PU is defined with only an **xid-rcv** value. Any downstream PU that attempts an incoming connection specifying the **xid-rcv** value, 05D00001, will be accepted without regard to remote MAC or SAP address (although the proper local SAP address must be enabled).

```
dspu pu ciscopu xid-rcv 05d00001
dspu lu 2 5 pool hostpool
interface tokenring 0
 dspu enable-pu lsap 8
```

In the following example, a downstream PU is defined with **xid-rcv**, **rmac**, and **rsap** keywords. Any downstream PU that attempts to connect in to the DSPU must match all three configured values for the connection to be accepted (the proper local SAP address must also be enabled).

```
dspu pu ciscopu rmac 1000.5AED.1F53 rsap 20 xid-rcv 05d00001
dspu lu 2 5 pool hostpool
interface tokenring 0
 dspu enable-pu lsap 8
```

Related Commands

Command	Description
dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)	Enables an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstream PU connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.
dspu ncia enable-pu	Enables a SAP on the NCIA server for use by downstream connections.
dspu rsrb enable-pu	Enables an RSRB SAP for use by DSPU downstream connections.
dspu rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name through the RSRB.
dspu start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name.
dspu vdlc enable-pu	Enables a SAP for use by DSPU virtual data-link control (VDLC) downstream connections.

dspu pu (Frame Relay)

To define a downstream physical unit (DSPU) host over a Frame Relay connection, use the **dspu pu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu pu *pu-name* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**interface** *slot | port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

no dspu pu *pu-name* **dlci** *dlci-number* [**rsap** *remote-sap*] [**lsap** *local-sap*] [**xid-rcv** *xid*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Syntax Description

pu-name	Name of the downstream physical unit (PU).
dlci *dlci-number*	Frame Relay data-link connection identifier (DLCI) number. This number is a decimal.
rsap *remote-sap*	(Optional) service access point (SAP) address of the downstream PU. The default is 4.
lsap *local-sap*	(Optional) Local SAP address used by the DSPU to establish connection with the downstream PU. The default is 8.
xid-rcv *xid*	(Optional) Specifies a match on exchange identification (XID).
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive sizes used for the downstream PU link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is from 1 to 600 seconds. The default is 30 seconds.

Defaults

The default remote SAP is 4.
The default local SAP is 8.
The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 4.
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 downstream PU:

```
dspu pu pub dlci 8
```

Related Commands

Command	Description
dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)	Enables an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstream PU connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu pu (QLLC)

To explicitly define a downstream physical unit (PU) over an X.25 connection, use the **dspu pu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu pu *pu-name* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**xid-rcv** *xid*] [**interface** *slot | port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

no dspu pu *pu-name* **x25** *remote-x121-addr* [**qllc** *local-x121-subaddr*] [**xid-rcv** *xid*] [**interface** *slot | port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Syntax Description

pu-name	Name of the downstream PU.
x25 *remote-x121-addr*	Variable-length X.121 address. It is assigned by the X.25 network service provider.
qllc *local-x121-subaddr*	(Optional) Local X.121 subaddress.
xid-rcv *xid*	(Optional) Specifies a match on exchange identification (XID).
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive sizes used for the downstream PU link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is from 1 to 600 seconds. The default is 30 seconds.

Defaults

The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 4.
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 downstream PU:

```
dspu pu testpu x25 32012 qllc 12 xid-rcv 05d00001
```

Related Commands

Command	Description
dspu enable-pu (QLLC)	Enables an X.121 subaddress for use by downstream PU connections through QLLC.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu pu (SDLC)

To define a downstream physical unit (DSPU) host over an Synchronous Data Link Control (SDLC) connection, use the **dspu pu** command in global configuration mode. To cancel the definition, use the **no** form of this command.

dspu pu *pu-name* **sdlc** *sdlc-addr* [**xid-rcv** *xid*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

no dspu pu *pu-name* **sdlc** *sdlc-addr* [**xid-rcv** *xid*] [**interface** *slot/port]*] [**window** *window-size*] [**maxiframe** *max-iframe*] [**retries** *retry-count*] [**retry-timeout** *retry-timeout*]

Syntax Description

pu-name	Name of the downstream PU.
sdlc *sdlc-addr*	SDLC address.
xid-rcv *xid*	(Optional) Specifies a match on exchange identification (XID).
interface *slot/port]*	(Optional) Slot and port number of the interface.
window *window-size*	(Optional) Send and receive sizes used for the downstream PU link. The range is from 1 to 127. The default is 7.
maxiframe *max-iframe*	(Optional) Maximum number of I-frames that can be sent or received across the link. The range is from 64 to 18432. The default is 1472.
retries *retry-count*	(Optional) Number of times the DSPU attempts to retry establishing connection with downstream PU. The range is from 0 to 255 (0 = no retry attempts, 255 = infinite retry attempts). The default is 4.
retry-timeout *retry-timeout*	(Optional) Delay (in seconds) between DSPU attempts to retry establishing connection with downstream PU. The range is from 1 to 600 seconds. The default is 30 seconds.

Defaults

The default window size is 7.
The default maximum I-frame is 1472.
The default retry count is 4.
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 downstream PU:

```
dspu pu testpu sdlc c1 interface serial 1/1
```

Related Commands

Command	Description
dspu enable-pu (SDLC)	Enables an SDLC address for use by downstream PU connections.
dspu lu	Defines a dedicated LU or a range of LUs for an upstream host and a downstream PU.

dspu rsrb

To define the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the downstream physical unit (DSPU) feature will simulate at the remote source-route bridging (RSRB), use the **dspu rsrb** command in global configuration mode. To cancel the definition, use the **no** form of this command.

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

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

Syntax Description

local-virtual-ring	DSPU local virtual ring number.
bridge-number	Bridge number connecting the DSPU local virtual ring and the RSRB target virtual ring. The valid range is from 1 to 15.
target-virtual-ring	RSRB target virtual ring number. The RSRB target virtual ring corresponds to the **ring-number** value defined by a **source-bridge ring-group** command.
virtual-macaddr	DSPU virtual MAC address.

Defaults

No default behavior or values.

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 *bridge-number* argument can be specified only once in a configuration.

Use the **dspu rsrb** command to enable DSPU host and downstream connections to be established across an RSRB link.

If the **local-ack** value is specified on the **source-bridge remote-peer** statement, DSPU will establish host connections across RSRB using local acknowledgment. DSPU cannot support local acknowledgment for downstream PU connections across RSRB.

Examples

The following example defines DSPU to start a connection to the host across an RSRB link (without local acknowledgment). The DSPU is identified by its local ring number 88 and its virtual MAC address 4000.FFFF.0001. When the DSPU attempts an outgoing connection to the ibm3745 host, the connection will be established across the RSRB virtual ring 99.

```
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

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

dspu host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10
dspu rsrb start ibm3745
interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

The following example defines the DSPU to start a connection to the host across an RSRB link (with local acknowledgment). The DSPU is identified by its local ring number 88 and its virtual MAC address 4000.FFFF.0001. When the DSPU attempts an outward connection to the ibm3745 host, the connection will be established across the RSRB virtual ring 99 using RSRB local acknowledgment.

```
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 local-ack

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

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

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

The following example define the s DSPU to allow a connection from the downstream PU across an RSRB link. The DSPU is identified by its local ring number 88 and its virtual MAC address 4000.FFFF.0001. The downstream PU will specify the DSPU virtual MAC address 4000.FFFF.0001 and SAP address 20 in its host definitions. The DSPU will accept incoming connections from the downstream PU across the RSRB virtual ring 99.

```
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

dspu rsrb 88 1 99 4000.FFFF.0001
dspu rsrb enable-pu lsap 20

dspu pu ciscopu xid-rcv 05D00001 lsap 20

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
dspu rsrb enable-host	Enables an RSRB SAP for use by DSPU host connections.
dspu rsrb enable-pu	Enables an RSRB SAP for use by DSPU downstream connections.
dspu rsrb start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name through the RSRB.
source-bridge ring-group	Defines or removes a ring group from the configuration.
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.

dspu rsrb enable-host

To enable an remote source-route bridging (RSRB) service access point (SAP) for use by downstream physical unit (DSPU) host connections, use the **dspu rsrb enable-host** command in global configuration mode. To disable the RSRB SAP, use the **no** form of this command.

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

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

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP 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 is 12.

Command Modes

Global configuration

Command History

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

Examples

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

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

dspu 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
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections.
dspu rsrb	Defines the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the DSPU feature will simulate at the RSRB.

dspu rsrb enable-pu

To enable an remote source-route bridging (RSRB) service access point (SAP) for use by downstream physical unit (DSPU) downstream connections, use the **dspu rsrb enable-pu** command in global configuration mode. To disable the SAP, use the **no** form of this command.

dspu rsrb enable-pu [**lsap** *local-sap*]

no dspu rsrb enable-pu [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts. The default is 8.

Defaults

The default local SAP is 8.

Command Modes

Global configuration

Command History

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

Examples

In the following example, the local SAP address 20 of the RSRB is enabled for use by the ciscopu DSPU downstream 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

dspu rsrb 88 1 99 4000.FFFF.0001
dspu rsrb enable-pu lsap 20

dspu pu ciscopu xid-rcv 05D00001 lsap 20
```

Related Commands

Command	Description
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.
dspu rsrb	Defines the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the DSPU feature will simulate at the RSRB.

dspu rsrb start

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

dspu rsrb start {*host-name* | *pu-name*}

no dspu rsrb start {*host-name* | *pu-name*}

Syntax Description

host-name	Name of a host defined in a **dspu host** (Token Ring, Ethernet, FDDI, RSRB, virtual data-link control (VDLC)) command.
pu-name	Name of a PU defined in a **dspu host** (Token Ring, Ethernet, FDDI, RSRB, VDLC) command.

Defaults

No default behavior or values.

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

Before issuing this command, you must enable the correct local service access point (SAP) with the appropriate enable command (**dspu rsrb enable-host** for a host resource, and **dspu rsrb enable-pu** for a PU resource).

This command is valid only if the target MAC address has been defined in the resource. For a host resource, this is not a problem because the MAC address is mandatory, but for a PU resource the MAC address is optional. The command will fail if the MAC address is missing.

Examples

In the following example, the downstream physical unit (DSPU) will initiate a connection with the ibm3745 host 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

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

dspu host ibm3745 xid-snd 06500001 rmac 4000.3745.0001 lsap 10
```

```
dspu rsrb start ibm3745

interface serial 0
 ip address 10.10.13.1 255.255.255.0
```

Related Commands

Command	Description
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.
dspu rsrb	Defines the local virtual ring, virtual bridge, target virtual ring, and virtual MAC address that the DSPU feature will simulate at the RSRB.
dspu rsrb enable-host	Enables an RSRB SAP for use by DSPU host connections.
dspu rsrb enable-pu	Enables an RSRB SAP for use by DSPU downstream connections.

dspu start

To specify that an attempt will be made to connect to the remote resource defined by host name or physical unit (PU) name, use the **dspu start** command in interface configuration mode. To cancel the definition, use the **no** form of this command.

dspu start {*host-name* | *pu-name*}

no dspu start {*host-name* | *pu-name*}

Syntax Description

host-name	Name of a host defined in a **dspu host** command.
pu-name	Name of a PU defined in a **dspu pu** command.

Defaults

No default behavior or values.

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

Before issuing this command, you must enable the correct address using the appropriate **dspu enable-host** or **dspu enable-pu** command.

This command is valid only if the target address (remote MAC [RMAC], Synchronous Data Link Control [SDLC], data-link connection identifier [DLCI], or X.25 parameter) has been defined for the resource. For a host resource, this is not a problem because the address specification is mandatory, but for a PU resource, specifying the address is optional. The **dspu start** command will fail if the address is missing.

Examples

In the following example, the downstream physical unit (DSPU) will initiate a connection with the ciscopu downstream PU on Token Ring interface 0:

```
dspu pu ciscopu xid-rcv 05D00001 rmac 1000.5AED.1F53 lsap 20
interface tokenring 0
 dspu enable-pu lsap 20
 dspu start ciscopu
```

Related Commands

Command	Description
dspu enable-host (Token Ring, Ethernet, FDDI, Frame Relay)	Enables a local service access point (SAP) on Token Ring, Ethernet, FDDI, or Frame Relay interfaces for use by upstream hosts.
dspu enable-host (QLLC)	Enables an X.121 subaddress for use by upstream host connections through QLLC.
dspu enable-host (SDLC)	Enables an SDLC address for use by upstream host connections.
dspu enable-pu (Ethernet, Frame Relay, Token Ring, FDDI)	Enables an Ethernet, Frame Relay, Token Ring, or FDDI address for use by downstream PU connections.
dspu enable-pu (SDLC)	Enables an SDLC address for use by downstream PU connections.
dspu enable-pu (QLLC)	Enables an X.121 subaddress for use by downstream PU connections through QLLC.
dspu host (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu host (QLLC)	Defines a DSPU host over an X.25/QLLC connection.
dspu host (SDLC)	Defines a DSPU host over an SDLC connection.
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
dspu pu (Frame Relay)	Defines a DSPU host over a Frame Relay connection.
dspu pu (QLLC)	Defines a downstream PU over an X.25 connection explicitly.
dspu pu (SDLC)	Defines a DSPU host over an SDLC connection.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.

dspu vdlc

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

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

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

Syntax Description

ring-group	Local virtual ring number identifying the SRB ring group.
virtual-mac-address	Virtual MAC address that represents the DSPU 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 example defines the DSPU to start a connection to the host using virtual data-link control. The DSPU virtual data-link control is identified by its virtual MAC address 4000.4500.01f0, existing on the SRB virtual ring 99. When the DSPU attempts an outgoing connection to the host HOST-B, the connection will be established across the virtual ring 99.

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

dspu vdlc 99 4000.4500.01f0
dspu vdlc enable-host lsap 12
```

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

dspu 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.
dspu vdlc enable-host	Enables a SAP for use by DSPU host connections.
dspu vdlc enable-pu	Enables a SAP for use by DSPU VDLC downstream connections.
dspu vdlc start	Specifies that an attempt will be made to connect to the remote resource defined by host name or PU name through VDLC.
source-bridge ring-group	Defines or removes a ring group from the configuration.

dspu vdlc enable-host

To enable a service access point (SAP) for use by downstream physical unit (DSPU) host connections, use the **dspu vdlc enable-host** command in global configuration mode. To disable the SAP, use the **no** form of this command.

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

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

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP 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 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 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

dspu vdlc 99 4000.4500.01f0
dspu vdlc enable-pu lsap 8
dspu vdlc enable-host lsap 12

dspu host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint
dspu pool pool-b host HOST-B lu 2 254

dspu host HOST3K-A xid-snd 05d0000a rmac 4000.3000.0100 rsap 8 lsap 12
dspu pool pool3k-a host HOST3K-A lu 2 254

dspu pu PU3K-A xid-rcv 05d0000a rmac 4000.3000.0100 rsap 10 lsap 8
dspu lu 2 254 pool pool-b

dspu default-pu
dspu lu 2 5 pool pool3k-a

dspu vdlc start HOST-B
```

```
dspu vdlc start HOST3K-A
dspu vdlc start PU3K-A

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

Related Commands

Command	Description
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or virtual data-link control (VDLC) connections.
dspu vdlc	Identifies the local virtual ring and virtual MAC address that will be used to establish DSPU host and downstream connections over DLSw+ using VDLC.

dspu vdlc enable-pu

To enable a service access point (SAP) for use by downstream physical unit (DSPU) virtual data-link control downstream connections, use the **dspu vdlc enable-pu** command in global configuration mode. To disable the SAP, use the **no** form of this command.

dspu vdlc enable-pu [**lsap** *local-sap*]

no dspu vdlc enable-pu [**lsap** *local-sap*]

Syntax Description

lsap *local-sap*	(Optional) Specifies that the local SAP address will be activated as an upstream SAP for both receiving incoming connection attempts and for starting outgoing connection attempts. The default is 8.

Defaults

The default local SAP is 8.

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 8 is enabled for use by the downstream PU PU3K-A:

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

dspu vdlc 99 4000.4500.01f0
dspu vdlc enable-pu lsap 8
dspu vdlc enable-host lsap 12

dspu host HOST-B xid-snd 065bbbb0 rmac 4000.7000.01f1 rsap 4 lsap 12 focalpoint
dspu pool pool-b host HOST-B lu 2 254

dspu host HOST3K-A xid-snd 05d0000a rmac 4000.3000.0100 rsap 8 lsap 12
dspu pool pool3k-a host HOST3K-A lu 2 254

dspu pu PU3K-A xid-rcv 05d0000a rmac 4000.3000.0100 rsap 10 lsap 8
dspu lu 2 254 pool pool-b

dspu default-pu
dspu lu 2 5 pool pool3k-a

dspu vdlc start HOST-B
```

```
dspu vdlc start HOST3K-A
dspu vdlc start PU3K-A
interface serial 3
 description IP connection to dspu7k
 ip address 10.10.16.2 255.255.255.0
 clockrate 4000000
```

Related Commands

Command	Description
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.
dspu vdlc	Identifies the local virtual ring and virtual MAC address that will be used to establish DSPU host and downstream connections over DLSw+ using VDLC.

dspu vdlc start

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

dspu vdlc start {*host-name* | *pu-name*}

no dspu vdlc start {*host-name* | *pu-name*}

Syntax Description

host-name	Name of a host defined in a **dspu host** command.
pu-name	Name of a PU defined in a **dspu host** 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 appropriate enable command (**dspu vdlc enable-host** for a host resource, and **dspu vdlc enable-pu** for a PU resource).

This command is valid only if the target MAC address has been defined in the resource. For a host resource, this is not a problem because the MAC address is mandatory, but for a PU resource the MAC address is optional. The command will fail if the MAC address is missing.

Examples

In the following example, the downstream physical unit (DSPU) attempts to initiate connections with host PU HOST-B, host PU HOST3k-A, and downstream PU PU3k-A over data-link switching plus (DLSw+) using virtual data-link control:

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

dspu vdlc 99 4000.4500.01f0
dspu vdlc enable-pu lsap 8
dspu vdlc enable-host lsap 12

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

```
dspu pool pool-b host HOST-B lu 2 254

dspu host HOST3K-A xid-snd 05d0000a rmac 4000.3000.0100 rsap 8 lsap 12
dspu pool pool3k-a host HOST3K-A lu 2 254

dspu pu PU3K-A xid-rcv 05d0000a rmac 4000.3000.0100 rsap 10 lsap 8
dspu lu 2 254 pool pool-b

dspu default-pu
dspu lu 2 5 pool pool3k-a
dspu vdlc start HOST-B
dspu vdlc start HOST3K-A
dspu vdlc start PU3K-A

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

Related Commands

Command	Description
dspu host (Token Ring, Ethernet, FDDI, RSRB, VDLC)	Defines a DSPU host over Token Ring, Ethernet, FDDI, RSRB, or VDLC connections.
dspu pu (Token Ring, Ethernet, FDDI, RSRB, VDLC, NCIA)	Defines an explicit downstream PU over Token Ring, Ethernet, FDDI, RSRB, VDLC, or NCIA connections.
dspu vdlc	Identifies the local virtual ring and virtual MAC address that will be used to establish DSPU host and downstream connections over DLSw+ using VDLC.
dspu vdlc enable-host	Enables a SAP for use by DSPU host connections.
dspu vdlc enable-pu	Enables a SAP for use by DSPU VDLC downstream connections.