

RIF Passthru in DLSw+

Feature Summary

By default, DLSw+ terminates the RIF for Token Ring, terminates the LLC for all media types and forwards data only across a WAN with DLSw+ and TCP/IP headers. The RIF is a field in source-route bridged frames that indicates the SRB path the frame should take when traversing a Token Ring network. In the case of an explorer packet, the RIF is a field of the source-route bridged frame that indicates the SRB path that the SRB explorer has traversed so far. The RIF is limited to seven hop counts by the IBM standards. Because DLSw+ terminates the RIF at the virtual ring, the network's scalability increases because the hop count of the packet starts over, and the packet can traverse seven additional hops. Also, RIF termination simplifies network design because ring numbers no longer have to be unique throughout an entire enterprise.

However, some environments do not function properly if the RIF is terminated. For that reason, DLSw+ now supports the RIF Passthru feature, in which the entire source-route bridged path appears in the RIF.

Figure 1 shows a DLSw+ network without the RIF Passthru feature configured.

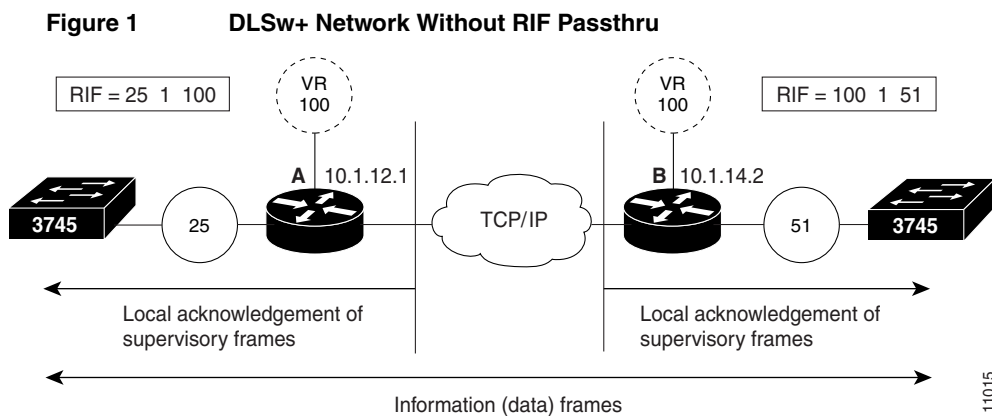
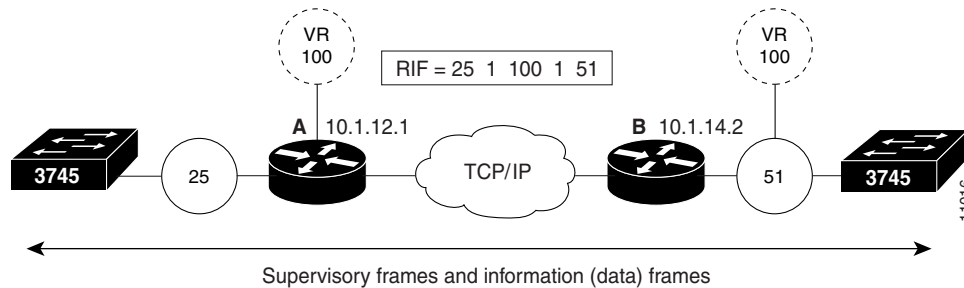


Figure 2 shows a DLSw+ network with the RIF Passthru feature configured.

Figure 2 DLSw+ Network with RIF Passthru



Benefits

When DLSw+ is used between FEPs (PU 4s), the RIF Passthru feature enables two key functions. First, RIF Passthru is required to allow multiple active paths between FEPs. Second, RIF Passthru is required to remotely load an NCP (in other words, set initialization mode/request initialization mode support).

List of Terms

Set initialization mode—DLC command that initiates system-specified procedures to initialize link-level functions.

Request initialization mode—DLC command that requests system-specified procedures to initialize link-level functions

Remote NCP load—Operation that occurs when an IBM 3745 does not contain a network control program (NCP). The IBM 3745 replies with request initialization mode when it is contacted by the host. The host (partner NCP) sends a set initialization mode, and then remotely transmits an NCP to the IBM 3745.

Restrictions

The DLSw+ RIF Passthru feature works only on Token Ring LANs via SRB. Other LAN types, such as SDLC and 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

Platforms

This feature is supported on the following platforms:

- Cisco 2500 series
- Cisco 3600 series
- Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco 7200 series
- Cisco 7500 series

Prerequisites

- Define a Source-Bridge Ring Group for DLSw+
- Define a DLSw+ Local Peer for the Router
- Enable DLSw+ on a Token Ring Interface

Define a Source-Bridge Ring Group for DLSw+

The source-bridge ring can be shared between DLSw+ and SRB/RSRB. In DLSw+, the source-bridge ring group specifies the virtual ring that will appear to be the last ring in the RIF. Because RIFs are terminated at the router, there is no correlation between the ring-group number specified in DLSw+ peers. The numbers can be the same for management simplicity, but they do not have to be the same.

In DLSw+ with RIF Passthru, however, the ring numbers must be unique throughout the network and DLSw peers must have the same virtual ring number because RIFs are passed through.

To define a source-bridge ring group for DLSw+, perform the following task in global configuration mode:

Task	Command
Define a ring group.	source-bridge ring-group <i>ring-group</i> [<i>virtual-mac-address</i>]

Define a DLSw+ Local Peer for the Router

Defining a DLSw+ local peer for a router enables DLSw+. You specify all local DLSw+ parameters as part of the local peer definition. To define a local peer, perform the following task in global configuration mode:

Task	Command
Define the DLSw+ local peer.	dlsw local-peer [peer-id <i>ip-address</i>] [group <i>group</i>] [border] [cost <i>cost</i>] [If <i>size</i>] [keepalive <i>seconds</i>] [passive] [promiscuous] [init-pacing-window <i>size</i>] [max-pacing-window <i>size</i>][biu-segment]

Enable DLSw+ on a Token Ring Interface

To enable DLSw+ on a Token Ring interface, perform the following task in interface configuration mode:

Task	Command
Enable DLSw+ on a Token Ring interface.	source-bridge <i>local-ring bridge-number ring-group</i>

Supported MIBs and RFCs

None.

Configuration Task

To configure DLSw+ RIF Passthru, define the DLSw+ remote peer with TCP encapsulation.

Configure Remote Peer with TCP Encapsulation

To configure TCP encapsulation on a remote peer, perform the following task in global configuration mode:

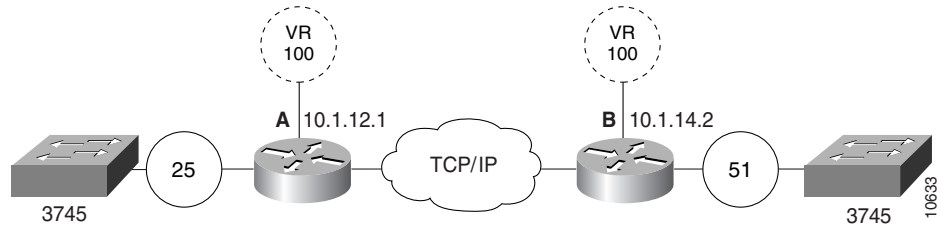
Task	Command
Define a TCP encapsulation remote peer.	dlsw remote-peer <i>list-number tcp ip-address</i> [backup-peer [<i>ip-address</i> frame-relay interface serial <i>number dlc-number</i> interface name]] [bytes-netbios-out <i>bytes-list-name</i>] [cost <i>cost</i>] [dest-mac <i>mac-address</i>] [dmac-output-list <i>access-list-number</i>] [dynamic] [host-netbios-out <i>host-list-name</i>] [keepalive <i>seconds</i>] [lf <i>size</i>] [linger <i>minutes</i>] [lsap-output-list <i>list</i>] [no-llc <i>minutes</i>] [priority] [rif-passthru <i>virtual ring number</i>] [tcp-queue-max <i>size</i>] [timeout <i>seconds</i>]

Note The *virtual ring number* specified when the **rif-passthru** keyword is used with the **dlsw remote-peer** command is the same *virtual ring number* specified in the local peer's **source-bridge ring-group** statement.

Configuration Examples

Figure 3 is a sample configuration for DLSw+ using the RIF Passthru feature.

Figure 3 Network Configuration with RIF Passthru



Router A

```
source-bridge ring-group 100
dlsw local-peer peer id 10.1.12.1
dlsw remote-peer 0 tcp 10.1.14.2 rif-passthru 100

interface tokenring 0
  ring-speed 16
  source-bridge 25 1 100
  source-bridge spanning
```

Router B

```
source-bridge ring-group 100
dlsw local-peer peer id 10.1.14.2
dlsw remote-peer 0 tcp 10.1.12.1 rif-passthru 100

interface tokenring 0
  ring-speed 16
  source-bridge 51 1 100
  source-bridge spanning
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 11.3 command references.

- **dlsw remote-peer tcp**

dlsw remote-peer tcp

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

```
dlsw remote-peer list-number tcp ip-address [backup-peer [ip-address | frame-relay
interface serial number dlci-number | interface name]] [bytes-netbios-out bytes-list-name]
[cost cost] [dest-mac mac-address] [dmac-output-list access-list-number] [dynamic]
[host-netbios-out host-list-name] [inactivity minutes] [dynamic] [keepalive seconds]
[If size] [linger minutes] [lsap-output-list list] [no-llc minutes] [passive] [priority]
[rif-passthru virtual ring number] [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]] [bytes-netbios-out bytes-list-name]
[cost cost] [dest-mac mac-address] [dmac-output-list access-list-number] [dynamic]
[host-netbios-out host-list-name] [inactivity minutes] [dynamic] [keepalive seconds]
[If size] [linger minutes] [lsap-output-list list] [no-llc minutes] [passive] [priority]
[rif-passthru virtual ring number] [tcp-queue-max size] [timeout seconds]
```

Syntax Description

<i>list-number</i>	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.
tcp <i>ip-address</i>	IP address of the remote peer with which the router is to communicate.
backup-peer <i>ip-address</i>	(Optional) IP address of the existing TCP/FST peer for which this peer is the backup peer.
backup-peer frame-relay interface serial <i>number dlci number</i>	(Optional) Serial interface and DLCI number of the existing direct LLC2 frame-relay peer for which this peer is the backup peer.
backup-peer interface <i>name</i>	(Optional) Interface name of the existing direct peer for which this peer is the backup peer.
bytes-netbios-out <i>bytes-list-name</i>	(Optional) Configures NetBIOS bytes output filtering for this peer. The <i>bytes-list-name</i> argument is the name of the previously defined NetBIOS bytes access list filter.
cost <i>cost</i>	(Optional) The cost to reach this remote peer. The valid range is 1 to 5.

dest-mac <i>mac-address</i>	(Optional) Permits the TCP connection to be established only when there is an explorer frame destined for the specified 48-bit MAC address written in dotted triplet form.
dmac-output-list <i>access-list-number</i>	(Optional) Permits the TCP connection to be established only when the explorer frame passes the specified access list. The <i>access-list-number</i> is the list number specified in an access-list command.
dynamic	(Optional) Permits the TCP connection to be established only when there is DLSw+ data to send.
host-netbios-out <i>host-list-name</i>	(Optional) Configures NetBIOS host output filtering for this peer. The <i>host-list-name</i> is the name of the previously defined NetBIOS host access list filter.
inactivity <i>minutes</i>	(Optional) Configures the length of time a connection can be idle before closing the dynamic remote peer connection. The valid range is 1 to 300 minutes. The default is 5 minutes.
keepalive <i>seconds</i>	(Optional) Sets the keepalive interval for this remote peer. The range is 0 to 1200 seconds. The default is 30 seconds in the absence of any data being sent over the peer connection.
if <i>size</i>	(Optional) Largest frame size, in bytes, this local peer will use on a circuit to avoid segmented frames. Valid sizes are 516, 1470, 1500, 2052, 4472, 8144, 11407, 11454, and 17800 bytes.
linger <i>minutes</i>	(Optional) Configures length of time the backup peer remains connected after the primary peer connection is reestablished. The valid range is 1 to 300 minutes. The default is 5 minutes.
lsap-output-list <i>list</i>	(Optional) Filters output IEEE 802.5 encapsulated packets. Valid access list numbers are in the range 200 to 299.
no-llc <i>minutes</i>	(Optional) Configures the length of time a remote peer remains connected after all LLC2 connections are gone. The valid range is 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: <ul style="list-style-type: none">• High—2065• Medium—1981• Normal—1982• Low—1983

rif-passthru <i>virtual ring number</i>	(Optional) Configures the remote peer as RIF-passthru. The <i>virtual ring number</i> value is the same number as the <i>ring number</i> value assigned in the source-bridge ring-group commands of the DLSw+ Passthru peers.
tcp-queue-max <i>size</i>	(Optional) Maximum output TCP queue size for this remote peer. The valid maximum TCP queue size is a number in the range 10 to 2000. The default queue size is 200.
timeout <i>seconds</i>	(Optional) Configures the retransmit time limit for TCP. The valid range is 5 to 1200 seconds. The default is 90 seconds.

Defaults

No peer IP address is identified.

The **linger** option is inactive. If the **linger** option is added with no minutes specified, the default is 5 minutes.

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.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3. The following keywords and arguments first appeared in Cisco IOS Release 11.1: **dynamic**, **inactivity** *minutes*, **linger** *minutes*, **no-llc** *minutes* and **timeout** *seconds*. The following keywords and arguments first appeared in Cisco IOS Release 11.2: **dest-mac** *mac-address*, **dmac-output-list** *access-list-number*, **linger** *minutes*. The following keyword first appeared in Cisco IOS Release 11.3 T: **rif-passthru** *virtual ring number*.

SNA DDR technology allows switched links to be closed during idle periods. To enable this feature, set the **keepalive** option to 0 and configure the **timeout** option. When the **dynamic** option is configured, the **keepalive** option 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** option is a shortcut over the **dmac-output-list** option.

Use the **linger** option to specify that a backup peer will remain connected for a specified period of time after the primary connection is gone.

When the **priority** option 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 APPN is running with DLSw+ and you specify the **priority** option on the **dlsw remote-peer** command, then the SNA TOS will map APPN class of service (COS) to TCP TOS and will preserve the APPN COS characteristics throughout the network.

Examples

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

```
dlsw remote-peer 0 fst 10.2.18.9
dlsw remote-peer 1 tcp 10.2.17.8 backup-peer 10.2.18.9
```

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

```
dlsw remote-peer 1 tcp 10.2.17.8
```

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 precedence to routine precedence.

```
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
```

Related Commands

show dlsw peers

