

DLSw+ Ethernet Redundancy

Feature Overview

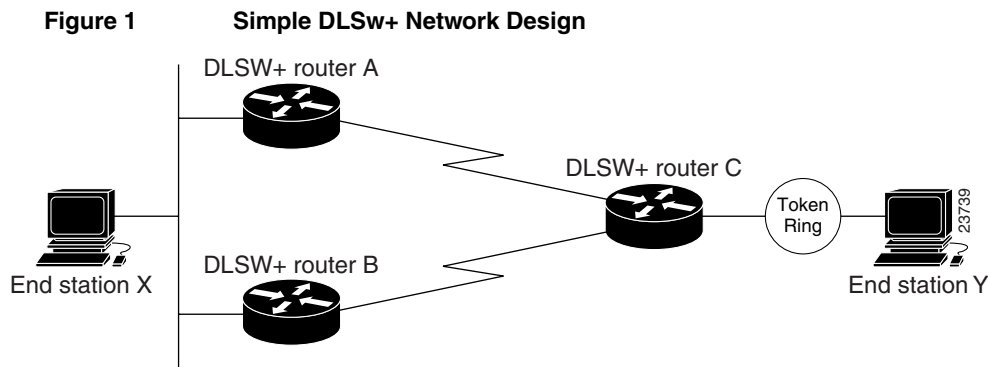
The DLSw+ Ethernet Redundancy feature provides redundancy and load balancing between multiple DLSw+ peers in an Ethernet environment. It enables DLSw+ to support parallel paths between two points in an Ethernet environment, ensuring resiliency in the case of a router failure and providing load balancing for traffic load. The feature also enables DLSw+ to support multiple DLSw+ routers on the same transparent bridged domain that can reach the same MAC address in a switched environment.

DLSw+ could provide redundancy prior to this feature in a Token Ring environment or via backup peers. When an end station on an Ethernet LAN had multiple active paths into a DLSw+ network, problems occurred (Figure 1).

The reason redundancy is not possible in an Ethernet environment is because, unlike Token Ring, it does not have a RIF field in its packet. The RIF notifies a router of the path a packet has traveled by tracking each ring number and bridge it travels through a path. If a bridge notices that the next ring matches a ring already in the RIF, then the frame is not copied on that ring. The RIF prevents:

- Unreliable Local Reachability Information
- Circuit Contention
- Undetected Looping Explorers

Configuring redundancy with Ethernet switches provides a special challenge. When there are multiple DLSw+ routers on the same transparent bridged domain that can reach the same MAC address, problems are created because of the inherent manner in which switches handle and direct traffic.



Unreliable Local Reachability Information

When DLSw+ services to a transparent bridged domain (such as Ethernet), the local cache is populated with unreliable information. Because there is no RIF, the DLSw+ device has no way of determining whether the frame it receives is locally sourced or whether it originates from another DLSw+ device within the same transparent bridged domain. The DLSw+ router updates its local or remote cache based on whether it receives the packet from its LAN or from a WAN.

In Figure 1, assume end station X and end station Y are trying to communicate with each other. (Suppose X is a terminal and Y is a host.) The following sequence typically occurs:

- End station Y searches for end station X and sends out a TEST frame with an SMAC of Y and a DMAC of X.
- Router C updates its LOCAL cache with end device Y when it receives the TEST frame.
- Router C goes into SEARCHING REMOTE state for MAC address X and sends CUR_ex frames to Router A and Router B because it has no reachability information for device X.
- Router A receives the CUR_ex explorer and sends out a TEST frame on the local LAN segment searching for device X because it does not have any reachability information on device X.
- Router B picks up the TEST frame transmitted on the LAN by Router A and observes that the SMAC is Y, and incorrectly assumes that Y sourced the frame on the LAN.
- Router B incorrectly updates its LOCAL cache with Y.
- Router B also receives the CUR_ex explorer frame from Router C and the same sequence of events occurs for Router B.

As a result, a loss of connectivity occurs because Router A and Router B think device Y is local.

Circuit Contention

Redundant paths in an Ethernet environment also cause circuit contention. In Figure 1, assume Router A and Router B correctly update their caches with REMOTE reachability information for end station Y. The following sequence occurs:

- End station X sends an XID on the Ethernet LAN for end station Y.
- Router A and Router B pick up the packet and attempt to start a DLSw+ circuit by sending a CUR_cs to Router C. Assume Router A's CUR_cs reaches Router C first.

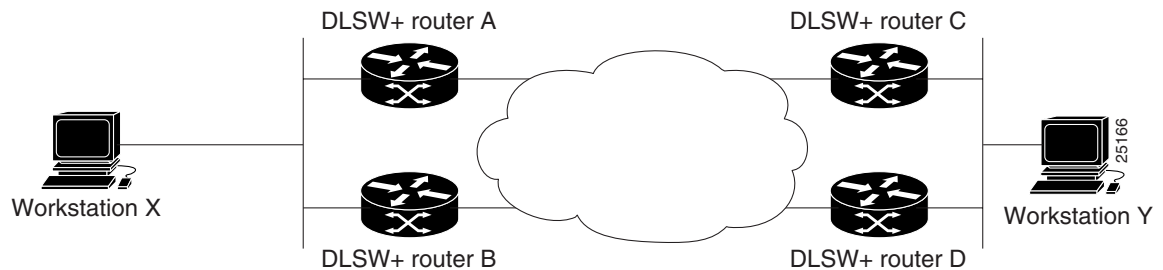
- Router C uses the CUR_cs information to set up a DLSw+ circuit and responds to Router A with an ICR_cs.
- Router C receives the second CUR_cs from Router B.

As a result, Router C interprets the second CUR_cs as a duplicate circuit. It disallows the second circuit and as per RFC 1795, it tears down the original circuit, thereby permitting no data flow between the end systems.

Undetected Looping Explorers

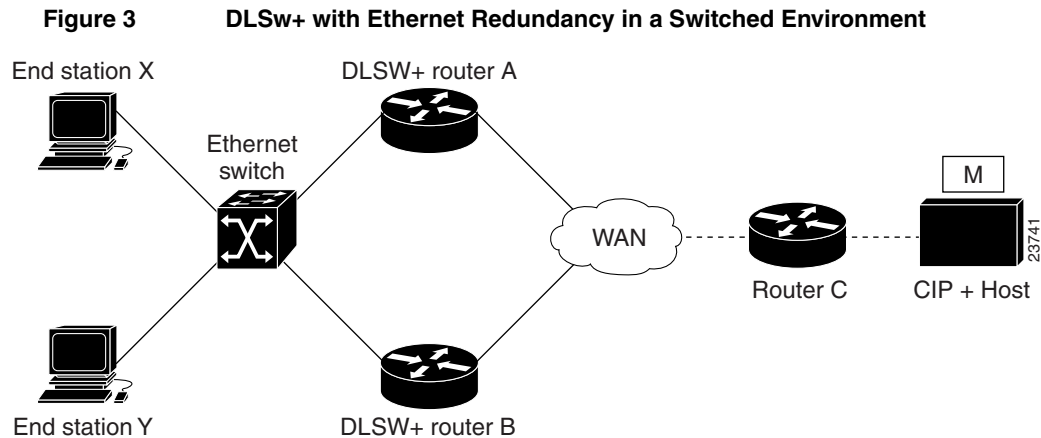
Figure 2 shows an Ethernet-to-Ethernet design that causes undetected looping explorers. It is a problematic design because Ethernet does not have a RIF. The routers do not know whether a packet destined for an unknown MAC address originated on their own LAN or from another LAN. As a result, the explorer packet would loop back to the originating LAN, wasting bandwidth and creating unnecessary CPU overhead.

Figure 2 Ethernet-to-Ethernet DLSw+ Network



Issues in a Switched Environment

Ethernet redundancy with switch devices requires further changes because of the way in which switches handle and direct traffic. Switches direct traffic by observing a frame's SMAC and by observing from which port the frame arrives. They forward all traffic to a particular address from a specific port rather than flooding all of its ports. In a normal Ethernet environment, this method is sufficient because there can only be one unique path to any MAC address. However, this method does not work in an environment where there are multiple DLSw+ routers on the same transparent bridged domain that can reach the same MAC address (Figure 3).



Because Routers A and B are connected to different ports on the Ethernet switch, the switch sees traffic from one SMAC coming into multiple ports. The Ethernet switch thinks the MAC address of the Host appears on two different places on a LAN. This design breaks the Ethernet rule of having only one path to any MAC address. It gives the appearance of a bridging loop that the Spanning-Tree Protocol did not resolve. Because SNA is connection oriented, the session is eventually torn down.

Benefits

Master Router

The DLSw+ Ethernet Redundancy feature solves the circuit contention issue by designating a master router in a transparent bridged domain. All devices on a transparent bridged domain advertise their presence to a multicast MAC address. One of the peers is elected as the master router. This master router maintains a database of all circuits being handled by the DLSw+ devices within its domain. Each device on the transparent bridged maintains an LLC2 session with the master router and asks the master router for permission before starting or accepting a new DLSw+ circuit. Because the master router keeps a database of the circuits being handled, it prevents duplicate circuits from being created for the same SNA session.

In Figure 4, DLSw+ Routers A, B, and C are on the same transparent bridged domain. Router B is configured to be the master router.

Note Master Router B can also be the master router by election. Once the routers within a transparent bridged domain learn each other's MAC address, the router with the lowest MAC address is elected as the master router if the master router is not already configured.

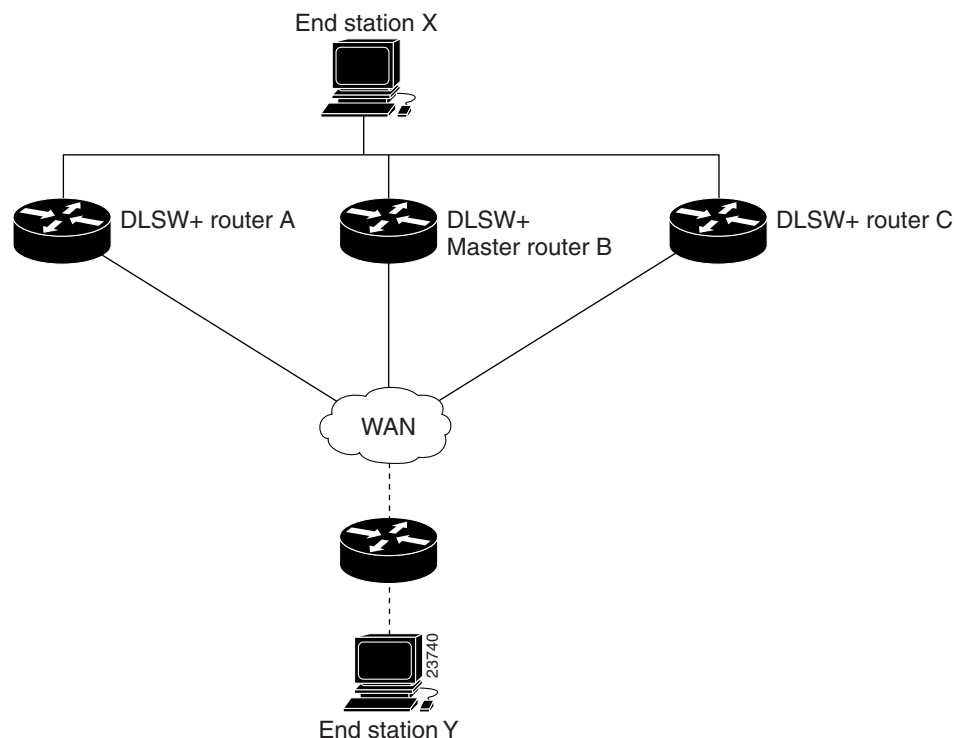
The following sequence occurs:

- End station X sends a SABME to Y (which is seen by all three routers) to begin a NetBIOS session to end station Y. Assume Routers A, B and C already have remote reachability for end station Y in their remote reachability caches at the time end station X sends a SABME.
- Router A and Router C indicate they want the circuit by sending IWANTIT frames to master Router B. IWANTIT frames are sent only in response to frames that start a circuit (SABME, XID); they are not sent in response to an explorer.

- Master Router B can also take the circuit. It waits, however, a designated amount of time before deciding which router gets the circuit in order to receive all qualified recipients. Master Router B bases its decision on the load information that is included in the IWANTIT frame of each router. In this particular case, we will assume that master Router B decides that Router A should have the circuit and sends Router A an UGOTIT primitive frame.
- Master Router B also denies permission to Router C by sending it a CIRCUIT_TAKEN (CKT_TKN) primitive frame. Master Router B then updates its own cache reachability tables, indicating that the circuit is taken.
- Router A sends a CUR_cs to its remote peer to establish a circuit once it receives permission from the master router.

When the circuit disconnects, Router A notifies master Router B by sending it a CIRCUIT_GONE (CKT_GONE) primitive. The master router then forwards the CKT_GONE primitive to the other devices on the LAN and removes the circuit from its CKT_TKN database. The only time a master router deletes a record is when it is notified by the device to which it granted the circuit or if there is a device failure and it loses its LLC2 session with that peer.

Figure 4 DLSw+ with the Ethernet Redundancy Feature Enabled



Source MAC (SMAC) Conversion

The DLSw+ Ethernet Redundancy feature enables more reliable local cache reachability information and decreases the chance for looping explorers. Normally, when DLSw+ devices receive a TEST frame they update their local or remote cache with the SMAC based on whether the packet came from its local LAN or off a WAN. As explained earlier in the document, in transparent bridged domains this can create a situation with unreliable reachability information. With the DLSw+ Ethernet Redundancy feature enabled, the SMAC of an explorer packet sent on the LAN is replaced

by the DLSw+ router's own MAC address. When another router on the transparent bridged domain receives the explorer, it recognizes that the SMAC belongs to a DLSw+ router on its own LAN. Therefore it does not update its local reachability cache and it does not forward the explorer over any of its peer connections.

In Figure 4, DLSw+ Routers A, B, and C are on the same transparent bridged domain. The following sequence occurs:

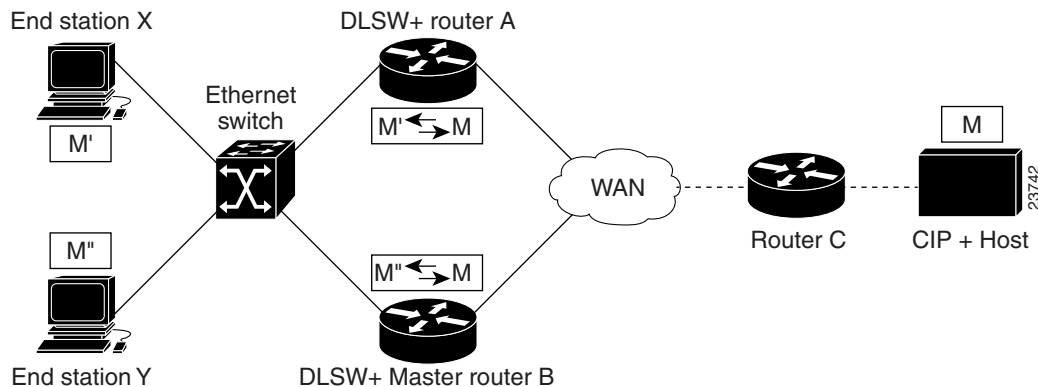
- End station Y sends an explorer looking for X. The remote peer sends a CUR_ex to A, B and C across the WAN.
- Router C populates its REMOTE reachability cache with Y.
- Router C internally tracks that it is SEARCHING for device X and that when it finds device X, it must inform device Y (from the peer path from which the original CUR_ex came).
- Router C transmits an explorer on the LAN because it does not have any reachability information on X. While doing so, it substitutes Y with its own MAC address in the SMAC field of the TEST frame and then it sends the TEST frame on the LAN.
- Routers A and B see the explorer from the LAN, but because they recognize Router C's MAC address in the SMAC field, they do not update their local reachability cache and do not forward the explorer over any of their DLSw+ peer connections. (Routers A, B and C have learned of each others MAC address during the master election process.)
- End station X recognizes its MAC address in the TEST poll frame and responds to the SMAC, which is Router C.
- Routers A and B recognize this MAC address and do not act on the frame. The frame reaches Router C, which recognizes the frame as a response to its test poll.
- Router C updates its LOCAL cache with X and remembers that end station Y was the original device searching for X. It replaces the MAC address with the original SMAC before sending an ICR_ex reply back to the peer that originally sent the CUR_ex.
- Routers A and B similarly respond to the remote peer's CUR_ex by sending a TEST frame and substituting Y with their own MAC addresses.

Switch Support

The DLSw+ Ethernet Redundancy feature provides redundancy in a switched environment with MAC address mapping. MAC address mapping ensures that a particular SMAC is seen by the switch on only one port at a time. Furthermore, the routers monitor each other's MAC address mapping so that they adequately serve as each other's back up in the case of a router failure.

In Figure 5, Router A is configured to map MAC address M' (M prime) to MAC address M and Router B is configured to map MAC address M'' (M double prime) to MAC address M. End device X is configured to use M' as its SNA DMAC and end device Y is configured to use M'' as its SNA DMAC.

Figure 5 DLSw+ Network Showing MAC Address Mapping



In Figure 5, the following sequence occurs:

- End device X sends out a TEST poll searching for its DMAC M'.
- The switch floods the request to all its ports because it is a new circuit and the switch does not recognize M'.
- The switch notes the port through which X can be reached.
- Router A sees the TEST poll and recognizes that it is mapping M' to MAC address M. It replies to the switch with a TEST final.
- The switch populates its cache with M' and, because it now knows the location of X, the frame is directed out a single port rather than flooded to all its ports.
- The end station sends an XID because it is ready to start an SNA session.
- The Ethernet switch directs the frame out the port to which Router A is attached because it has seen a packet with the SMAC of M'.
- Router A asks Router B permission to take the circuit since Router B is configured as the master.
- Router A receives permission to take the circuit because Router A is doing MAC address mapping for M' to M. Router A sends a CUR_cs to begin the process of creating a circuit.
- Router A does MAC address translation by replacing M' in the DMAC field with M, the actual MAC address of the mainframe resource. From this point forward, any frames directed from Router A toward the WAN are referred to as M and any frames being directed from Router A toward the LAN are referred to as M'. Some level of load balancing is achieved if half of the end stations are configured to use DMAC M' and the other half are configured to use M''.

In the case of a router failure, the other router detects the failure and seamlessly takes over the failed router's mapping responsibilities. In Figure 5, if Router A fails, the switch thinks it can still reach MAC address M' out the port that is connected to failed Router A. Router B takes over the mapping responsibilities for Router A by sending a TEST frame with SMAC M' and a multicast DMAC to the switch. The switch notes the SMAC M' and assumes the resource moved and updates its CAM table appropriately. Now end station X tries to reestablish its connection to the mainframe by sending out an XID poll to its configured DMAC M'. The switch knows to direct this frame out the port to which Router B is attached because of the TEST frame Router B sent earlier. Router B assumes the mapping responsibilities of Router A by mapping M' to M and continues its own mapping responsibilities of mapping M'' to M.

When Router A recovers, master Router B realizes that Router A should be mapping M' to M. Both Routers cannot map M' to M simultaneously because the switch cannot handle multiple ports with reachability to the same MAC address. Master Router B, therefore, stops mapping M' to M and the existing sessions are taken down and recovered through Router A.

Restrictions

- Transparent bridging cannot be enabled on an Ethernet interface configured for Ethernet Redundancy.
- Do not configure the **dlsw bridge-group** command on the same router on which Ethernet redundancy has been configured on one or more interfaces.
- DLSw+ local switching is not supported between two Ethernet Redundancy interfaces, nor between an Ethernet Redundancy interface and any other LAN-type media (TR, ISL, LANE, or FDDI).
- Correct operation cannot be guaranteed unless all DLSw+ devices connected to a shared, switched, or transparently bridged Ethernet domain support are configured for Ethernet redundancy. All such devices must be configured to use the same multicast MAC address. Incorrect configuration can easily result in loss of connectivity to all devices on the Ethernet domain.
- Because of issues with the propagation of UI frames, NetBIOS browsing is not supported in this release. A user must know the NetBIOS name of the server to which they wish to connect.

Supported Platforms

This feature is supported on the following platforms:

- Cisco 1600 series (bnr2sy and bnr2y images)
- Cisco 1720 router (bnr2sy and bnr2y images)
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 3800 series
- Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco 7200 series
- Cisco 7500 series
- Catalyst 5000 with RSM or RSFC

Supported MIBs and RFCs

MIBs

No MIBs are supported.

For descriptions of supported MIBs and how to use MIBs, see Cisco's MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

None.

Configuration Tasks

Perform the following tasks to configure the DLSw+ Ethernet Redundancy feature:

- Configuring Ethernet Redundancy
- Configuring Ethernet Redundancy in a Switched Environment

Configuring Ethernet Redundancy

Command	Purpose
<code>Router(config-if)# dlsw transparent redundancy-enable</code>	Enables the Ethernet Redundancy feature.

All routers on any given transparent bridged domain should configure the same MAC multicast address in the **dlsw transparent redundancy enable** command.

Configuring Ethernet Redundancy in a Switched Environment

Command	Purpose
<code>Router(config)# dlsw transparent-switch support</code>	Enables DLSw+ Ethernet Redundancy feature when using a switch device.
<code>Router(config-if)# dlsw transparent map</code>	Configures a single destination MAC address to which multiple MAC addresses on a transparent bridged are mapped.

Configuration, Verification, and Troubleshooting Tips

- Verify that the link is active.
- Verify that the peers are connected.

Perform the following steps to verify that the Ethernet Redundancy feature is configured properly:

- Step 1** Verify that the master router is configured correctly by issuing the **show dlsw transparent neighbor** command on the appropriate routers.
- Step 2** Verify that the created MAC address to which all the Ethernet Redundancy routers are mapped is configured correctly by issuing the **show dlsw transparent map** command on all the routers configured for Ethernet Redundancy. By viewing the output you can also verify that a router is configured to backup another router's MAC address mapping functions.
- Step 3** Verify that the cache of the routers is populating correctly by issuing the **show dlsw reachability** command on the Ethernet Redundancy routers.
- Step 4** Verify that circuits are being established through the Ethernet ports by issuing the **show dlsw circuits** command.
- Step 5** Verify that the master router has the correct circuits in its cache by issuing the **show dlsw transparent cache** command.
- Step 6** Verify the number of circuits being handled by each of those peers by issuing the **show dlsw peer** command on the Ethernet redundancy routers.

Monitoring and Maintaining

Command	Purpose
show dlsw transparent cache	Displays the master circuit cache for each transparent bridged domain.
show dlsw transparent map	Displays the MAC address mappings on the local router and any mappings for which the local router is acting as backup.
show dlsw transparent neighbor	Displays DLSw+ neighbors in a transparent bridged domain.

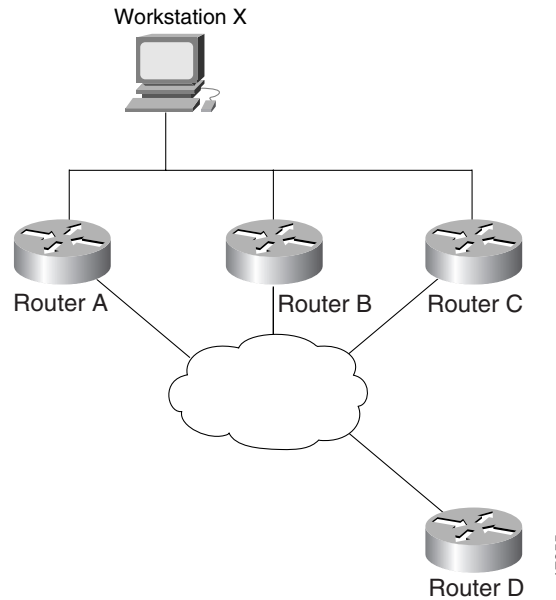
Configuration Examples

This section provides the following configuration examples:

- DLSw+ with Ethernet Redundancy Enabled
- DLSw+ and Ethernet Switch Support

Figure 6 shows that Router A, Router B, and Router C advertise their presence on the Ethernet via their Ethernet interfaces to the multicast MAC address 9999.9999.9999. Because Router B is the master router, it keeps a database of all circuits handled within the domain and grants or denies permission for new circuit requests for Router A and Router C. There is no special configuration required for the end stations or for the remote peer. Only the DLSw+ devices on the LAN need the extra configuration. Master Router B waits 1.5 seconds after it receives the first IWANTIT primitive before assigning the new SNA circuit to one of its ethernet redundancy peers because of the **dlsw transparent timers sna 1500** command.

Figure 6 DLSw+ with Ethernet Redundancy Enabled



Router A

```
dlsw local-peer peer id 10.2.24.2
dlsw remote-peer 0 tcp 10.2.17.1
int e1
 ip address 150.150.2.1 255.255.255.0
dlsw transparent redundancy-enable 9999.9999.9999
```

Router B

```
dlsw local-peer peer-id 10.2.24.3
dlsw remote-peer 0 tcp 10.1.12.1
int e1
 ip address 150.150.2.3 255.255.255.0
dlsw transparent redundancy-enable 9999.9999.9999 master priority 1
dlsw transparent timers sna 1500
```

Router C

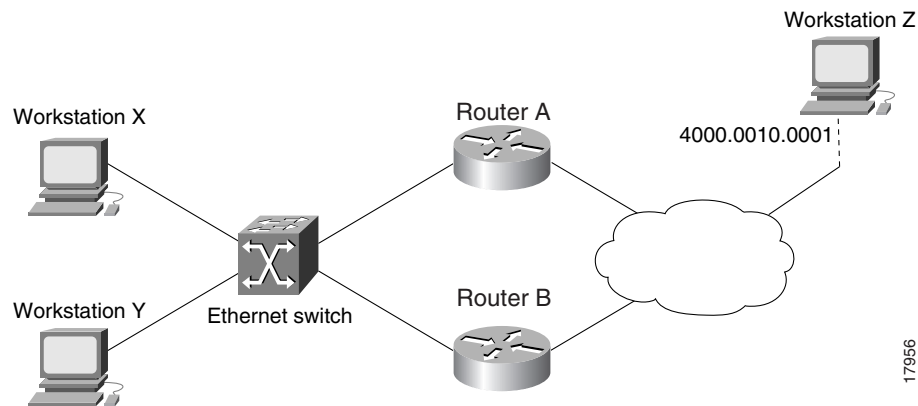
```
dlsw local-peer peer-id 10.2.24.4
dlsw remote-peer 0 tcp 10.2.17.1
int e1
 ip address 150.150.2.3 255.255.255.0
dlsw transparent redundancy-enable 9999.9999.9999
```

Router D

```
dlsw local-peer peer-id 10.2.17.1 promiscuous
```

Figure 7 is a sample configuration of the DLSw+ Ethernet Redundancy feature in a switched environment. The ethernet switch sees the device with MAC address 4000.0010.0001 one port at a time because Router A and Router B have mapped different MAC addresses to it. This configuration is known as MAC-address mapping. Router A is configured so that MAC address 4000.0001.0000 maps to the actual device with MAC address 4000.0010.0001. Router B is configured so that MAC address 4000.0201.0001 maps to the actual device with MAC address 4000.0010.0001. Router A and B backup one another. Router A is configured as the master with a default priority of 100. Master Router A waits 1.5 seconds after it receives the first IWANTIT primitive before assigning the new SNA circuit to one of its ethernet redundancy peers because of the **dlsw transparent timers sna 1500** command.

Figure 7 DLSw+ and Ethernet Switch Support



Router A

```
dlsw local peer peer-id 10.2.17.1
dlsw remote-peer 0 tcp 10.3.2.1
dlsw transparent switch-support
int e 0
  mac-address 4000.0000.0001
  ip address 150.150.2.1 255.255.255.0
dlsw transparent redundancy-enable 9999.9999.9999 master-priority
dlsw transparent map local-mac 4000.0001.0000 remote-mac 4000.0010.0001
neighbor 4000.0000.0011
dlsw transparent timers sna 1500
```

Router B

```
dlsw local peer peer-id 10.2.17.2 promiscuous
dlsw transport switch-support
int e 1
  mac-address 4000.0000.0011
  ip address 150.150.3.1 255.255.255.0
dlsw transparent redundancy-enable 9999.9999.9999
dlsw transparent local-mac 4000.0201.0001 remote-mac 4000.0010.0001
neighbor 4000.0000.0001
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- **dls w transparent map**
- **dls w transparent redundancy-enable**
- **dls w transparent switch-support**
- **dls w transparent timers**
- **show dls w transparent cache**
- **show dls w transparent map**
- **show dls w transparent neighbor**

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (`|`), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

```
command | {begin | include | exclude} regular-expression
```

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression “PeakRate” appears:

```
show atm vc | begin PeakRate
```

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

dlsw transparent map

To enable MAC address mapping in a switch-based environment, use the **dlsw transparent map** interface configuration command. 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* MAC address of the DLSw+ device that takes over mapping if the primary DLSw+ device becomes unavailable.

Command Mode

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was first introduced.

Usage Guidelines

Only the routers that are connected to the switch are configured for address mapping, therefore the command is required on all routers even if using just one local-mac address. You can configure the command with dummy local mac address

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
---------	-------------

dls w transparent-switch support Configures the DLSw+ Ethernet Redundancy feature when using a switch device. Must be configured prior to the **dls w transparent map** command.

dlsw transparent redundancy-enable

To configure transparent redundancy, use the **dlsw transparent redundancy-enable** interface configuration command. 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

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

Command Mode

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was first introduced.

Usage Guidelines

The same *multicast-mac-address* 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*.

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** of 100:

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

Related Commands

Command	Description
show dls w transparent neighbor	Displays whether the router with the lowest master priority is configured properly as the master router. This command displays all the neighbors within that transparent bridged domain.
show dls w transparent cache	Displays the content of the master's circuit cache.

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** global configuration command. To disable dlsw transparent switch support, use the **no** form of this command.

dlsw transparent switch-support
no dlsw transparent switch-support

Syntax

This command has no arguments or keywords.

Defaults

Switch support is off.

Command Mode

Global configuration

Command History

Release	Modification
12.0(5)T	This command was first introduced.

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	Maps multiple MAC addresses on a transparent bridged domain to a single destination MAC address.

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** interface configuration command. 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 <i>value</i>	(Optional) Timeout value for the NetBIOS session. The valid range is 100 to 900 ms. The default value is 400 ms.
sna <i>value</i>	(Optional) Timeout value for the SNA session. The valid range is 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.

Command Mode

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was first introduced.

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	Enables the Ethernet Redundancy feature and configures the master router.

show dlsw transparent cache

To display the master circuit cache for each transparent bridged domain, use the **show dlsw transparent cache** privileged EXEC command.

show dlsw transparent cache

Syntax

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

Issue the **show dlsw transparent cache** command on the master router of the transparent bridged domain.

Command History

Release	Modification
12.0(5)T	This command was first introduced.

Examples

The following is sample output from the **show dlsw transparent cache** command:

```
router#show dlsw transparent cache
Interface Ethernet0/1
  Circuit Cache
  local addr(lsap)    remote addr(dsap)  state           Owner
  0000.3028.92b6(08)  0007.0db1.238c(08) POSITIVE        SELF
  0000.3028.92b6(08)  0008.dec3.609e(12) NEGATIVE        0009.fa50.0b1c
Total number of circuits in the Cache:2
```

show dlsw transparent map

To display MAC address mappings on the local router and any mappings for which the local router is acting as backup for a neighbor peer, use the **show dlsw transparent map** privileged EXEC command.

show dlsw transparent map

Syntax

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was first introduced.

Usage Guidelines

Issue the **show dlsw transparent map** command to ensure that the local MAC address is the address created in the **dlsw transparent map** command. The command should be issued on all the routers configured for the Ethernet Redundancy feature to ensure the local MAC addresses match.

Examples

The following is sample output from the **show dlsw transparent map** command on two routers configured for the Ethernet Redundancy feature:

```
router6#show dlsw transparent map

Interface Ethernet6/2
  LOCAL Mac          REMOTE MAC          BACKUP
  -----          -
  0008.dec3.0080     0008.dec3.609e     0007.7fb0.1080     STATIC
  0008.dec3.0040     0008.dec3.609e     0007.7fb0.1080     DYNAMIC (Passive)

router7#show dlsw transparent map

Interface Ethernet0/1
  LOCAL Mac          REMOTE MAC          BACKUP
  -----          -
  0008.dec3.0080     0008.dec3.609e     0006.3a0a.1a55     DYNAMIC (Passive)
  0008.dec3.0040     0008.dec3.609e     0006.3a0a.1a55     STATIC
```

The output from Router 6 and Router 7 shows the created MAC addresses are 0008.dec3.0080 and 0008.dec3.0040.

show dlsw transparent neighbor

To display DLSw neighbors in a transparent bridged domain, use the **show dlsw transparent neighbor** privileged EXEC command.

show dlsw transparent neighbor

Syntax

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was first introduced.

Examples

The following is sample output from the **show dlsw transparent neighbor** command:

```
router7#show dlsw transparent neighbor
Interface ATM0.1
0006.e278.6c0e SELF Master
0009.fa50.0b1c Rcvd Master-Accepted VALID
```

The output shows that Router 7 is the master router whose MAC address is 0006.e278.6c0e. The other router, with a MAC address of 0009.fa50.0b1c, is a slave router on the common domain. The master router received a packet from the slave and notes the router is VALID