Configuring LDP

SYSTEM ADMINISTRATOR GUIDE

Contents

1 Overview

This document provides an overview of the Label Distribution Protocol (LDP) and describes the tasks and commands used to configure, monitor, troubleshoot, and administer LDP features through the SmartEdge router.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **Product Overview** folder of this Customer Product Information library.

1.1 LDP Implementation

The SmartEdge router implementation of LDP supports RFC 3036, *LDP Specification*. LDP enables dynamic label allocation and distribution in a Multiprotocol Label Switching (MPLS) network. A label-switched router (LSR) enabled with LDP can establish label-switched paths (LSPs) to other LSRs in the network. LDP creates label bindings by assigning labels to connected routers and by advertising the bindings to neighbors. LDP also assigns labels to label bindings learned from neighbors, and readvertises the binding to other neighbors. When an LSR advertises a label binding for a route, the LSR is advertising the availability of an LSP to the destination of that route. LDP can learn several LSPs from different neighbors for the same route. In this case, LDP activates only the path selected by the underlying Interior Gateway Protocol (IGP). For this reason, LDP must work together with an IGP, such as the Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) protocol.

To discover LDP peers, an LSR periodically transmits LDP Hello messages. After two LDP peers discover each other in this manner, LDP establishes a Transmission Control Protocol (TCP) connection between them. When the TCP connection is complete, an LDP session is established. In our implementation, the LDP router ID is used as the transport address.

During the LDP session, LSRs send LDP label mapping and withdrawal messages. LSRs allocate labels to directly connected interfaces and learn about labels from neighbors. If a directly connected interface is shut down, an LSR withdraws the label and stops advertising it to neighbors. If a neighbor stops advertising a label to an LSR, the label is withdrawn from that LSR's Label

Forwarding Information Base (LFIB). Teardown of LDP adjacencies or sessions results if Hello or keepalive messages are not received within the timer interval.

Be aware that the SmartEdge router supports a maximum of 1,200 targeted LDP sessions or a combination of up to 50 nontargeted sessions and 1,150 targeted sessions. Use the `max-session` command to configure the maximum number of LDP sessions supported on the router.

Note: LDP configuration is supported in the local context only.

1.2 LDP Neighbor Discovery

There are two types of LDP neighbor discovery mechanisms: basic LDP discovery and extended LDP discovery. Basic LDP discovery is used to discover immediate neighbors; extended LDP discovery is used to discover neighbors that can be multiple hops away.

1.3 LDP Hello Messages

There are two types of LDP Hello messages: link Hello messages and targeted Hello messages. Link Hello messages are multicast on an interface to immediate neighbors. Link Hello messages are used in basic LDP discovery. Targeted Hello messages are unicast directly to remote neighbors. Targeted Hello messages are used in extended LDP discovery. Two LDP speaking LSRs can form LDP adjacencies after discovering each other. LDP adjacencies discovered by link Hello are link Hello adjacencies. LDP adjacencies discovered by targeted Hello are targeted Hello adjacencies.

1.4 LDP over RSVP

The SmartEdge® router supports the Label Distribution Protocol (LDP) over Resource Reservation Protocol (RSVP) for single-hop and multi-hop RSVP label-switched paths (LSPs). LDP over RSVP enables RSVP LSPs to carry LDP control and data traffic when Open Shortest Path First (OSPF) is configured as the Interior Gateway Protocol (IGP). LDP over RSVP is not supported when Intermediate System-to-Intermediate System (IS-IS) is the IGP. To enable LDP over RSVP, you must configure RSVP LSPs to be used as tunnel shortcuts and enable tunnel shortcuts on the OSPF routing instance and the LDP neighbors. If the RSVP LSP configured as a tunnel shortcut is also configured with next-hop fast reroute (NFRR) for link and node protection, or end-to-end backup(s), LDP traffic will also be protected. For more information, see *Configuring MPLS*

The following commands must be configured to enable LDP over RSVP:

* The `tunnel-shortcut` command in either RSVP router configuration mode or RSVP LSP configuration mode

* The `mpls tunnel-shortcut` command in OSPF router configuration mode

- The `tunnel-shortcut` command in LDP router configuration mode for all configured targeted neighbors or for a specific neighbor (`neighbor address targeted tunnel-shortcut`)

You can enable both IGP shortcuts and tunnel shortcuts on the same RSVP LSP.

Figure 1 shows an example in which an LDP LSP tunnels over an RSVP LSP from LSR A to LSR B and in the event of a link failure, the LDP LSP tunnels over a bypass RSVP to LSR B. Traffic then continues across the LDP LSP to LSR D.
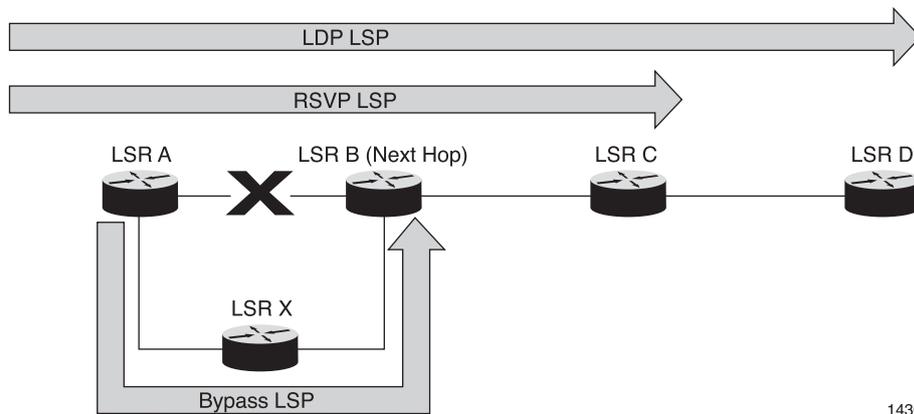
Figure 1   Link Failure Example

Figure 2 shows an example in which an LDP LSP tunnels over an RSVP LSP from LSR A to LSR C and in the event of a node failure, the LDP LSP tunnels over a bypass RSVP to LSR C. Traffic then continues across the LDP LSP to LSR E.
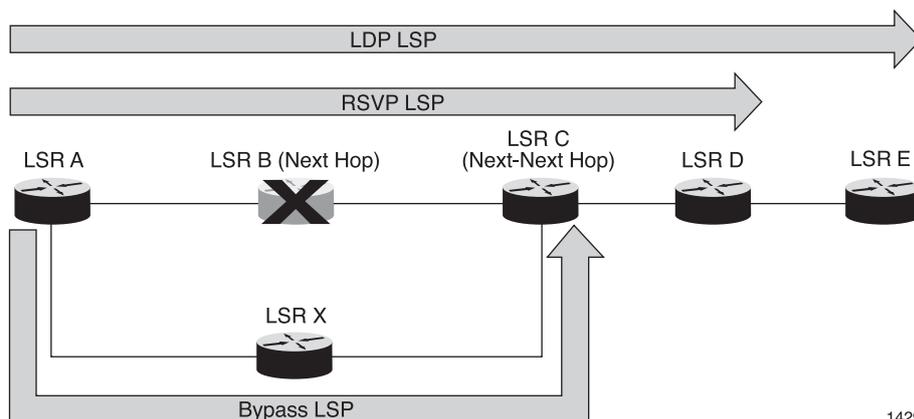
Figure 2   Node Failure Example

2 Configuration and Operations Tasks

> **Note:** In this section, the command syntax in the task tables displays only the root command.

To configure LDP, perform the tasks described in the sections that follow.

2.1 Creating the Minimum LDP Configuration

This section provides instructions on how to create the minimum LDP configuration.

To create the minimum LDP configuration:

1. Enable an LDP routing instance in the local context and access LDP router configuration mode by entering the *router ldp* command in context configuration mode.

2. Enable LDP on an interface so that it can be used to exchange Hello messages with neighbors and to establish an LSP by entering the *interface (LDP)* command in LDP router configuration mode.

In the local context, you must also:

- Configure an MPLS routing instance.

- Enable MPLS on the interface on which you enable LDP.

- Configure an Interior Gateway Protocol (IGP), such as OSPF or IS-IS. For LDP to be able to establish sessions, the LDP transport address of an LDP instance must be reachable. It is recommended that you configure a loopback interface whose address is advertised by the underlying IGP.

  > **Note:** To configure MPLS, see *Configuring MPLS*. To configure an IGP routing instance and interface, see either *Configuring IS-IS* or *Configuring OSPF*.

2.2 Specifying the LDP Router ID (Optional)

Configure the interface to be used as the LDP router ID by entering the *router-id (LDP)* command in LDP router configuration mode.

Because the router ID is used as the transport IP address for establishing a TCP connection, changing the router ID causes an active LDP session to be torn down, and then reestablished. Take care not to change the router ID when an LDP session is active.

By default, the SmartEdge router determines the LDP router ID in the following sequence:

1. If a fixed LDP router ID is configured through the router-id command in LDP configuration mode, it is used.

2. If neither router ID is configured, the configured loopback interface with the highest IP address is used as the LDP router ID.

3. If a loopback interface is not configured, the operational interface with the highest IP address is used as the LDP router ID.

Use the `no` form of this command to return the system to its default behavior.

2.3   Configuring Extended LDP Neighbor (Optional)

Configure a remote LDP neighbor and enable extended LDP discovery of the specified neighbor by entering the *neighbor targeted* command in LDP router configuration mode.

There are two types of LDP neighbor discovery mechanisms: basic LDP discovery and extended LDP discovery. Basic LDP discovery is used to discover immediate neighbors; extended LDP discovery is used to discover neighbors that can be multiple hops away. There are two types of LDP Hello messages: link Hello messages and targeted Hello messages. Link Hello messages are multicast on an interface to immediate neighbors. Link Hello messages are used in basic LDP discovery. Targeted Hello messages are unicast directly to remote neighbors, and are used in extended LDP discovery. Two LDP speaking label-switched routers (LSRs) can form LDP adjacencies after discovering each other. LDP adjacencies discovered by link Hello messages are link Hello adjacencies. LDP adjacencies discovered by targeted Hello messages are targeted Hello adjacencies. Use the neighbor targeted command to configure a remote LDP neighbor and enable extended LDP discovery of the specified neighbor. Targeted Hello messages can be transmitted or accepted to or from the specified neighbor. Use the no form of this command to remove a configured remote LDP neighbor, and to disable extended LDP discovery of the specified neighbor.

LDP targeted neighbor discovery is required for L2VPN support if the PE routers are not directly connected. Using the targeted discovery mechanism, the PE routers establish an LDP session using an extended discovery mechanism where they do not have to be directly connected (as is required in hop-by-hop neighbors). LDP is used to distribute L2VPN labels to the remote router.

LDP is used for distributing the VC labels across the path from the egress PE router to the ingress PE router. The VC label bindings are distributed using LDP downstream unsolicited mode. The PE routers establish an LDP session using an extended discovery mechanism where they do not have to be directly connected (as required in hop-by-hop neighbors). A new forwarding equivalence class (FEC) type element is used for targeted discovery. A single VC FEC element must be advertised per VC label.

For distributing L2VPN labels, targeted LDP implementation supports the following features:

- LDP downstream Unsolicited Mode

- LDP request operation implemented in LDP

- VC labels allocated from per platform label space

Use the `no` form of this command to remove a configured remote LDP neighbor, and to disable extended LDP discovery of the specified neighbor.

2.4 Enabling The Collection of LDP LSP Packet Statistics (Optional)

Before packet statistics for LDP LSPs can be collected, LDP LSP pseudo-circuits must first be created. Enable the creation of LDP LSP pseudo-circuits by entering the *create-lsp-circuit* command in LDP router configuration mode.

Use the `no` form of this command to disable the creation of pseudocircuits for LDP LSPs.

2.5 Enabling ECMP on LSP Transit Nodes (Optional)

Enable equal cost multipath (ECMP) on LSP transit nodes by entering the *ecmp-transit* command in LDP router configuration mode.

A constituent of an ECMP LSP can be protected against link failure at the label edge router (LER) using next-hop fast reroute (NFRR) for link protection when the LDP traffic is carried over a bypass RSVP LSP. Currently, ECMP over multiple bypass LSPs is not supported.

Use the `no` form of this command to disable ECMP on LSP transit nodes.

2.6 Configuring LDP Graceful Restart (Optional)

Enable an LSR to restart an LDP component while preserving its MPLS forwarding state during restart by entering the *graceful-restart (LDP)* command in LDP router configuration mode.

After an LSR restarts its control plane, it starts an internal recovery timer and continues to forward traffic using the preserved MPLS forwarding state entries. Before the recovery timer expires, the LSR creates local label bindings by following the normal LDP procedure. When the recovery timer expires, the MPLS forwarding entries that are not refreshed from the LDP peer are deleted and the refreshed ones are preserved without any disruption to the forwarding path.

Use the `no` form of this command to disable graceful restart.

2.7 Configuring the Maximum Number of LDP Sessions (Optional)

Enable the creation of pseudo-circuits for the LDP LSPs and configure the maximum number of LDP sessions allowed on the router by entering the *max-session* command in LDP router configuration mode.

Use the `no` form of this command to disable the creation of pseudo-circuits for the LDP LSPs.

Use the `default` form of this command to return the maximum number of LDP sessions to the default of 1200 sessions.

2.8 Filtering LDP Label Advertisements (Optional)

Apply an IP prefix list to filter LDP label advertisements by entering the *label-binding* command in LDP router configuration mode.

A typical filtering application is to apply a prefix list that restricts LDP to advertise labels for only loopback interface IP addresses. Limiting LDP label advertisements to loopback interfaces provides fast and reliable transportation of label binding information and streamlines the efforts to build LSPs.

Use the `no` form of this command to remove LDP label advertisement filtering.

2.9 Assigning an Encrypted MD5 Password to an LDP Neighbor (Optional)

Assign an encrypted MD5 password to an LDP neighbor by entering the *neighbor password* command in LDP router configuration mode.

For an LDP session to be established, the MD5 password must be the same on both the router and its neighbor.

Use the `no` form of this command to remove the password from an LDP neighbor.

2.10 Enabling LDP LSPs to Inherit IS-IS Routing Metric for BGP (Optional)

Enable LDP LSPs to inherit the Intermediate System-to-Intermediate System (IS-IS) routing metric for Border Gateway Protocol (BGP) to use when selecting a path by entering the *track-igp-metric*command in LDP router configuration mode.

Use the `no` or `default` form of this command to restore the default setting.

2.11 Enabling LDP IGP Synchronization with IS-IS or OSPF (Optional)

Set the maximum number of seconds LDP waits before notifying IS-IS or OSPF that label exchange is complete by entering the `igp-synchronization` command in LDP router configuration mode. You must also enable LDP-IGP synchronization for IS-IS or OSPF. Fore more information, see *Configuring IS-IS* or *Configuring OSPF*.

Use the `no` form of this command to remove the interval limitation.

2.12 Configuring the Transport Address Advertised in LDP Hello Messages (Optional)

Configure the transport address advertised in LDP Hello messages by entering the *transport address* command in LDP router configuration mode.

Transport addresses are advertised in LDP Hello messages and are exchanged among LDP neighbors. LDP uses the local transport address as the source, and the received transport address as the destination when trying to establish a TCP connection to a neighbor. Therefore, transport addresses must be reachable. LDP also uses transport addresses to determine which of the two LSRs should perform active open.

If a transport address is not explicitly configured, the LSR router ID is used as the transport address. In this case, the router ID must be reachable; however, if a transport address is explicitly configured, then the specified value is used. In this case, the router ID is not required to be reachable.

Use the `no` form of this command to remove the transport address.

2.13 Enabling LDP over RSVP (Optional)

To enable LDP over RSVP, complete the following tasks:

- Configure the `tunnel-shortcut` command in LDP router configuration mode for all targeted LDP neighbors or for a specific targeted LDP neighbor (`neighbor address targeted tunnel-shortcut`).

  Use the `no` form of this command to disable LDP over RSVP.

- Configure the `tunnel-shortcut` command in either RSVP router configuration mode for all RSVP LSPs or in RSVP LSP configuration mode for a specific RSVP LSP.

  Use the `no` form of this command to disable LDP over RSVP.

- Configure Open Shortest Path First (OSPF) as the Interior Gateway Protocol (IGP) and configure the `mpls tunnel-shortcut` command in OSPF router configuration mode. (LDP over RSVP is not supported when Intermediate System-to-Intermediate System (IS-IS) is the IGP.)

  Use the `no` form of this command to disable LDP over RSVP.

In order for LDP over RSVP to work, you must also:

- Configure the remote LDP neighbors and extended LDP discovery of the specified neighbors. Use the `neighbor targeted` command in LDP router configuration mode to configure LDP peers as targeted neighbors.

- Configure the IP address specified for the targeted LDP neighbor and for the RSVP LSP egress label-switched router (LSR) to be same address. These addresses must be loopback addresses (/32). Use the `egress` command in RSVP LSP configuration mode to specify the IP address of the egress LSR; for more information about the `egress` command, see *Configuring MPLS*.

Note: If the RSVP LSP configured as a tunnel shortcut is also configured with next-hop fast reroute (NFRR) for link and node protection, or end-to-end backup(s), LDP traffic will also be protected. For more information see *Configuring MPLS*.

2.14 Preserving QoS Settings with LDP Explicit Null (Optional)

Enable an egress router to advertise an explicit null label (value 0), in place of an implicit null label (value 3), to the penultimate hop router, by entering the *explicit-null (LDP)* in LPD router configuration mode.

By default, LDP advertises an implicit null label for directly connected prefixes. An implicit null label causes the upstream router to perform penultimate hop popping (PHP), and the implicit null label is not transmitted on the last hop. In some cases, such as QoS enforcement, you may not want PHP. In those cases, you can use the `explicit-null` command to cause a router to advertise an explicit null label in place of an implicit null label for directly connected prefixes, which forces the upstream router to transmit packets with an explicit null label on the last hop.

If a neighbor IP address is specified, the `explicit-null` command is neighbor-specific, and applies only to the LDP neighbor whose transport address matches the IP address specified in the command. If a neighbor address is not specified, the `explicit-null` command is non neighbor-specific, and applies to all LDP neighbors in the context. When both a neighbor-specific `explicit-null` command and a non neighbor-specific `explicit-null` command exist, only the neighbor-specific command applies to the neighbor whose transport address matches the IP address given in the neighbor-specific `explicit-null` command. Use the `no` form of this command to disable explicit null label advertisement.

Use the `no` form of this command to disable explicit null label advertisement.

2.15 Configuring the Hello Adjacency Holdtime (Optional)

2.15.1 Configure the Hello Adjacency Holdtime for Basic LDP Discovery

Configure the time for which an LDP link Hello adjacency is maintained in the absence of link Hello messages from the LDP neighbor by entering the *hello holdtime* command in LDP router configuration mode. The default link Hello adjacency holdtime is 15 seconds.

LDP neighbors periodically exchange Hello messages to maintain their adjacencies. The Hello holdtime determines the time after which, if LDP messages from the LDP neighbor are not received, the LDP hello adjacency is deleted. When the last LDP adjacency to a LDP neighbor is deleted, the LDP session to that LDP neighbor is torn down.

For LDP neighbors to negotiate a Hello holdtime, each LDP neighbor includes a proposed Hello holdtime in their transmitted Hello message. The negotiated Hello holdtime used between the two neighbors is the lesser of the two proposed values.

The locally configured link Hello holdtime as specified in `hello holdtime` command is included in the link Hello messages sent to immediate LDP neighbors. The negotiated holdtime used to timeout a link Hello adjacency is the lesser of the time value specified in the `hello holdtime` command and the hello holdtime received in link hello messages from the LDP neighbor of the adjacency.

Use the `default` form of this command to return to the default value of 15 seconds.

2.15.2 Configure the Hello Adjacency Holdtime for Extended LDP Discovery

Configure the time for which LDP targeted Hello adjacency is maintained in the absence of targeted Hello messages from an LDP neighbor by entering the *targeted-hello holdtime* command in LDP router configuration mode. The default LDP targeted Hello adjacency holdtime is 45 seconds

If LDP targeted Hello messages from an LDP neighbor are not received after the specified Hello holdtime, the LDP adjacency is deleted. If this is the last adjacency between the local LDP instance and an LDP neighbor, the LDP session to that LDP neighbor is torn down.

The locally configured targeted Hello holdtime as specified by the `targeted-hello holdtime` command is included in the targeted Hello messages sent to remote LDP neighbors. The negotiated holdtime used to

timeout a targeted Hello adjacency is the minimum of the time value specified by the `targeted-hello holdtime` command and the Hello holdtime received in targeted Hello messages from the LDP neighbor of the adjacency.

Use the `default` form of this command to return to the default value of 45 seconds.

2.16 Configuring the Hello Message Interval (Optional)

2.16.1 Configure the Hello Message Interval for Basic LDP Discovery

Configure the interval between consecutive LDP link Hello messages used in basic LDP discovery by entering the *hello interval (LDP)* command in LDP router configuration mode. The default LDP link Hello interval is five seconds.

If the Hello interval is explicitly configured, then the specified value is used to control the link Hello interval regardless of the link Hello holdtime; however, if the Hello interval is not explicitly configured, the Hello interval used is the negotiated LDP link Hello holdtime divided by three. The negotiated LDP link Hello holdtime is the lesser of the received LDP link Hello holdtime and the locally configured LDP link Hello holdtime.

Use the `no` form of this command to restore the default Hello packet interval.

2.16.2 Configure the Hello Message Interval for Extended LDP Discovery

Configure the interval between consecutive LDP targeted Hello messages used in extended LDP discovery by entering the *targeted-hello interval* command in LDP router configuration mode. The default LDP targeted Hello interval is 15 seconds.

If the targeted Hello interval is explicitly configured, then the specified value is used to control targeted Hello interval regardless of the targeted Hello holdtime; however, if the targeted Hello interval is not explicitly configured, the targeted Hello interval used is the negotiated LDP targeted Hello holdtime divided by three. The negotiated LDP targeted Hello holdtime is the lesser of the received LDP targeted Hello holdtime and the locally configured LDP targeted Hello holdtime.

Use the `no` form of this command to use the negotiated LDP targeted Hello holdtime divided by three as the targeted-hello interval.

Use the `default` form of this command to return to the default value of 15 seconds.

2.17 Configure LDP Liveliness Detection and Keepalive Packet Transmission (Optional)

Enable the configuration of intervals controlling LDP liveliness detection and LDP keepalive packet transmission for a SmartEdge® router Label Switched Router (LSR).

The **holdtime** option sets the number of seconds after which an inactive LDP session will be terminated and the corresponding TCP session will be closed. The interval option sets the number of seconds between successive transmission of keepalive packets.

Use the **no** or **default** form of this command to return to the default holdtime of 90 seconds or to return to the default interval of 30 seconds.

2.18 Ignore the Changed in the Configuration Sequence Number Specified in an LDP Neighbor's Hello Packet (Optional)

Use the **ignore config-seq-num** command to ignore the change in the Configuration Sequence Number specified in an LDP neighbor's hello packets. Normally, a SmartEdge® router will terminate the LDP session when a change in Configuration Sequence Number is detected.

Use the **no** form of this command to acknowledge the change in the Configuration Sequence Number specified in an LDP neighbor's hello packets.

2.19 LDP Operations

To manage LDP functions, perform the appropriate tasks described in Table 1. Enter the **show** commands in any mode; enter the **debug** commands in exec mode.

Table 1   LDP Operations Tasks

Task	Root Command
Enable the generation of debug messages for all LDP events.	*debug ldp all*
Limit the generation of LDP debug messages to specific interfaces, neighbor IP addresses, or IP prefixes.	*debug ldp filter*
Enable the generation of debug messages for LDP messages.	*debug ldp message*
Enable the generation of debug messages for LDP protocol interaction.	*debug ldp protocol*
Display the LDP commands that are configured in the current context.	*show configuration ldp*

Table 1   LDP Operations Tasks

Task	Root Command
Display LDP interface IP address to label-switched router (LSR) ID mappings.	*show ldp address*
Display LDP label binding information.	*show ldp binding*
Display any filters that may be currently enabled to control the generation of LDP debug messages.	*show ldp debug-filter*
Display LDP interface information.	*show ldp interface*
Display LDP neighbor information.	*show ldp neighbor*
Display a summary of LDP information.	*show ldp summary*

3   Configuration Examples

The following sections provide examples of LDP configuration.

3.1   Basic LDP

The following example configures an IS-IS backbone network between two SmartEdge routers. Each has an IS-IS, MPLS, and LDP routing instance and a single interface (the backbone between the two routers) enabled for IS-IS, MPLS, and LDP. Each router has an IS-IS loopback interface that is used as the LDP router ID. A filter restricts LDP to advertise labels for only loopback interface IP addresses.

The configuration for **LSR-A** is as follows:

```
[local]LSR-A(config)#context local

[local]LSR-A(config-ctx)#router isis isis-backbone

[local]LSR-A(config-isis)#net 49.2222.0010.0100.1001.00

[local]LSR-A(config-isis)#exit

[local]LSR-A(config-ctx)#ip prefix-list loop-only

[local]LSR-A(config-prefix-list)#permit 0.0.0.0/0 eq 32

[local]LSR-A(config-prefix-list)#exit

[local]LSR-A(config-ctx)#interface backbone1

[local]LSR-A(config-if)#ip address 10.1.1.1/24

[local]LSR-A(config-if)#isis router isis-backbone

[local]LSR-A(config-if)#exit

[local]LSR-A(config-ctx)#interface loop1 loopback

[local]LSR-A(config-if)#ip address 1.1.1.1/32

[local]LSR-A(config-if)#isis router isis-backbone

[local]LSR-A(config-if)#isis passive-interface

[local]LSR-A(config-if)#exit
```

```
[local]LSR-A(config-ctx)#router mpls 1

[local]LSR-A(config-mpls)#interface backbone1

[local]LSR-A(config-mpls-interface)#exit

[local]LSR-A(config-mpls)#exit

[local]LSR-A(config-ctx)#exit

[local]LSR-A(config)#port pos 6/1

[local]LSR-A(config-port)#bind interface backbone1 local

[local]LSR-A(config-port)#no shutdown

[local]LSR-A(config-port)#exit

[local]LSR-A(config)#context local

[local]LSR-A(config-ctx)#router ldp

[local]LSR-A(config-ldp)#interface backbone1
```

The configuration for **LSR-B** is as follows:

```
[local]LSR-B(config)#context local

[local]LSR-B(config-ctx)#router isis isis-backbone

[local]LSR-B(config-isis)#net 49.2222.0010.0100.1001.00

[local]LSR-B(config-isis)#exit

[local]LSR-B(config-ctx)#ip prefix-list loop-only

[local]LSR-B(config-prefix-list)#permit 0.0.0.0/0 eq 32

[local]LSR-B(config-prefix-list)#exit

[local]LSR-B(config-ctx)#interface backbone1

[local]LSR-B(config-if)#ip address 10.2.2.2/24

[local]LSR-B(config-if)#isis router isis-backbone

[local]LSR-B(config-if)#exit
```

```
[local]LSR-B(config-ctx)#interface loop1 loopback

[local]LSR-B(config-if)#ip address 1.1.1.1/32

[local]LSR-B(config-if)#isis router isis-backbone

[local]LSR-B(config-if)#exit

[local]LSR-B(config-ctx)#router mpls 1

[local]LSR-B(config-mpls)#interface backbone1

[local]LSR-B(config-mpls-interface)#exit

[local]LSR-B(config-mpls)#exit

[local]LSR-B(config-ctx)#exit

[local]LSR-B(config)#port pos 6/1

[local]LSR-B(config-port)#bind interface backbone1 local

[local]LSR-B(config-port)#no shutdown

[local]LSR-B(config-port)#exit

[local]LSR-B(config)#context local

[local]LSR-B(config-ctx)#router ldp

[local]LSR-B(config-ldp)#interface backbone1

[local]LSR-B(config-ldp)#label-binding prefix-list loop-only out
```

3.2   Targeted LDP

The following example configures two PE routers (**PE1** and **PE2**) for targeted LDP discovery. The two routers are connected over an IGP in an MPLS network, so their router IDs are known to each other through IGP. Figure 3 shows the network topology for this example.
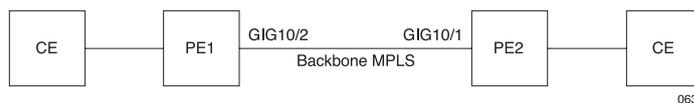

Figure 3   Targeted LDP Network Topology

The LDP router ID address is also used as the LDP transport address for establishing the LDP targeted neighbor. The `router-id` command is used in LDP router configuration mode to configure the LDP router ID on the router. If the `router- id` command is removed from the configuration example, the LDP router ID is picked up as follows:

- If one or more loopback addresses are present, the highest loopback address is used as the neighbor, and the router ID address is used as transport address.

- If no loopback addresses are present, the highest interface address is used as the LDP router ID.

The configuration for the **PE1** router is as follows:

```
[local]PE1(config)#context local

[local]PE1(config-ctx)#interface loop1 loopback

[local]PE1(config-if)#ip address 11.200.1.1/32

[local]PE1(config-if)#exit

[local]PE1(config-ctx)#router ldp

[local]PE1(config-ldp)#router-id 11.200.1.1

[local]PE1(config-ldp)#neighbor 11.200.1.2 targeted

[local]PE1(config-ldp)#end
```

The configuration for the **PE2** router is as follows:

```
[local]PE2(config)#context local

[local]PE2(config-ctx)#interface loop1 loopback

[local]PE2(config-if)#ip address 11.200.1.2

[local]PE2(config-if)#exit

[local]PE2(config-ctx)#router ldp

[local]PE2(config-ldp)#router-id 11.200.1.2

[local]PE2(config-ldp)#neighbor 11.200.1.1 targeted

[local]PE2(config-ldp)#end
```

3.3 LDP over RSVP

The following example configures two LSRs to tunnel LDP traffic over RSVP LSPs. LDP uses the two RSVP LSPs, **lsp-lsrA-to-lsrB** and **lsp-lsrB-to-lsrA**, to carry traffic between LSR A and LSR B. If a link fails, LDP traffic switches to the bypass LSPs, **bypass-lsp-lsrA-to-lsrB** and **bypass-lsp-lsrB-to-lsrA**, to carry traffic between LSR A and LSR B. LDP traffic is carried between LSR B and LSR C using the standard LDP configuration. Figure 4 shows the network topology for this example.
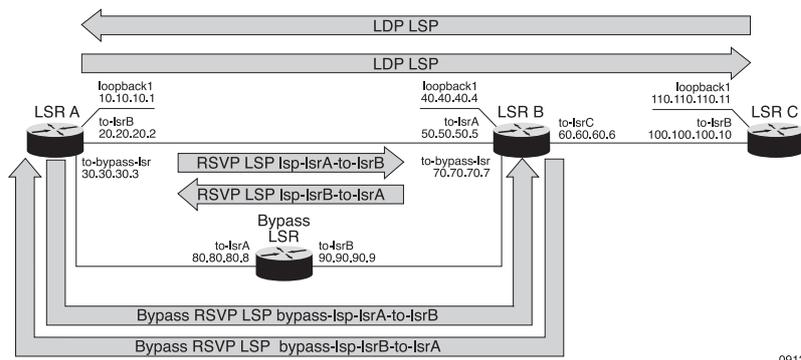
Figure 4   Typical LDP over RSVP Network Topology

The configuration for LSR A is as follows:

```
[local]LSR-A#config

[local]LSR-A(config)#context local

[local]LSR-A(config-ctx)#no ip domain-lookup

[local]LSR-A(config-ctx)#interface loopback1 loopback

[local]LSR-A(config-if)#ip address 10.10.10.1

[local]LSR-A(config-if)#exit

[local]LSR-A(config-ctx)#interface to-lsrB

[local]LSR-A(config-if)#ip address 20.20.20.2

[local]LSR-A(config-if)#exit

[local]LSR-A(config-ctx)#interface to-bypass-lsr

[local]LSR-A(config-if)#ip address 30.30.30.3

[local]LSR-A(config-if)#exit

[local]LSR-A(config-ctx)#router ospf 1
```

```
[local]LSR-A(config-ospf)#mpls tunnel-shortcut

[local]LSR-A(config-ospf)#area 0.0.0.0

[local]LSR-A(config-ospf-area)#interface to-lsrB

[local]LSR-A(config-ospf-if)#exit

[local]LSR-A(config-ospf-area)#interface loopback1

[local]LSR-A(config-ospf-if)#exit

[local]LSR-A(config-ospf-area)#interface to-bypass-lsr

[local]LSR-A(config-ospf-if)#exit

[local]LSR-A(config-ospf)#exit

[local]LSR-A(config-ctx)#router mpls

[local]LSR-A(config-mpls)#interface to-lsrB

[local]LSR-A(config-mpls-if)#exit

[local]LSR-A(config-mpls)#interface loopback1

[local]LSR-A(config-mpls-if)#exit

[local]LSR-A(config-mpls)#interface to-bypass-lsr

[local]LSR-A(config-mpls-if)#exit

[local]LSR-A(config-mpls)#exit

[local]LSR-A(config-ctx)#router rsvp

[local]LSR-A(config-rsvp)#tunnel-shortcut

[local]LSR-A(config-rsvp)#interface to-lsrB

[local]LSR-A(config-rsvp-if)#exit

[local]LSR-A(config-rsvp)#interface loopback1

[local]LSR-A(config-rsvp-if)#exit

[local]LSR-A(config-rsvp)#interface to-bypass-lsr

[local]LSR-A(config-rsvp-if)#exit
```

```
[local]LSR-A(config-rsvp)#explicit-route to-lsrB

[local]LSR-A(config-rsvp-explicit-route)#next-hop 50.50.50.5

[local]LSR-A(config-rsvp-explicit-route)#exit

[local]LSR-A(config-rsvp)#lsp lsrA-to-lsrB

[local]LSR-A(config-rsvp-lsp)#ingress 10.10.10.1

[local]LSR-A(config-rsvp-lsp)#egress 40.40.40.4

[local]LSR-A(config-rsvp-lsp)#local-protection

[local]LSR-A(config-rsvp-lsp)#exit

[local]LSR-A(config-rsvp)#explicit-route to-lsrB-2

[local]LSR-A(config-rsvp-explicit-route)#next-hop 80.80.80.8

[local]LSR-A(config-rsvp-explicit-route)#next-hop 70.70.70.7

[local]LSR-A(config-rsvp-explicit-route)#exit

[local]LSR-A(config-rsvp)#lsp bypass-lsp-lsrA-to-lsrB bypass 50.50.50.5

[local]LSR-A(config-rsvp-lsp)#egress 40.40.40.4

[local]LSR-A(config-rsvp-lsp)#exit

[local]LSR-A(config-rsvp)#exit

[local]LSR-A(config-ctx)#router ldp

[local]LSR-A(config-ldp)#interface to-lsrB

[local]LSR-A(config-ldp)#interface loopback1

[local]LSR-A(config-ldp)#neighbor 40.40.40.4 targeted tunnel-shortcut

[local]LSR-A(config-ldp)#neighbor 110.110.110.11 targeted tunnel-shortcut
```

The configuration for **LSR-B** is as follows:

```
[local]LSR-B#config

[local]LSR-B(config)#context local

[local]LSR-B(config-ctx)#no ip domain-lookup
```

```
[local]LSR-B(config-ctx)#interface loopback1 loopback

[local]LSR-B(config-if)#ip address 40.40.40.4

[local]LSR-B(config-if)#exit

[local]LSR-B(config-ctx)#interface to-lsrA

[local]LSR-B(config-if)#ip address 50.50.50.5

[local]LSR-B(config-if)#exit

[local]LSR-B(config-ctx)#interface to-lsrC

[local]LSR-B(config-if)#ip address 60.60.60.6

[local]LSR-B(config-if)#exit

[local]LSR-B(config-ctx)#interface to-bypass-lsr

[local]LSR-B(config-if)#ip address 70.70.70.7

[local]LSR-B(config-if)#exit

[local]LSR-B(config-ctx)#router ospf 1

[local]LSR-A(config-ospf)#mpls tunnel-shortcut

[local]LSR-B(config-ospf)#area 0.0.0.0

[local]LSR-B(config-ospf-area)#interface to-lsrA

[local]LSR-B(config-ospf-if)#exit

[local]LSR-B(config-ospf-area)#interface to-lsrC

[local]LSR-B(config-ospf-if)#exit

[local]LSR-B(config-ospf-area)#interface loopback1

[local]LSR-B(config-ospf-if)#exit

[local]LSR-B(config-ospf-area)#interface to-bypass-lsr

[local]LSR-B(config-ospf-if)#exit

[local]LSR-B(config-ospf-area)#exit

[local]LSR-B(config-ospf)#exit
```

```
[local]LSR-B(config-ctx)#router mpls

[local]LSR-B(config-mpls)#interface to-lsrA

[local]LSR-B(config-mpls-if)#exit

[local]LSR-B(config-mpls)#interface to-lsrC

[local]LSR-B(config-mpls-if)#exit

[local]LSR-B(config-mpls)#interface loopback1

[local]LSR-B(config-mpls-if)#exit

[local]LSR-B(config-mpls)#interface to-bypass-lsr

[local]LSR-B(config-mpls-if)#exit

[local]LSR-B(config-mpls)#exit

[local]LSR-B(config-ctx)#router rsvp

[local]LSR-B(config-rsvp)#tunnel-shortcut

[local]LSR-B(config-rsvp)#interface to-lsrA

[local]LSR-B(config-rsvp-if)#exit

[local]LSR-B(config-rsvp)#interface to-lsrC

[local]LSR-B(config-rsvp-if)#exit

[local]LSR-B(config-rsvp)#interface loopback1

[local]LSR-B(config-rsvp-if)#exit

[local]LSR-B(config-rsvp)#interface to-bypass-lsr

[local]LSR-B(config-rsvp-if)#exit

[local]LSR-B(config-rsvp)#explicit-route to-lsrA

[local]LSR-B(config-rsvp-explicit-route)#next-hop 20.20.20.2

[local]LSR-B(config-rsvp-explicit-route)#exit

[local]LSR-B(config-rsvp)#lsp lsp-lsrB-to-lsrA

[local]LSR-B(config-rsvp-lsp)#ingress 40.40.40.4

[local]LSR-B(config-rsvp-lsp)#egress 10.10.10.1
```

```
[local]LSR-B(config-rsvp-lsp)#local-protection

[local]LSR-B(config-rsvp-lsp)#exit

[local]LSR-B(config-rsvp)#explicit-route to-lsrA-2

[local]LSR-B(config-rsvp-explicit-route)#next-hop 90.90.90.9

[local]LSR-B(config-rsvp-explicit-route)#next-hop 30.30.30.3

[local]LSR-B(config-rsvp-explicit-route)#exit

[local]LSR-B(config-rsvp)#lsp bypass-lsrB-to-lsrA bypass 20.20.20.2

[local]LSR-B(config-rsvp-lsp)#egress 40.40.40.4

[local]LSR-B(config-rsvp-lsp)#exit

[local]LSR-B(config-rsvp)#exit

[local]LSR-B(config-ctx)#router ldp

[local]LSR-B(config-ldp)#interface to-lsrA

[local]LSR-B(config-ldp)#interface to-lsrC

[local]LSR-B(config-ldp)#interface loopback1

[local]LSR-B(config-ldp)#interface to-bypass-lsr

[local]LSR-B(config-ldp)#neighbor 10.10.10.1 targeted tunnel-shortcut

[local]LSR-B(config-ldp)#neighbor 110.110.110.11 targeted tunnel-shortcut

[local]LSR-B(config-ldp)#end
```