Implementing MPLS Label Distribution Protocol

The Multiprotocol Label Switching (MPLS) is a standards-based solution driven by the Internet Engineering Task Force (IETF) that was devised to convert the Internet and IP backbones from best-effort networks into business-class transport mediums.

MPLS, with its label switching capabilities, eliminates the need for an IP route look-up and creates a virtual circuit (VC) switching function, allowing enterprises the same performance on their IP-based network services as with those delivered over traditional networks such as Frame Relay or ATM.

Label Distribution Protocol (LDP) performs label distribution in MPLS environments. LDP provides the following capabilities:

- LDP performs hop-by-hop or dynamic path setup; it does not provide end-to-end switching services.
- LDP assigns labels to routes using the underlying Interior Gateway Protocols (IGP) routing protocols.
- LDP provides constraint-based routing using LDP extensions for traffic engineering.

Finally, LDP is deployed in the core of the network and is one of the key protocols used in MPLS-based Layer 2 and Layer 3 virtual private networks (VPNs).

**Feature History for Implementing MPLS LDP**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release 4.0.1</td>
<td>Support was added for these features:</td>
</tr>
<tr>
<td></td>
<td>• IP LDP Fast Reroute Loop Free Alternate</td>
</tr>
<tr>
<td></td>
<td>• Downstream on Demand</td>
</tr>
<tr>
<td>Release 4.2.1</td>
<td>Support was added for LDP Implicit Null for IGP Routes.</td>
</tr>
<tr>
<td>Release 5.1.1</td>
<td>The feature MPLS LDP Carrier Supporting Carrier for Multiple VRFs was introduced.</td>
</tr>
<tr>
<td>Release 5.3.0</td>
<td>IPv6 Support in MPLS LDP was introduced.</td>
</tr>
</tbody>
</table>
Prerequisites for Implementing Cisco MPLS LDP

These prerequisites are required to implement MPLS LDP:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- You must be running Cisco IOS XR software.
- You must install a composite mini-image and the MPLS package.
- You must activate IGP.
- We recommend to use a lower session holdtime bandwidth such as neighbors so that a session down occurs before an adjacency-down on a neighbor. Therefore, the following default values for the hello times are listed:
  - Holdtime is 15 seconds.
  - Interval is 5 seconds.

For example, the LDP session holdtime can be configured as 30 seconds by using the `holdtime` command.

Information About Implementing Cisco MPLS LDP

To implement MPLS LDP, you should understand these concepts:

Overview of Label Distribution Protocol

LDP performs label distribution in MPLS environments. LDP uses hop-by-hop or dynamic path setup, but does not provide end-to-end switching services. Labels are assigned to routes that are chosen by the underlying IGP routing protocols. The Label Switched Paths (LSPs) that result from the routes, forward labeled traffic across the MPLS backbone to adjacent nodes.

Label Switched Paths

LSPs are created in the network through MPLS. They can be created statically, by RSVP traffic engineering (TE), or by LDP. LSPs created by LDP perform hop-by-hop path setup instead of an end-to-end path.
LDP Control Plane

The control plane enables label switched routers (LSRs) to discover their potential peer routers and to establish LDP sessions with those peers to exchange label binding information.

Related Topics
- Configuring LDP Discovery Parameters, on page 16
- Configuring LDP Discovery Over a Link, on page 17
- Configuring LDP Link: Example, on page 45
- Configuring LDP Discovery for Active Targeted Hellos, on page 19
- Configuring LDP Discovery for Passive Targeted Hellos, on page 21
- Configuring LDP Discovery for Targeted Hellos: Example, on page 45

Exchanging Label Bindings

LDP creates LSPs to perform the hop-by-hop path setup so that MPLS packets can be transferred between the nodes on the MPLS network.

This figure illustrates the process of label binding exchange for setting up LSPs.

**Figure 1: Setting Up Label Switched Paths**

For a given network (10.0.0.0), hop-by-hop LSPs are set up between each of the adjacent routers (or, nodes) and each node allocates a local label and passes it to its neighbor as a binding:

1. R4 allocates local label L4 for prefix 10.0.0.0 and advertises it to its neighbors (R3).
2. R3 allocates local label L3 for prefix 10.0.0.0 and advertises it to its neighbors (R1, R2, R4).
3. R1 allocates local label L1 for prefix 10.0.0.0 and advertises it to its neighbors (R2, R3).
4. R2 allocates local label L2 for prefix 10.0.0.0 and advertises it to its neighbors (R1, R3).
5 R1’s label information base (LIB) keeps local and remote labels bindings from its neighbors.
6 R2’s LIB keeps local and remote labels bindings from its neighbors.
7 R3’s LIB keeps local and remote labels bindings from its neighbors.
8 R4’s LIB keeps local and remote labels bindings from its neighbors.

Related Topics
- Setting Up LDP Neighbors, on page 25
- Configuring LDP Neighbors: Example, on page 46

LDP Forwarding

Once label bindings are learned, the LDP control plane is ready to setup the MPLS forwarding plane as shown in the following figure.

Once label bindings are learned, the LDP control plane is ready to setup the MPLS forwarding plane as shown in this figure.

**Figure 2: Forwarding Setup**

1 Because R3 is next hop for 10.0.0.0 as notified by the FIB, R1 selects label binding from R3 and installs forwarding entry (Layer 1, Layer 3).
2 Because R3 is next hop for 10.0.0.0 (as notified by FIB), R2 selects label binding from R3 and installs forwarding entry (Layer 2, Layer 3).
3 Because R4 is next hop for 10.0.0.0 (as notified by FIB), R3 selects label binding from R4 and installs forwarding entry (Layer 3, Layer 4).
4 Because next hop for 10.0.0.0 (as notified by FIB) is beyond R4, R4 uses NO-LABEL as the outbound and installs the forwarding entry (Layer 4); the outbound packet is forwarded IP-only.
5 Incoming IP traffic on ingress LSR R1 gets label-imposed and is forwarded as an MPLS packet with label L3.
6  Incoming IP traffic on ingress LSR R2 gets label-imposed and is forwarded as an MPLS packet with label L3.

7  R3 receives an MPLS packet with label L3, looks up in the MPLS label forwarding table and switches this packet as an MPLS packet with label L4.

8  R4 receives an MPLS packet with label L4, looks up in the MPLS label forwarding table and finds that it should be Unlabeled, pops the top label, and passes it to the IP forwarding plane.

9  IP forwarding takes over and forwards the packet onward.

Related Topics

- Setting Up LDP Forwarding, on page 27
- Configuring LDP Forwarding: Example, on page 47

LDP Graceful Restart

LDP (Label Distribution Protocol) graceful restart provides a control plane mechanism to ensure high availability and allows detection and recovery from failure conditions while preserving Nonstop Forwarding (NSF) services. Graceful restart is a way to recover from signaling and control plane failures without impacting forwarding.

Without LDP graceful restart, when an established session fails, the corresponding forwarding states are cleaned immediately from the restarting and peer nodes. In this case LDP forwarding restarts from the beginning, causing a potential loss of data and connectivity.

The LDP graceful restart capability is negotiated between two peers during session initialization time, in FT SESSION TLV. In this typed length value (TLV), each peer advertises the following information to its peers:

- **Reconnect time**
  
  Advertises the maximum time that other peer will wait for this LSR to reconnect after control channel failure.

- **Recovery time**
  
  Advertises the maximum time that the other peer has on its side to reinstate or refresh its states with this LSR. This time is used only during session reestablishment after earlier session failure.

- **FT flag**
  
  Specifies whether a restart could restore the preserved (local) node state for this flag.

Once the graceful restart session parameters are conveyed and the session is up and running, graceful restart procedures are activated.

When configuring the LDP graceful restart process in a network with multiple links, targeted LDP hello adjacencies with the same neighbor, or both, make sure that graceful restart is activated on the session before any hello adjacency times out in case of neighbor control plane failures. One way of achieving this is by configuring a lower session hold time between neighbors such that session timeout occurs before hello adjacency timeout. It is recommended to set LDP session hold time using the following formula:

\[
\text{Session Holdtime} \leq (\text{Hello holdtime} - \text{Hello interval}) \times 3
\]
This means that for default values of 15 seconds and 5 seconds for link Hello holdtime and interval respectively, session hold time should be set to 30 seconds at most.

For more information about LDP commands, see *MPLS Label Distribution Protocol Commands* module of the *Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference*.

**Related Topics**
- Setting Up LDP NSF Using Graceful Restart, on page 28
- Configuring LDP Nonstop Forwarding with Graceful Restart: Example, on page 47

**Control Plane Failure**

When a control plane failure occurs, connectivity can be affected. The forwarding states installed by the router control planes are lost, and the in-transit packets could be dropped, thus breaking NSF.

This figure illustrates a control plane failure and shows the process and results of a control plane failure leading to loss of connectivity.

**Figure 3: Control Plane Failure**

1. The R4 LSR control plane restarts.
2. LIB is lost when the control plane restarts.
3. The forwarding states installed by the R4 LDP control plane are immediately deleted.
4. Any in-transit packets flowing from R3 to R4 (still labeled with L4) arrive at R4.
5. The MPLS forwarding plane at R4 performs a lookup on local label L4 which fails. Because of this failure, the packet is dropped and NSF is not met.
6. The R3 LDP peer detects the failure of the control plane channel and deletes its label bindings from R4.
7 The R3 control plane stops using outgoing labels from R4 and deletes the corresponding forwarding state (rewrites), which in turn causes forwarding disruption.

8 The established LSPs connected to R4 are terminated at R3, resulting in broken end-to-end LSPs from R1 to R4.

9 The established LSPs connected to R4 are terminated at R3, resulting in broken LSPs end-to-end from R2 to R4.

Phases in Graceful Restart

The graceful restart mechanism is divided into different phases:

Control communication failure detection

Control communication failure is detected when the system detects either:

- Missed LDP hello discovery messages
- Missed LDP keepalive protocol messages
- Detection of Transmission Control Protocol (TCP) disconnection a with a peer

Forwarding state maintenance during failure

Persistent forwarding states at each LSR are achieved through persistent storage (checkpoint) by the LDP control plane. While the control plane is in the process of recovering, the forwarding plane keeps the forwarding states, but marks them as stale. Similarly, the peer control plane also keeps (and marks as stale) the installed forwarding rewrites associated with the node that is restarting. The combination of local node forwarding and remote node forwarding plane states ensures NSF and no disruption in the traffic.

Control state recovery

Recovery occurs when the session is reestablished and label bindings are exchanged again. This process allows the peer nodes to synchronize and to refresh stale forwarding states.

Related Topics

- Setting Up LDP NSF Using Graceful Restart, on page 28
- Configuring LDP Nonstop Forwarding with Graceful Restart: Example, on page 47
Recovery with Graceful-Restart

This figure illustrates the process of failure recovery using graceful restart.

Figure 4: Recovering with Graceful Restart

1. The router R4 LSR control plane restarts.
2. With the control plane restart, LIB is gone but forwarding states installed by R4’s LDP control plane are not immediately deleted but are marked as stale.
3. Any in-transit packets from R3 to R4 (still labeled with L4) arrive at R4.
4. The MPLS forwarding plane at R4 performs a successful lookup for the local label L4 as forwarding is still intact. The packet is forwarded accordingly.
5. The router R3 LDP peer detects the failure of the control plane and channel and deletes the label bindings from R4. The peer, however, does not delete the corresponding forwarding states but marks them as stale.
6. At this point there are no forwarding disruptions.
7. The peer also starts the neighbor reconnect timer using the reconnect time value.
8. The established LSPs going toward the router R4 are still intact, and there are no broken LSPs.

When the LDP control plane recovers, the restarting LSR starts its forwarding state hold timer and restores its forwarding state from the checkpointed data. This action reinstates the forwarding state and entries and marks them as old.

The restarting LSR reconnects to its peer, indicated in the FT Session TLV, that it either was or was not able to restore its state successfully. If it was able to restore the state, the bindings are resynchronized.

The peer LSR stops the neighbor reconnect timer (started by the restarting LSR), when the restarting peer connects and starts the neighbor recovery timer. The peer LSR checks the FT Session TLV if the restarting
peer was able to restore its state successfully. It reinstates the corresponding forwarding state entries and receives binding from the restarting peer. When the recovery timer expires, any forwarding state that is still marked as stale is deleted.

If the restarting LSR fails to recover (restart), the restarting LSR forwarding state and entries will eventually timeout and is deleted, while neighbor-related forwarding states or entries are removed by the Peer LSR on expiration of the reconnect or recovery timers.

**Related Topics**
- Setting Up LDP NSF Using Graceful Restart, on page 28
- Configuring LDP Nonstop Forwarding with Graceful Restart: Example, on page 47

**Label Advertisement Control (Outbound Filtering)**

By default, LDP advertises labels for all the prefixes to all its neighbors. When this is not desirable (for scalability and security reasons), you can configure LDP to perform outbound filtering for local label advertisement for one or more prefixes to one more peers. This feature is known as LDP outbound label filtering, or local label advertisement control.

**Related Topics**
- Configuring Label Advertisement Control (Outbound Filtering), on page 24
- Configuring Label Advertisement (Outbound Filtering): Example, on page 46

**Label Acceptance Control (Inbound Filtering)**

By default, LDP accepts labels (as remote bindings) for all prefixes from all peers. LDP operates in liberal label retention mode, which instructs LDP to keep remote bindings from all peers for a given prefix. For security reasons, or to conserve memory, you can override this behavior by configuring label binding acceptance for set of prefixes from a given peer.

The ability to filter remote bindings for a defined set of prefixes is also referred to as LDP inbound label filtering.

**Note**

Inbound filtering can also be implemented using an outbound filtering policy; however, you may not be able to implement this system if an LDP peer resides under a different administration domain. When both inbound and outbound filtering options are available, we recommend that you use outbound label filtering.

**Related Topics**
- Configuring Label Acceptance Control (Inbound Filtering), on page 31
- Configuring Label Acceptance (Inbound Filtering): Example, on page 47
Local Label Allocation Control

By default, LDP allocates local labels for all prefixes that are not Border Gateway Protocol (BGP) prefixes. This is acceptable when LDP is used for applications other than Layer 3 virtual private networks (L3VPN) core transport. When LDP is used to set up transport LSPs for L3VPN traffic in the core, it is not efficient or even necessary to allocate and advertise local labels for, potentially, thousands of IGP prefixes. In such a case, LDP is typically required to allocate and advertise local label for loopback /32 addresses for PE routers. This is accomplished using LDP local label allocation control, where an access list can be used to limit allocation of local labels to a set of prefixes. Limiting local label allocation provides several benefits, including reduced memory usage requirements, fewer local forwarding updates, and fewer network and peer updates.

You can configure label allocation using an IP access list to specify a set of prefixes that local labels can allocate and advertise.

Related Topics

- Configuring Local Label Allocation Control, on page 32
- Configuring Local Label Allocation Control: Example, on page 48

Session Protection

When a link comes up, IP converges earlier and much faster than MPLS LDP and may result in MPLS traffic loss until MPLS convergence. If a link flaps, the LDP session will also flap due to loss of link discovery. LDP session protection minimizes traffic loss, provides faster convergence, and protects existing LDP (link) sessions by means of “parallel” source of targeted discovery hello. An LDP session is kept alive and neighbor label bindings are maintained when links are down. Upon reestablishment of primary link adjacencies, MPLS convergence is expedited as LDP need not relearn the neighbor label bindings.

LDP session protection lets you configure LDP to automatically protect sessions with all or a given set of peers (as specified by peer-acl). When configured, LDP initiates backup targeted hellos automatically for neighbors for which primary link adjacencies already exist. These backup targeted hellos maintain LDP sessions when primary link adjacencies go down.

The Session Protection figure illustrates LDP session protection between neighbors R1 and R3. The primary link adjacency between R1 and R3 is directly connected link and the backup; targeted adjacency is maintained between R1 and R3. If the direct link fails, LDP link adjacency is destroyed, but the session is kept up and

---

1 For L3VPN Inter-AS option C, LDP may also be required to assign local labels for some BGP prefixes.
running using targeted hello adjacency (through R2). When the direct link comes back up, there is no change in the LDP session state and LDP can converge quickly and begin forwarding MPLS traffic.

Figure 5: Session Protection

Note

When LDP session protection is activated (upon link failure), protection is maintained for an unlimited period time.

Related Topics

Configuring Session Protection, on page 33
Configuring LDP Session Protection: Example, on page 48

IGP Synchronization

Lack of synchronization between LDP and IGP can cause MPLS traffic loss. Upon link up, for example, IGP can advertise and use a link before LDP convergence has occurred; or, a link may continue to be used in IGP after an LDP session goes down.

LDP IGP synchronization synchronizes LDP and IGP so that IGP advertises links with regular metrics only when MPLS LDP is converged on that link. LDP considers a link converged when at least one LDP session is up and running on the link for which LDP has sent its applicable label bindings and received at least one label binding from the peer. LDP communicates this information to IGP upon link up or session down events and IGP acts accordingly, depending on sync state.

In the event of an LDP graceful restart session disconnect, a session is treated as converged as long as the graceful restart neighbor is timed out. Additionally, upon local LDP restart, a checkpointed recovered LDP graceful restart session is used and treated as converged and is given an opportunity to connect and resynchronize.

Under certain circumstances, it might be required to delay declaration of resynchronization to a configurable interval. LDP provides a configuration option to delay declaring synchronization up for up to 60 seconds. LDP communicates this information to IGP upon linkup or session down events.
The configuration for LDP IGP synchronization resides in respective IGPs (OSPF and IS-IS) and there is no LDP-specific configuration for enabling of this feature. However, there is a specific LDP configuration for IGP sync delay timer.

Related Topics
- Configuring LDP IGP Synchronization: OSPF, on page 34
- Configuring LDP IGP Synchronization—OSPF: Example, on page 48
- Configuring LDP IGP Synchronization: ISIS, on page 35
- Configuring LDP IGP Synchronization—ISIS: Example, on page 49

IGP Auto-configuration

To enable LDP on a large number of interfaces, IGP auto-configuration lets you automatically configure LDP on all interfaces associated with a specified IGP interface; for example, when LDP is used for transport in the core network. However, there needs to be one IGP set up to enable LDP auto-configuration.

Typically, LDP assigns and advertises labels for IGP routes and must often be enabled on all active interfaces by an IGP. Without IGP auto-configuration, you must define the set of interfaces under LDP, a procedure that is time-intensive and error-prone.

Note
LDP auto-configuration is supported for IPv4 unicast family in the default VRF. The IGP is responsible for verifying and applying the configuration.

You can also disable auto-configuration on a per-interface basis. This permits LDP to enable all IGP interfaces except those that are explicitly disabled and prevents LDP from enabling an interface when LDP auto-configuration is configured under IGP.

Related Topics
- Enabling LDP Auto-Configuration for a Specified OSPF Instance, on page 36
- Enabling LDP Auto-Configuration in an Area for a Specified OSPF Instance, on page 38
- Disabling LDP Auto-Configuration, on page 39
- Configuring LDP Auto-Configuration: Example, on page 49

LDP Nonstop Routing

LDP nonstop routing (NSR) functionality makes failures, such as Route Processor (RP) or Distributed Route Processor (DRP) failover, invisible to routing peers with minimal to no disruption of convergence performance. By default, NSR is globally enabled on all LDP sessions except AToM.

A disruption in service may include any of these events:

- Route processor (RP) or distributed route processor (DRP) failover
- LDP process restart
- In-service system upgrade (ISSU)
Minimum disruption restart (MDR)

Unlike graceful restart functionality, LDP NSR does not require protocol extensions and does not force software upgrades on other routers in the network, nor does LDP NSR require peer routers to support NSR.

Note
Process failures of active TCP or LDP results in session loss and, as a result, NSR cannot be provided unless RP switchover is configured as a recovery action. For more information about how to configure switchover as a recovery action for NSR, see Configuring Transports module in Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

Related Topics
Configuring LDP Nonstop Routing, on page 40

IP LDP Fast Reroute Loop Free Alternate

The IP Fast Reroute is a mechanism that enables a router to rapidly switch traffic, after an adjacent link failure, node failure, or both, towards a pre-programmed loop-free alternative (LFA) path. This LFA path is used to switch traffic until the router installs a new primary next hop again, as computed for the changed network topology.

The goal of LFA FRR is to reduce failure reaction time to 50 milliseconds by using a pre-computed alternate next hop, in the event that the currently selected primary next hop fails, so that the alternate can be rapidly used when the failure is detected.

This feature targets to address the fast convergence ability by detecting, computing, updating or enabling prefix independent pre-computed alternate loop-free paths at the time of failure.

IGP pre-computes a backup path per IGP prefix. IGP selects one and only one backup path per primary path. RIB installs the best path and download path protection information to FIB by providing correct annotation for protected and protecting paths. FIB pre-installs the backup path in dataplane. Upon the link or node failure, the routing protocol detects the failure, all the backup paths of the impacted prefixes are enabled in a prefix-independent manner.

Prerequisites
The Label Distribution Protocol (LDP) can use the loop-free alternates as long as these prerequisites are met:

The Label Switching Router (LSR) running LDP must distribute its labels for the Forwarding Equivalence Classes (FECs) it can provide to all its neighbors, regardless of whether they are upstream, or not.

There are two approaches in computing LFAs:

- Link-based (per-link)--In link-based LFAs, all prefixes reachable through the primary (protected) link share the same backup information. This means that the whole set of prefixes, sharing the same primary, also share the repair or fast reroute (FRR) ability. The per-link approach protects only the next hop address. The per-link approach is suboptimal and not the best for capacity planning. This is because all traffic is redirected to the next hop instead of being spread over multiple paths, which may lead to potential congestion on link to the next hop. The per-link approach does not provide support for node protection.
• **Prefix-based (per-prefix)**—Prefix-based LFAs allow computing backup information per prefix. It protects the destination address. The per-prefix approach is the preferred approach due to its greater applicability, and the greater protection and better bandwidth utilization that it offers.

**Note**
The repair or backup information computed for a given prefix using prefix-based LFA may be different from the computed by link-based LFA.

The per-prefix LFA approach is preferred for LDP IP Fast Reroute LFA for these reasons:

• Better node failure resistance
• Better capacity planning and coverage

**Features Not Supported**
These interfaces and features are not supported for the IP LDP Fast Reroute Loop Free Alternate feature:

• BVI interface (IRB) is not supported either as primary or backup path.
• GRE tunnel is not supported either as primary or backup path.
• Cisco ASR 9000 Series SPA Interface Processor-700 POS line card on Cisco ASR 9000 Series Router is not supported as primary link. It can be used as LFA backup only on main interface.
• In a multi-topology scenario, the route in topology T can only use LFA within topology T. Hence, the availability of a backup path depends on the topology.

For more information about configuring the IP Fast Reroute Loop-free alternate, see Implementing IS-IS on Cisco IOS XR Software module of the *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*.

**Related Topics**
- Configure IP LDP Fast Reroute Loop Free Alternate: Examples, on page 50
- Verify IP LDP Fast Reroute Loop Free Alternate: Example, on page 51

**Downstream on Demand**
This Downstream on demand feature adds support for downstream-on-demand mode, where the label is not advertised to a peer, unless the peer explicitly requests it. At the same time, since the peer does not automatically advertise labels, the label request is sent whenever the next-hop points out to a peer that no remote label has been assigned.

To enable downstream-on-demand mode, this configuration must be applied at mpls ldp configuration mode:

```
mpls ldp downstream-on-demand with ACL
```

The ACL contains a list of peer IDs that are configured for downstream-on-demand mode. When the ACL is changed or configured, the list of established neighbors is traversed. If a session’s downstream-on-demand configuration has changed, the session is reset in order that the new down-stream-on-demand mode can be configured. The reason for resetting the session is to ensure that the labels are properly advertised between the peers. When a new session is established, the ACL is verified to determine whether the session should
negotiate for downstream-on-demand mode. If the ACL does not exist or is empty, downstream-on-demand mode is not configured for any neighbor.

For it to be enabled, the Downstream on demand feature has to be configured on both peers of the session. If only one peer in the session has downstream-on-demand feature configured, then the session does not use downstream-on-demand mode.

If, after, a label request is sent, and no remote label is received from the peer, the router will periodically resend the label request. After the peer advertises a label after receiving the label request, it will automatically readvertise the label if any label attribute changes subsequently.

Related Topics

 Configuring LDP Downstream on Demand mode, on page 41

Explicit-Null and Implicit-Null Labels

Cisco MPLS LDP uses null label, implicit or explicit, as local label for routes or prefixes that terminate on the given LSR. These routes include all local, connected, and attached networks. By default, the null label is **implicit-null** that allows LDP control plane to implement penultimate hop popping (PHOP) mechanism. When this is not desirable, you can configure **explicit-null** that allows LDP control plane to implement ultimate hop popping (UHOP) mechanism. You can configure this explicit-null feature on the ultimate hop LSR. This configuration knob includes an access-list to specify the IP prefixes for which PHOP is desired.

This new enhancement allows you to configure implicit-null local label for **non-egress (ultimate hop LSR)** prefixes by using the **implicit-null-override** command. This enforces implicit-null local label for a specific prefix even if the prefix requires a non-null label to be allocated by default. For example, by default, an LSR allocates and advertises a non-null label for an IGP route. If you wish to terminate LSP for this route on penultimate hop of the LSR, you can enforce implicit-null label allocation and advertisement for this prefix using **implicit-null-override** feature.

---

**Note**

If a given prefix is permitted in both explicit-null and implicit-null-override feature, then implicit-null-override supercedes and an implicit-null label is allocated and advertised for the prefix.

In order to enable implicit-null-override mode, this configuration must be applied at MPLS LDP label configuration mode:

```conf
mpls ldp
  label
    implicit-null-override for <prefix><ACL>
```

This feature works with any prefix including static, IGP, and BGP, when specified in the ACL.

How to Implement MPLS LDP

A typical MPLS LDP deployment requires coordination among several global neighbor routers. Various configuration tasks are required to implement MPLS LDP:
Configuring LDP Discovery Parameters

Perform this task to configure LDP discovery parameters (which may be crucial for LDP operations).

Note
The LDP discovery mechanism is used to discover or locate neighbor nodes.

SUMMARY STEPS

1. configure
2. mpls ldp
3. \[ vrf vrf-name \] router-id \ ip-address \ lsr-id
4. discovery \{ hello | targeted-hello \} holdtime seconds
5. discovery \{ hello | targeted-hello \} interval seconds
6. commit
7. (Optional) show mpls ldp \[ vrf vrf-name \] parameters

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mpls ldp</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> [ vrf vrf-name ] router-id \ ip-address \ lsr-id</td>
<td>(Optional) Specifies a non-default VRF. Specifies the router ID of the local node.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.168.70.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> discovery { hello</td>
<td>targeted-hello } holdtime seconds</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp)# discovery hello holdtime 30</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp)# discovery targeted-hello holdtime 180</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring LDP Discovery Over a Link

Perform this task to configure LDP discovery over a link.

**Note**
There is no need to enable LDP globally.

**Before You Begin**
A stable router ID is required at either end of the link to ensure the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> discovery { hello</td>
<td>targeted-hello } interval seconds</td>
</tr>
</tbody>
</table>
| **Example:** RP/0/RSP0/CPU0:router(config-ldp) # discovery hello interval 15  
RP/0/RSP0/CPU0:router(config-ldp) # discovery targeted-hello interval 20 | |
| **Step 6** commit | (Optional) Displays all the current MPLS LDP parameters. |
| **Step 7** show mpls ldp [vrf vrf-name] parameters | Displays the LDP parameters for the specified VRF. |
| **Example:** RP/0/RSP0/CPU0:router  
# show mpls ldp parameters  
RP/0/RSP0/CPU0:router  
# show mpls ldp vrf red parameters | |
SUMMARY STEPS

1. configure
2. mpls ldp
3. [vrf vrf-name] router-id  ip-address lsr-id
4. interface  type interface-path-id
5. commit
6. (Optional) show mpls ldp discovery
7. (Optional) show mpls ldp vrf vrf-name discovery
8. (Optional) show mpls ldp vrf all discovery summary
9. (Optional) show mpls ldp vrf all discovery brief
10. (Optional) show mpls ldp vrf all ipv4 discovery summary
11. (Optional) show mpls ldp discovery summary all

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mpls ldp</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>[vrf vrf-name] router-id  ip-address lsr-id</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.168.70.1</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>interface  type interface-path-id</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ldp-if)# interface tunnel-te 12001</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>commit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>show mpls ldp discovery</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router# show mpls ldp discovery</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>show mpls ldp vrf vrf-name discovery</td>
</tr>
<tr>
<td>Example:</td>
<td>Displays the status of the LDP discovery process for the specified VRF.</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router# show mpls ldp vrf red discovery</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>show mpls ldp vrf all discovery summary</td>
</tr>
<tr>
<td>Example:</td>
<td>Displays the summarized status of the LDP discovery process for all VRFs.</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery summary</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>show mpls ldp vrf all discovery brief</td>
</tr>
<tr>
<td>Example:</td>
<td>Displays the brief status of the LDP discovery process for all VRFs.</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery brief</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>show mpls ldp vrf all ipv4 discovery summary</td>
</tr>
<tr>
<td>Example:</td>
<td>Displays the summarized status of the LDP discovery process for all VRFs for the IPv4 address family.</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router# show mpls ldp vrf all ipv4 discovery summary</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>show mpls ldp discovery summary all</td>
</tr>
<tr>
<td>Example:</td>
<td>Displays the aggregate summary across all the LDP discovery processes.</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router# show mpls ldp discovery summary all</td>
</tr>
</tbody>
</table>

**Related Topics**

LDP Control Plane, on page 3  
Configuring LDP Link: Example, on page 45

**Configuring LDP Discovery for Active Targeted Hellos**

Perform this task to configure LDP discovery for active targeted hellos.

**Note**

The active side for targeted hellos initiates the unicast hello toward a specific destination.

**Before You Begin**

These prerequisites are required to configure LDP discovery for active targeted hellos:
• Stable router ID is required at either end of the targeted session. If you do not assign a router ID to the routers, the system will default to the global router ID. Please note that default router IDs are subject to change and may cause an unstable discovery.

• One or more MPLS Traffic Engineering tunnels are established between non-directly connected LSRs.

SUMMARY STEPS

1. configure
2. mpls ldp
3. [vrf vrf-name] router-id ip-address lsr-id
4. interface type interface-path-id
5. commit
6. (Optional) show mpls ldp discovery
7. (Optional) show mpls ldp vrf vrf-name discovery
8. (Optional) show mpls ldp vrf all discovery summary
9. (Optional) show mpls ldp vrf all discovery brief
10. (Optional) show mpls ldp vrf all ipv4 discovery summary
11. (Optional) show mpls ldp discovery summary all

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>Step 2 mpls ldp</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>Step 3 [vrf vrf-name] router-id ip-address lsr-id</td>
<td>(Optional) Specifies a non-default VRF. Specifies the router ID of the local node. In Cisco IOS XR software, the router ID is specified as an interface name or IP address or LSR ID. By default, LDP uses the global router ID (configured by global router ID process).</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Specifies a non-default VRF. Specifies the router ID of the local node. In Cisco IOS XR software, the router ID is specified as an interface name or IP address or LSR ID. By default, LDP uses the global router ID (configured by global router ID process).</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.168.70.1</td>
<td>(Optional) Specifies a non-default VRF. Specifies the router ID of the local node. In Cisco IOS XR software, the router ID is specified as an interface name or IP address or LSR ID. By default, LDP uses the global router ID (configured by global router ID process).</td>
</tr>
<tr>
<td>Step 4 interface type interface-path-id</td>
<td>Enters interface configuration mode for the LDP protocol.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters interface configuration mode for the LDP protocol.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp)# interface tunnel-te 12001</td>
<td>Enters interface configuration mode for the LDP protocol.</td>
</tr>
<tr>
<td>Step 5 commit</td>
<td>Enters interface configuration mode for the LDP protocol.</td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose |
--- | --- |
**Step 6** | **show mpls ldp discovery**  
*Example:*  
RP/0/RSP0/CPU0:router# show mpls ldp discovery  
(Optional)  
Displays the status of the LDP discovery process. This command, without an interface filter, generates a list of interfaces over which the LDP discovery process is running. The output information contains the state of the link (xmt/rcv hellos), local LDP identifier, the discovered peer's LDP identifier, and holdtime values. |
**Step 7** | **show mpls ldp vrf vrf-name discovery**  
*Example:*  
RP/0/RSP0/CPU0:router# show mpls ldp vrf red discovery  
(Optional)  
Displays the status of the LDP discovery process for the specified VRF. |
**Step 8** | **show mpls ldp vrf all discovery summary**  
*Example:*  
RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery summary  
(Optional)  
Displays the summarized status of the LDP discovery process for all VRFs. |
**Step 9** | **show mpls ldp vrf all discovery brief**  
*Example:*  
RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery brief  
(Optional)  
Displays the brief status of the LDP discovery process for all VRFs. |
**Step 10** | **show mpls ldp vrf all ipv4 discovery summary**  
*Example:*  
RP/0/RSP0/CPU0:router# show mpls ldp vrf all ipv4 discovery summary  
(Optional)  
Displays the summarized status of the LDP discovery process for all VRFs for the IPv4 address family. |
**Step 11** | **show mpls ldp discovery summary all**  
*Example:*  
RP/0/RSP0/CPU0:router# show mpls ldp discovery summary all  
(Optional)  
Displays the aggregate summary across all the LDP discovery processes. |

### Related Topics

- LDP Control Plane, on page 3
- Configuring LDP Discovery for Targeted Hellos: Example, on page 45

### Configuring LDP Discovery for Passive Targeted Hellos

Perform this task to configure LDP discovery for passive targeted hellos.
A passive side for targeted hello is the destination router (tunnel tail), which passively waits for an incoming hello message. Because targeted hellos are unicast, the passive side waits for an incoming hello message to respond with hello toward its discovered neighbor.

**Before You Begin**

Stable router ID is required at either end of the link to ensure that the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

**SUMMARY STEPS**

1. configure
2. mpls ldp
3. \[vrf vrf-name\] router-id ip-address lsr-id
4. discovery targeted-hello accept
5. commit
6. (Optional) show mpls ldp discovery
7. (Optional) show mpls ldp vrf vrf-name discovery
8. (Optional) show mpls ldp vrf all discovery summary
9. (Optional) show mpls ldp vrf all discovery brief
10. (Optional) show mpls ldp vrf all ipv4 discovery summary
11. (Optional) show mpls ldp discovery summary all

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>Step 2 mpls ldp</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
</tr>
<tr>
<td>Step 3 [vrf vrf-name] router-id ip-address lsr-id</td>
<td>(Optional) Specifies a non-default VRF.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.168.70.1</td>
</tr>
<tr>
<td>Step 4 discovery targeted-hello accept</td>
<td>Directs the system to accept targeted hello messages from any source and activates passive mode on the LSR for targeted hello acceptance.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# discovery targeted-hello accept</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>• You can control the targeted-hello acceptance using the <code>discovery targeted-hello accept</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>
| **Step 6** | `show mpls ldp discovery`  
**Example:**  
RP/0/RSP0/CPU0:router# show mpls ldp discovery |
| (Optional) Displays the status of the LDP discovery process. This command, without an interface filter, generates a list of interfaces over which the LDP discovery process is running. The output information contains the state of the link (xmt/rcv hellos), local LDP identifier, the discovered peer's LDP identifier, and holdtime values. | |
| **Step 7** | `show mpls ldp vrf vrf-name discovery`  
**Example:**  
RP/0/RSP0/CPU0:router# show mpls ldp vrf red discovery |
| (Optional) Displays the status of the LDP discovery process for the specified VRF. | |
| **Step 8** | `show mpls ldp vrf all discovery summary`  
**Example:**  
RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery summary |
| (Optional) Displays the summarized status of the LDP discovery process for all VRFs. | |
| **Step 9** | `show mpls ldp vrf all discovery brief`  
**Example:**  
RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery brief |
| (Optional) Displays the brief status of the LDP discovery process for all VRFs. | |
| **Step 10** | `show mpls ldp vrf all ipv4 discovery summary`  
**Example:**  
RP/0/RSP0/CPU0:router# show mpls ldp vrf all ipv4 discovery summary |
| (Optional) Displays the summarized status of the LDP discovery process for all VRFs for the IPv4 address family. | |
| **Step 11** | `show mpls ldp discovery summary all`  
**Example:**  
RP/0/RSP0/CPU0:router# show mpls ldp discovery summary all |
| (Optional) Displays the aggregate summary across all the LDP discovery processes. | |

**Related Topics**
- LDP Control Plane, on page 3
- Configuring LDP Discovery for Targeted Hellos: Example, on page 45
Configuring Label Advertisement Control (Outbound Filtering)

Perform this task to configure label advertisement (outbound filtering).

By default, a label switched router (LSR) advertises all incoming label prefixes to each neighboring router. You can control the exchange of label binding information using the `mpls ldp label advertise` command. Using the optional keywords, you can advertise selective prefixes to all neighbors, advertise selective prefixes to defined neighbors, or disable label advertisement to all peers for all prefixes.

**Note**
Prefixes and peers advertised selectively are defined in the access list.

**Before You Begin**
Before configuring label advertisement, enable LDP and configure an access list.

**SUMMARY STEPS**

1. `configure`
2. `mpls ldp`
3. `label advertise { disable | for prefix-acl [ to peer-acl ] | interface type interface-path-id }`
4. `commit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>mpls ldp</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config)# mpls ldp</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`label advertise { disable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config-ldp)# label advertise interface POS 0/1/0/0</code></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-ldp)# for pfx_acl1 to peer_acl1</code></td>
</tr>
<tr>
<td></td>
<td>Configures label advertisement by specifying one of the following options:</td>
</tr>
<tr>
<td></td>
<td><strong>disable</strong></td>
</tr>
<tr>
<td></td>
<td>Disables label advertisement to all peers for all prefixes (if there are no other conflicting rules).</td>
</tr>
<tr>
<td></td>
<td><strong>interface</strong></td>
</tr>
<tr>
<td></td>
<td>Specifies an interface for label advertisement of an interface address.</td>
</tr>
</tbody>
</table>
### Purpose

Command or Action | Purpose
---|---
| for prefix-acl to peer-acl | Specifies neighbors to advertise and receive label advertisements.

### Step 4

commit

--

**Related Topics**

Label Advertisement Control (Outbound Filtering), on page 9

Configuring Label Advertisement (Outbound Filtering): Example, on page 46

### Setting Up LDP Neighbors

Perform this task to set up LDP neighbors.

**Before You Begin**

Stable router ID is required at either end of the link to ensure the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

**SUMMARY STEPS**

1. configure
2. mpls ldp
3. interface type interface-path-id
4. discovery transport-address [ ip-address | interface ]
5. exit
6. holdtime seconds
7. neighbor ip-address password [ encryption ] password
8. backoff initial maximum
9. commit
10. (Optional) show mpls ldp neighbor

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
</tbody>
</table>
### Setting Up LDP Neighbors

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> mpls ldp</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type interface-path-id</td>
<td>Enters interface configuration mode for the LDP protocol.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ldp)# interface POS 0/1/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> discovery transport-address [ ip-address</td>
<td>Provides an alternative transport address for a TCP connection.</td>
</tr>
<tr>
<td>or interface ]</td>
<td>• Default transport address advertised by an LSR (for TCP connections) to its peer is the router ID.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ldp-if-asf)# discovery transport-address interface</td>
<td>• Transport address configuration is applied for a given LDP-enabled interface.</td>
</tr>
<tr>
<td>or</td>
<td>• If the interface version of the command is used, the configured IP address of the interface is passed to its neighbors as the transport address.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits the current configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ldp-if)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> holdtime seconds</td>
<td>Changes the time for which an LDP session is maintained in the absence of LDP messages from the peer.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ldp)# holdtime 30</td>
<td>• Outgoing keepalive interval is adjusted accordingly (to make three keepalives in a given holdtime) with a change in session holdtime value.</td>
</tr>
<tr>
<td>or</td>
<td>• Session holdtime is also exchanged when the session is established.</td>
</tr>
<tr>
<td>or</td>
<td>• In this example holdtime is set to 30 seconds, which causes the peer session to timeout in 30 seconds, as well as transmitting outgoing keepalive messages toward the peer every 10 seconds.</td>
</tr>
<tr>
<td><strong>Step 7</strong> neighbor ip-address password [ encryption ] password</td>
<td>Configures password authentication (using the TCP MD5 option) for a given neighbor.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ldp)# neighbor 192.168.2.44 password secretpasswd</td>
<td></td>
</tr>
</tbody>
</table>
Purpose
Command or Action | Purpose
--- | ---
Step 8 | backoff  initial maximum
Example: | Configures the parameters for the LDP backoff mechanism. The LDP backoff mechanism prevents two incompatibly configured LSRs from engaging in an unthrottled sequence of session setup failures. If a session setup attempt fails due to such incompatibility, each LSR delays its next attempt (backs off), increasing the delay exponentially with each successive failure until the maximum backoff delay is reached.

Step 9 | commit

Step 10 | show mpls ldp neighbor
Example: | (Optional) Displays the status of the LDP session with its neighbors. This command can be run with various filters as well as with the brief option.

Related Topics
Configuring LDP Neighbors: Example, on page 46

Setting Up LDP Forwarding

Perform this task to set up LDP forwarding.

By default, the LDP control plane implements the penultimate hop popping (PHOP) mechanism. The PHOP mechanism requires that label switched routers use the implicit-null label as a local label for the given Forwarding Equivalence Class (FEC) for which LSR is the penultimate hop. Although PHOP has certain advantages, it may be required to extend LSP up to the ultimate hop under certain circumstances (for example, to propagate MPL QoS). This is done using a special local label (explicit-null) advertised to the peers after which the peers use this label when forwarding traffic toward the ultimate hop (egress LSR).

Before You Begin
Stable router ID is required at either end of the link to ensure the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

SUMMARY STEPS
1. configure
2. mpls ldp
3. explicit-null
4. commit
5. (Optional) show mpls ldp forwarding
6. (Optional) show mpls forwarding
7. (Optional) ping ip-address
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mpls ldp</td>
<td>Causes a router to advertise an explicit null label in situations where it normally advertises an implicit null label (for example, to enable an ultimate-hop disposition instead of PHOP).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> explicit-null</td>
<td>(Optional) Displays the MPLS LDP view of installed forwarding states (rewrites).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp-af)# explicit-null</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> commit</td>
<td>Displays a global view of all MPLS installed forwarding states (rewrites) by various applications (LDP, TE, and static).</td>
</tr>
<tr>
<td><strong>Step 5</strong> show mpls ldp forwarding</td>
<td>(Optional) Checks for connectivity to a particular IP address (going through MPLS LSP as shown in the <code>show mpls forwarding</code> command).</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# show mpls ldp forwarding</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show mpls forwarding</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# show mpls forwarding</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ping <code>ip-address</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# ping 192.168.2.55</td>
<td></td>
</tr>
</tbody>
</table>

**Related Topics**

- LDP Forwarding, on page 4
- Configuring LDP Forwarding: Example, on page 47

**Setting Up LDP NSF Using Graceful Restart**

Perform this task to set up NSF using LDP graceful restart.

LDP graceful restart is a way to enable NSF for LDP. The correct way to set up NSF using LDP graceful restart is to bring up LDP neighbors (link or targeted) with additional configuration related to graceful restart.
Before You Begin

Stable router ID is required at either end of the link to ensure the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

SUMMARY STEPS

1. configure
2. mpls ldp
3. interface  type interface-path-id
4. exit
5. graceful-restart
6. graceful-restart forwarding-state-holdtime  seconds
7. graceful-restart reconnect-timeout  seconds
8. commit
9. (Optional)  show mpls ldp  parameters
10. (Optional)  show mpls ldp neighbor
11. (Optional)  show mpls ldp graceful-restart

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
</tbody>
</table>
| **Step 2**  | mpls ldp  
The system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery. |
| **Step 3**  | interface  type interface-path-id  
The system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery. |
| **Step 4**  | exit  
The system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery. |
| **Step 5**  | graceful-restart  
The system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery. |

Example:

```
RP/0/RSP0/CPU0:router(config) # mpls ldp
```

```
RP/0/RSP0/CPU0:router(config-ldp) # interface
POS 0/1/0/0
RP/0/RSP0/CPU0:router(config-ldp-if) #
```

```
RP/0/RSP0/CPU0:router(config-ldp-if) # exit
```

```
RP/0/RSP0/CPU0:router(config-ldp) # graceful-restart
```

Enables the LDP graceful restart feature.
### Setting Up LDP NSF Using Graceful Restart

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>graceful-restart forwarding-state-holdtime seconds</strong> Specifies the length of time that forwarding can keep LDP-installed forwarding states and rewrites, and specifies when the LDP control plane restarts.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# graceful-restart forwarding-state-holdtime 180</td>
</tr>
<tr>
<td></td>
<td>• After restart of the control plane, when the forwarding state holdtime expires, any previously installed LDP forwarding state or rewrite that is not yet refreshed is deleted from the forwarding.</td>
</tr>
<tr>
<td></td>
<td>• Recovery time sent after restart is computed as the current remaining value of the forwarding state hold timer.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>graceful-restart reconnect-timeout seconds</strong> Specifies the length of time a neighbor waits before restarting the node to reconnect before declaring an earlier graceful restart session as down. This command is used to start a timer on the peer (upon a neighbor restart). This timer is referred to as <strong>Neighbor Liveness</strong> timer.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# graceful-restart reconnect-timeout 169</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>commit</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>show mpls ldp parameters</strong> (Optional) Displays all the current MPLS LDP parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router # show mpls ldp parameters</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>show mpls ldp neighbor</strong> (Optional) Displays the status of the LDP session with its neighbors. This command can be run with various filters as well as with the brief option.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router# show mpls ldp neighbor</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>show mpls ldp graceful-restart</strong> (Optional) Displays the status of the LDP graceful restart feature. The output of this command not only shows states of different graceful restart timers, but also a list of graceful restart neighbors, their state, and reconnect count.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router# show mpls ldp graceful-restart</td>
</tr>
</tbody>
</table>

### Related Topics
- LDP Graceful Restart, on page 5
- Phases in Graceful Restart, on page 7
- Recovery with Graceful-Restart, on page 8
- Configuring LDP Nonstop Forwarding with Graceful Restart: Example, on page 47
Configuring Label Acceptance Control (Inbound Filtering)

Perform this task to configure LDP inbound label filtering.

By default, there is no inbound label filtering performed by LDP and thus an LSR accepts (and retains) all remote label bindings from all peers.

SUMMARY STEPS

1. configure
2. mpls ldp
3. label accept for prefix-acl from ip-address
4. [vrf vrf-name] address-family {ipv4}
5. label remote accept from ldp-id for prefix-acl
6. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters the MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>Step 2 mpls ldp</td>
<td>Enters the MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/O/RSP0/CPF0:router(config)# mpls ldp</td>
</tr>
<tr>
<td>Step 3 label accept for prefix-acl from ip-address</td>
<td>Configures inbound label acceptance for prefixes specified by prefix-acl from neighbor (as specified by its IP address).</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/O/RSP0/CPF0:router(config-ldp)# label accept for pfx_acl_1 from 192.168.1.1 \ RP/O/RSP0/CPF0:router(config-ldp)# label accept for pfx_acl_2 from 192.168.2.2</td>
</tr>
<tr>
<td>Step 4 [vrf vrf-name] address-family {ipv4}</td>
<td>(Optional) Specifies a non-default VRF. Enables the LDP IPv4 or IPv6 address family.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/O/RSP0/CPF0:router(config-ldp)# address-family ipv4 \ RP/O/RSP0/CPF0:router(config-ldp)# address-family ipv6</td>
</tr>
</tbody>
</table>
### Configuring Local Label Allocation Control

Perform this task to configure label allocation control.

**Note**  
By default, local label allocation control is disabled and all non-BGP prefixes are assigned local labels.

**SUMMARY STEPS**

1. configure  
2. mpls ldp  
3. label allocate for *prefix-acl*  
4. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters the MPLS LDP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mpls ldp</td>
<td></td>
</tr>
</tbody>
</table>
| **Example:**  
  `RP/0/RSP0/CPU0:router(config)# mpls ldp` | |
Purpose
Command or Action

Step 3
label allocate for prefix-acl

Example:
RP/0/RSP0/CPU0:router(config-ldp)# label allocate for pfx_acl_1

Step 4
commit

Configures label allocation control for prefixes as specified by prefix-acl.

Related Topics
Local Label Allocation Control, on page 10
Configuring Local Label Allocation Control: Example, on page 48

Configuring Session Protection

Perform this task to configure LDP session protection.
By default, there is no protection is done for link sessions by means of targeted hellos.

SUMMARY STEPS
1. configure
2. mpls ldp
3. session protection [ for peer-acl ] [ duration seconds ]
4. commit

DETAILED STEPS

Command or Action

Step 1
configure

Step 2
mpls ldp

Example:
RP/0/RSP0/CPU0:router(config)# mpls ldp

Step 3
session protection [ for peer-acl ] [ duration seconds ]

Example:
RP/0/RSP0/CPU0:router(config-ldp)# session protection for peer_acl_1 duration 60

Step 4
commit

Enables LDP session protection for peers specified by peer-acl with a maximum duration, in seconds.
Perform this task to configure LDP IGP Synchronization under OSPF.

### Summary Steps

1. `configure`  
2. `router ospf` `process-name`  
3. Use one of the following commands:  
   - `mpls ldp sync`  
   - `area area-id mpls ldp sync`  
   - `area area-id interface name mpls ldp sync`  
4. `commit`

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router ospf</code> <code>process-name</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0# router(config)# router ospf 100</code></td>
</tr>
</tbody>
</table>
| Step 3 | Use one of the following commands:  
   - `mpls ldp sync`  
   - `area area-id mpls ldp sync`  
   - `area area-id interface name mpls ldp sync` | Enables LDP IGP synchronization on an interface. |
### Configuring LDP IGP Synchronization: ISIS

Perform this task to configure LDP IGP Synchronization under ISIS.

**Note**  
By default, there is no synchronization between LDP and ISIS.

#### SUMMARY STEPS

1. configure
2. router isis instance-id
3. interface type interface-path-id
4. address-family {ipv4 } unicast
5. mpls ldp sync
6. commit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> router isis instance-id</td>
<td>Enables the Intermediate System-to-Intermediate System (IS-IS) routing protocol and defines an IS-IS instance.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config)# mpls ldp sync
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>interface type interface-path-id</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;RP/0/RSP0/CPU0:router(config-isis)# interface POS 0/2/0/0&lt;br&gt;RP/0/RSP0/CPU0:router(config-isis-if)#</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>address-family {ipv4 } unicast</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;RP/0/RSP0/CPU0:router(config-isis-if)# address-family ipv4 unicast&lt;br&gt;RP/0/RSP0/CPU0:router(config-isis-if-af)#</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>mpls ldp sync</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;RP/0/RSP0/CPU0:router(config-isis-if-af)# mpls ldp sync</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>commit</strong></td>
</tr>
</tbody>
</table>

**Related Topics**
- IGP Synchronization, on page 11
- Configuring LDP IGP Synchronization—ISIS: Example, on page 49

**Enabling LDP Auto-Configuration for a Specified OSPF Instance**

Perform this task to enable IGP auto-configuration globally for a specified OSPF process name.

You can disable auto-configuration on a per-interface basis. This lets LDP enable all IGP interfaces except those that are explicitly disabled.

**Note**

This feature is supported for IPv4 unicast family in default VRF only.
SUMMARY STEPS

1. configure
2. router ospf  process-name
3. mpls ldp auto-config
4. area  area-id
5. interface  type interface-path-id
6. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  configure</td>
<td></td>
</tr>
<tr>
<td>Step 2  router ospf  process-name</td>
<td>Enters a uniquely identifiable OSPF routing process. The process name is any alphanumeric string no longer than 40 characters without spaces.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0# router ospf 190</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0# router ospf</td>
<td></td>
</tr>
<tr>
<td>Step 3  mpls ldp auto-config</td>
<td>Enables LDP auto-configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0# mpls ldp auto-config</td>
<td></td>
</tr>
<tr>
<td>Step 4  area  area-id</td>
<td>Configures an OSPF area and identifier.</td>
</tr>
<tr>
<td>Example:</td>
<td>Either a decimal value or an IP address.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0# area 8</td>
<td></td>
</tr>
<tr>
<td>Step 5  interface  type interface-path-id</td>
<td>Enables LDP auto-configuration on the specified interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>LDP configurable limit for maximum number of interfaces does not apply to IGP auto-configuration interfaces.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0# interface pos 0/6/0/0</td>
<td></td>
</tr>
<tr>
<td>Step 6  commit</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- IGP Auto-configuration, on page 12
- Configuring LDP Auto-Configuration: Example, on page 49
- Disabling LDP Auto-Configuration, on page 39
Enabling LDP Auto-Configuration in an Area for a Specified OSPF Instance

Perform this task to enable IGP auto-configuration in a defined area with a specified OSPF process name. You can disable auto-configuration on a per-interface basis. This lets LDP enable all IGP interfaces except those that are explicitly disabled.

**Note**

This feature is supported for IPv4 unicast family in default VRF only.

**SUMMARY STEPS**

1. configure
2. router ospf  process-name
3. area  area-id
4. mpls ldp auto-config
5. interface type interface-path-id
6. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters a uniquely identifiable OSPF routing process. The process name is any alphanumeric string no longer than 40 characters without spaces.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router ospf  process-name</td>
<td>Configures an OSPF area and identifier.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# router ospf 100</td>
<td>Either a decimal value or an IP address.</td>
</tr>
<tr>
<td><strong>Step 3</strong> area  area-id</td>
<td>Enables LDP auto-configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ospf)# area 8</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> mpls ldp auto-config</td>
<td>Enables LDP auto-configuration on the specified interface. The LDP configurable limit for maximum number of interfaces does not apply to IGP auto-config interfaces.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ospf-ar)# mpls ldp auto-config</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface type interface-path-id</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ospf-ar)# interface</td>
<td></td>
</tr>
</tbody>
</table>
Disabling LDP Auto-Configuration

Perform this task to disable IGP auto-configuration.

You can disable auto-configuration on a per-interface basis. This lets LDP enable all IGP interfaces except those that are explicitly disabled.

SUMMARY STEPS

1. configure
2. mpls ldp
3. interface type interface-path-id
4. igp auto-config disable
5. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters the MPLS LDP configuration mode.</td>
</tr>
<tr>
<td>Step 2 mpls ldp</td>
<td>Enters interface configuration mode and configures an interface.</td>
</tr>
<tr>
<td>Step 3 interface type interface-path-id</td>
<td></td>
</tr>
</tbody>
</table>

Example:

```
RP/0/RSP0/CPU0:router(config)# mpls ldp
RP/0/RSP0/CPU0:router(config-ldp)#
```

```
RP/0/RSP0/CPU0:router(config-ldp)# interface pos 0/6/0/0
```
### Configuring LDP Nonstop Routing

Perform this task to configure LDP NSR.

**Note**
By default, NSR is globally-enabled on all LDP sessions except AToM.

**SUMMARY STEPS**

1. configure
2. mpls ldp
3. nsr
4. commit
5. (Optional) `show mpls ldp nsr statistics`
6. (Optional) `show mpls ldp nsr summary`
7. (Optional) `show mpls ldp nsr pending`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters the MPLS LDP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> mpls ldp</td>
<td></td>
</tr>
</tbody>
</table>

#### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>igp auto-config disable</code></td>
<td>Disables auto-configuration on the specified interface.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config-ldp-if)# igp auto-config disable
```
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>nsr</strong></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config-ldp)# nsr</code></td>
</tr>
<tr>
<td>Enables LDP nonstop routing.</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 4** | **commit** |
| **Step 5** | **show mpls ldp nsr statistics** |
| Example: | `RP/0/RSP0/CPU0:router# show mpls ldp nsr statistics` |
| (Optional) Displays MPLS LDP NSR statistics. |

| **Step 6** | **show mpls ldp nsr summary** |
| Example: | `RP/0/RSP0/CPU0:router# show mpls ldp nsr summary` |
| (Optional) Displays MPLS LDP NSR summarized information. |

| **Step 7** | **show mpls ldp nsr pending** |
| Example: | `RP/0/RSP0/CPU0:router# show mpls ldp nsr pending` |
| (Optional) Displays MPLS LDP NSR pending information. |

### Related Topics
- LDP Nonstop Routing, on page 12

### Configuring LDP Downstream on Demand mode

#### SUMMARY STEPS

1. `configure`
2. `mpls ldp`
3. `[vrf vrf-name session] downstream-on-demand`
4. `commit`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure</code></td>
</tr>
</tbody>
</table>
### Setting Up Implicit-Null-Override Label

Perform this task to configure implicit-null label for non-egress prefixes.

**SUMMARY STEPS**

1. configure
2. mpls ldp
3. label
4. implicit-null-override for *access-list*
5. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mpls ldp</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config)# mpls ldp
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>label</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ldp-af)# label</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Configures the allocation, advertisement, and acceptance of labels.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>implicit-null-override for access-list</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ldp-af-lbl)# implicit-null-override for 70</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This feature works with any prefix including static, IGP, and BGP, when specified in the ACL.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

**Redistributing MPLS LDP Routes into BGP**

Perform this task to redistribute Border Gateway Protocol (BGP) autonomous system into an MPLS LDP.

**SUMMARY STEPS**

1. configure
2. mpls ldp
3. redistribute bgp
4. end or commit
5. show run mpls ldp

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router# configure</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enters Global Configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>mpls ldp</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Enters MPLS LDP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>redistribute bgp</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>Allows the redistribution of BGP routes into an MPLS LDP processes.</td>
</tr>
</tbody>
</table>
### Purpose

Autonomous system numbers (ASNs) are globally unique identifiers used to identify autonomous systems (ASs) and enable ASs to exchange exterior routing information between neighboring ASs. A unique ASN is allocated to each AS for use in BGP routing. ASNs are encoded as 2-byte numbers and 4-byte numbers in BGP.

### Step 4

**end or commit**

- When you issue the **end** command, the system prompts you to commit changes:

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:
```

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

### Step 5

**show run mpls ldp**

**Example:**

```
RP/0/RSP0/CPU0:router# show run mpls ldp
```

Displays information about the redistributed route information.

### Configuration Examples for Implementing MPLS LDP

These configuration examples are provided to implement LDP:

#### Configuring LDP with Graceful Restart: Example

The example shows how to enable LDP with graceful restart on the POS interface 0/2/0/0.

```
mls ldp
  graceful-restart
  interface pos0/2/0/0
```
Configuring LDP Discovery: Example

The example shows how to configure LDP discovery parameters.

```plaintext
mpls ldp
  router-id 192.168.70.1
  discovery hello holdtime 15
  discovery hello interval 5
!
show mpls ldp parameters
show mpls ldp discovery
```

Configuring LDP Link: Example

The example shows how to configure LDP link parameters.

```plaintext
mpls ldp
  interface pos 0/1/0/0
!
!
show mpls ldp discovery
```

Related Topics

- Configuring LDP Discovery Over a Link, on page 17
- LDP Control Plane, on page 3

Configuring LDP Discovery for Targeted Hellos: Example

The examples show how to configure LDP Discovery to accept targeted hello messages.

Active (tunnel head)

```plaintext
mpls ldp
  router-id 192.168.70.1
  interface tunnel-te 12001
!
!
```

Passive (tunnel tail)

```plaintext
mpls ldp
  router-id 192.168.70.2
  discovery targeted-hello accept
!
```

Related Topics

- Configuring LDP Discovery for Active Targeted Hellos, on page 19
- Configuring LDP Discovery for Passive Targeted Hellos, on page 21
Configuring Label Advertisement (Outbound Filtering): Example

The example shows how to configure LDP label advertisement control.

```plaintext
mpls ldp
  label advertise
disable
  for pfx_acl_1 to peer_acl_1
  for pfx_acl_2 to peer_acl_2
  for pfx_acl_3
    interface POS 0/1/0/0
    interface POS 0/2/0/0

! ipv4 access-list pfx_acl_1
  10 permit ip host 1.0.0.0 any
! ipv4 access-list pfx_acl_2
  10 permit ip host 2.0.0.0 any
! ipv4 access-list peer_acl_1
  10 permit ip host 1.1.1.1 any
  20 permit ip host 1.1.1.2 any
! ipv4 access-list peer_acl_2
  10 permit ip host 2.2.2.2 any
!
show mpls ldp binding
```

Related Topics

- Configuring Label Advertisement Control (Outbound Filtering), on page 24
- Label Advertisement Control (Outbound Filtering), on page 9

Configuring LDP Neighbors: Example

The example shows how to disable label advertisement.

```plaintext
mpls ldp
  router-id 192.168.70.1
  neighbor 1.1.1.1 password encrypted 110A1016141E
  neighbor 2.2.2.2 implicit-withdraw
!
```

Related Topics

- Setting Up LDP Neighbors, on page 25
Configuring LDP Forwarding: Example

The example shows how to configure LDP forwarding.

```config
mpls ldp
  address-family ipv4
  label local advertise explicit-null

show mpls ldp forwarding
show mpls forwarding
```

Related Topics

- Setting Up LDP Forwarding, on page 27
- LDP Forwarding, on page 4

Configuring LDP Nonstop Forwarding with Graceful Restart: Example

The example shows how to configure LDP nonstop forwarding with graceful restart.

```config
mpls ldp
log graceful-restart
  graceful-restart forwarding state-holdtime 180
  graceful-restart reconnect-timeout 15
  interface pos0/1/0/0

show mpls ldp graceful-restart
show mpls ldp neighbor gr
show mpls ldp forwarding
show mpls forwarding
```

Related Topics

- Setting Up LDP NSF Using Graceful Restart, on page 28
- LDP Graceful Restart, on page 5
- Phases in Graceful Restart, on page 7
- Recovery with Graceful-Restart, on page 8

Configuring Label Acceptance (Inbound Filtering): Example

The example shows how to configure inbound label filtering.

```config
mpls ldp
label accept
  for pfx_aci_2 from 192.168.2.2

```
mpls ldp
  address-family ipv4
  label remote accept from 192.168.1.1:0 for pfx_acl_2
  
Related Topics
  Configuring Label Acceptance Control (Inbound Filtering), on page 31
  Label Acceptance Control (Inbound Filtering), on page 9

Configuring Local Label Allocation Control: Example

The example shows how to configure local label allocation control.

mpls ldp
  label
  allocate for pfx_acl_1
  
Related Topics
  Configuring Local Label Allocation Control, on page 32
  Local Label Allocation Control, on page 10

Configuring LDP Session Protection: Example

The example shows how to configure session protection.

mpls ldp
  session protection duration 60 for peer_acl_1
  
Related Topics
  Configuring Session Protection, on page 33
  Session Protection, on page 10

Configuring LDP IGP Synchronization—OSPF: Example

The example shows how to configure LDP IGP synchronization for OSPF.

router ospf 100
  mpls ldp sync
  mpls ldp
    igp sync delay 30
  

Configuring LDP IGP Synchronization—ISIS: Example

The example shows how to configure LDP IGP synchronization.

```
router isis 100
  interface POS 0/2/0/0
  address-family ipv4 unicast
  mpls ldp sync
    !
    !
  mpls ldp
  igp sync delay 30
```

Related Topics

- Configuring LDP IGP Synchronization: ISIS, on page 35
- IGP Synchronization, on page 11

Configuring LDP Auto-Configuration: Example

The example shows how to configure the IGP auto-configuration feature globally for a specific OSPF interface ID.

```
router ospf 100
  mpls ldp auto-config
  area 0
    interface pos 1/1/1/1
```

The example shows how to configure the IGP auto-configuration feature on a given area for a given OSPF interface ID.

```
router ospf 100
  area 0
    mpls ldp auto-config
    interface pos 1/1/1/1
```

Related Topics

- Enabling LDP Auto-Configuration for a Specified OSPF Instance, on page 36
- Enabling LDP Auto-Configuration in an Area for a Specified OSPF Instance, on page 38
- Disabling LDP Auto-Configuration, on page 39
- IGP Auto-configuration, on page 12
Configure IP LDP Fast Reroute Loop Free Alternate: Examples

This example shows how to configure LFA FRR with default tie-break configuration:

```
router isis TEST
net 49.0001.0000.0000.0001.00
  address-family ipv4 unicast
  metric-style wide
  interface GigabitEthernet0/6/0/13
    point-to-point
    address-family ipv4 unicast
    fast-reroute per-prefix
    # primary path GigabitEthernet0/6/0/13 will exclude the interface
    # GigabitEthernet0/6/0/33 in LFA backup path computation.
    fast-reroute per-prefix exclude interface GigabitEthernet0/6/0/33!
  interface GigabitEthernet0/6/0/23
    point-to-point
  interface GigabitEthernet0/6/0/24
  interface GigabitEthernet0/6/0/33

This example shows how to configure TE tunnel as LFA backup:

```
router isis TEST
net 49.0001.0000.0000.0001.00
  address-family ipv4 unicast
  metric-style wide
  interface GigabitEthernet0/6/0/13
    point-to-point
    address-family ipv4 unicast
    fast-reroute per-prefix
    # primary path GigabitEthernet0/6/0/13 will exclude the interface
    # GigabitEthernet0/6/0/33 in LFA backup path computation, TE tunnel 1001
    fast-reroute per-prefix lfa-candidate interface tunnel-te1001!
  interface GigabitEthernet0/6/0/33
```

This example shows how to configure LFA FRR with configurable tie-break configuration:

```
router isis TEST
net 49.0001.0000.0000.0001.00
  address-family ipv4 unicast
  metric-style wide
  fast-reroute per-prefix tiebreaker?
  downstream Prefer backup path via downstream node
  lc-disjoint Prefer line card disjoint backup path
  lowest-backup-metric Prefer backup path with lowest total metric
  node-protecting Prefer node protecting backup path
  primary-path Prefer backup path from ECMP set
  secondary-path Prefer non-ECMP backup path
```
Fast-reroute per-prefix tiebreaker lc-disjoint index 10
<1-255> Index
Fast-reroute per-prefix tiebreaker lc-disjoint index 10
Sample configuration:
router isis TEST
net 49.0001.0000.0000.0001.00
address-family ipv4 unicast
metric-style wide
fast-reroute per-prefix tiebreaker downstream index 60
fast-reroute per-prefix tiebreaker lc-disjoint index 10
fast-reroute per-prefix tiebreaker lowest-backup-metric index 40
fast-reroute per-prefix tiebreaker node-protecting index 30
fast-reroute per-prefix tiebreaker primary-path index 20
fast-reroute per-prefix tiebreaker secondary-path index 50
!
interface GigabitEthernet0/6/0/13
point-to-point
address-family ipv4 unicast
fast-reroute per-prefix
!
interface GigabitEthernet0/1/0/13
point-to-point
address-family ipv4 unicast
fast-reroute per-prefix
!
interface GigabitEthernet0/3/0/0.1
point-to-point
address-family ipv4 unicast
!
interface GigabitEthernet0/3/0/0.2
point-to-point
address-family ipv4 unicast

Related Topics
IP LDP Fast Reroute Loop Free Alternate, on page 13

Verify IP LDP Fast Reroute Loop Free Alternate: Example

The following examples show how to verify the IP LDP FRR LFA feature on the router. The following example shows how to verify ISIS FRR output:

```
RP/0/RSP0/CPU0:router#show isis fast-reroute summary
IS-IS 1 IPv4 Unicast FRR summary

<table>
<thead>
<tr>
<th>Prefixes reachable in L1</th>
<th>Critical Priority</th>
<th>High Priority</th>
<th>Medium Priority</th>
<th>Low Priority</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>All paths protected</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>1008</td>
<td>1012</td>
</tr>
<tr>
<td>Some paths protected</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unprotected</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Protection coverage</td>
<td>0.00%</td>
<td>0.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

Prefixes reachable in L2
<table>
<thead>
<tr>
<th>Prefixes reachable in L2</th>
<th>Critical Priority</th>
<th>High Priority</th>
<th>Medium Priority</th>
<th>Low Priority</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>All paths protected</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Some paths protected</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unprotected</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Protection coverage</td>
<td>0.00%</td>
<td>0.00%</td>
<td>100.00%</td>
<td>0.00%</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

The following example shows how to verify the IGP route 211.1.1.1/24 in ISIS Fast Reroute output:

RP/0/RSP0/CPU0:router#show isis fast-reroute 211.1.1.1/24
### Implementing MPLS Label Distribution Protocol

#### Verify IP LDP Fast Reroute Loop Free Alternate: Example

L1 211.1.1.1/24 [40/115]
- via 12.0.0.2, GigabitEthernet0/6/0/13, NORTH
- FRR backup via 14.0.2.2, GigabitEthernet0/6/0/0.3, SOUTH

RP/0/RSP0/CPU0# show isis fast-reroute 211.1.1.1/24 detail

L1 211.1.1.1/24 [40/115] low priority
- via 12.0.0.2, GigabitEthernet0/6/0/13, NORTH
- FRR backup via 14.0.2.2, GigabitEthernet0/6/0/0.3, SOUTH
- P: No, TM: 130, LC: No, NP: Yes, D: Yes
- src sr1.00-00, 173.1.1.2

L2 adv [40] native, propagated

The following example shows how to verify the IGP route 211.1.1.1/24 in RIB output:

RP/0/RSP0/CPU0# show route 211.1.1.1/24

Routing entry for 211.1.1.0/24
- Known via “isis 1”, distance 115, metric 40, type level-1
- Installed Nov 27 10:22:20.311 for 1d08h
- Routing Descriptor Blocks
  - 12.0.0.2, from 173.1.1.2, via GigabitEthernet0/6/0/13, Protected
    - Route metric is 40
  - 14.0.2.2, from 173.1.1.2, via GigabitEthernet0/6/0/0.3, Backup
    - Route metric is 0
- No advertising protos.

The following example shows how to verify the IGP route 211.1.1.1/24 in FIB output:

RP/0/RSP0/CPU0# show cef 211.1.1.1/24

211.1.1.0/24, version 0, internal 0x40040001 (ptr 0x9d9e1a68) [1], 0x0 (0x9ce0ec40), 0x4500 (0x9e2c69e4)
- remote adjacency to GigabitEthernet0/6/0/13
- Prefix Len 24, traffic index 0, precedence routine (0)
- Protected [flags 0x400]
  - path-idx 0, bkup-idx 1 [0x9e5b71b4 0x0]
  - next hop 12.0.0.2
  - local label 16080 labels imposed {16082}
  - via 14.0.2.2, GigabitEthernet0/6/0/0.3, 3 dependencies, weight 0, class 0, backup [flags 0x300]
    - path-idx 1
    - next hop 14.0.2.2
    - remote adjacency
    - local label 16080 labels imposed {16079}

RP/0/RSP0/CPU0# show cef 211.1.1.1/24 detail

211.1.1.0/24, version 0, internal 0x40040001 (ptr 0x9d9e1a68) [1], 0x0 (0x9ce0ec40), 0x4500 (0x9e2c69e4)
- Updated Nov 27 10:22:28.625
- remote adjacency to GigabitEthernet0/6/0/13
- Prefix Len 24, traffic index 0, precedence routine (0)
- protected [flags 0x400]
  - path-idx 0, bkup-idx 1 [0x9e5b71b4 0x0]
  - next hop 12.0.0.2
  - local label 16080 labels imposed {16082}
  - via 14.0.2.2, GigabitEthernet0/6/0/0.3, 3 dependencies, weight 0, class 0, backup [flags 0x300]
    - path-idx 1
    - next hop 14.0.2.2
    - remote adjacency
    - local label 16080 labels imposed {16079}
The following example shows how to verify the IGP route 211.1.1.1/24 in MPLS LDP output:

```
RP/0/RSP0/CPU0:router#show mpls ldp forwarding 211.1.1.1/24
```

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Label In</th>
<th>Label Out</th>
<th>Outgoing Interface</th>
<th>Next Hop</th>
<th>GR</th>
<th>Stale</th>
</tr>
</thead>
<tbody>
<tr>
<td>211.1.1.0/24</td>
<td>16080</td>
<td>16082</td>
<td>Gi0/6/0/13</td>
<td>12.0.0.2</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>16079</td>
<td></td>
<td>Gi0/6/0/0.3</td>
<td>14.0.2.2 (!)</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

```
RP/0/RSP0/CPU0:router#show mpls ldp forwarding 211.1.1.1/24 detail
```

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Label In</th>
<th>Label Out</th>
<th>Outgoing Interface</th>
<th>Next Hop</th>
<th>GR</th>
<th>Stale</th>
</tr>
</thead>
<tbody>
<tr>
<td>211.1.1.0/24</td>
<td>16080</td>
<td>16082</td>
<td>Gi0/6/0/13</td>
<td>12.0.0.2</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>16079</td>
<td></td>
<td>Gi0/6/0/0.3</td>
<td>14.0.2.2 (!)</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

Routing update : Nov 27 10:22:19.560 (1d08h ago)
Forwarding update: Nov 27 10:22:29.060 (1d08h ago)

**Related Topics**

- [IP LDP Fast Reroute Loop Free Alternate](#), on page 13

---

## Additional References

For additional information related to Implementing MPLS Label Distribution Protocol, refer to the following references:

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDP Commands</td>
<td><em>MPLS Label Distribution Protocol Commands</em> module in <em>Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference.</em></td>
</tr>
</tbody>
</table>

**Standards**

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

---

*Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide, Release 4.2.x*
### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>—</td>
<td>To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs Note</th>
<th>Not all supported RFCs are listed.</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3031</td>
<td></td>
<td>Multiprotocol Label Switching Architecture</td>
</tr>
<tr>
<td>RFC 3036</td>
<td></td>
<td>LDP Specification</td>
</tr>
<tr>
<td>RFC 3037</td>
<td></td>
<td>LDP Applicability</td>
</tr>
<tr>
<td>RFC 3478</td>
<td></td>
<td>Graceful Restart Mechanism for Label Distribution Protocol</td>
</tr>
<tr>
<td>RFC 3815</td>
<td></td>
<td>Definitions of Managed Objects for MPLS LDP</td>
</tr>
<tr>
<td>RFC 5036</td>
<td></td>
<td>Label Distribution and Management Downstream on Demand Label Advertisement</td>
</tr>
<tr>
<td>RFC 5286</td>
<td></td>
<td>Basic Specification for IP Fast Reroute: Loop-Free Alternates</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>