MPLS—LDP MD5 Global Configuration

First Published: February 28, 2006
Last Updated: February 19, 2007

The MPLS—LDP MD5 Global Configuration feature provides enhancements to the Label Distribution Protocol (LDP) implementation of the Message Digest 5 (MD5) password. This feature allows you to enable LDP MD5 globally instead of on a per-peer basis. Using this feature you can set up password requirements for a set of LDP neighbors to help prevent unauthorized peers from establishing LDP sessions and to block spoofed TCP messages.

This document provides information about and configuration information for the global configuration of LDP MD5 protection.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for MPLS—LDP MD5 Global Configuration" section on page 42.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for MPLS—LDP MD5 Global Configuration

- Cisco Express Forwarding or distributed Cisco Express Forwarding must be enabled on the label switch router (LSR).
- Routing (static or dynamic) must be configured for the LSR.
- Multiprotocol Label Switching (MPLS) LDP must be configured on the LSR. However, you can configure LDP MD5 protection before you configure MPLS LDP. You can then use LDP MD5 protection after you configure MPLS LDP.
- A Virtual Private Network (VPN) routing and forwarding instance (VRF) must be configured if you want to configure MPLS LDP MD5 global configuration for a VRF. If you delete a VRF, the LDP MD5 global configuration for that VRF is automatically removed.

Restrictions for MPLS—LDP MD5 Global Configuration

MD5 protection described in this document applies only to the LDP sessions. All enhancements described in this document do not affect Tag Distribution Protocol (TDP) sessions.

Information About MPLS—LDP MD5 Global Configuration

Before you configure the MPLS—LDP MD5 Global Configuration feature, you must understand the following:

Enhancements to LDP MD5 Protection for LDP Messages Between Peers

The MPLS—LDP MD5 Global Configuration feature provides the following enhancements to the LDP support of MD5 passwords:

- You can specify peers for which MD5 protection is required. This can prevent the establishment of LDP sessions with unexpected peers.
- You can configure passwords for groups of peers. This increases the scalability of LDP password configuration management.
- The established LDP session with a peer is not automatically torn down when the password for that peer is changed. The new password is used the next time an LDP session is established with the peer.
- You can control when the new password is used. You can configure the new password on the peer before forcing the use of the new password.

- If the neighboring nodes support graceful restart, then LDP sessions are gracefully restarted. The LDP MD5 password configuration is checkpointed to the standby Route Processors (RPs). The LDP MD5 password is used by the router when the new active RP attempts to establish LDP sessions with neighbors after the switchover.

LDP session, advertisement, and notification messages are exchanged between two LDP peers over a TCP connection. You can configure the TCP MD5 option to protect LDP messages that are exchanged over a TCP connection. You can configure this protection for each potential LDP peer. As a result, an LDP ignores any LDP hello messages sent from an LSR for which you have not configured a password. (LDP tries to establish an LDP session with each neighbor from which a hello message is received.)

Before the introduction of the MPLS—LDP MD5 Global Configuration feature, you needed to configure a separate password for each LDP peer for which you wanted MD5 protection. This was the case even when the same password was used for multiple LDP peers. Before this feature, LDP would tear down LDP sessions with a peer immediately if a password for that peer had changed.

LDP MD5 Password Configuration Information

Before the introduction of the MPLS—LDP MD5 Global Configuration feature, the command used for configuring a password for an LDP neighbor was **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password*. This command configures a password for one neighbor whose router ID is the IP address in the specified VRF. An LSR can have zero or one such configuration for each LDP neighbor.

You can use the commands provided by the MPLS—LDP MD5 Global Configuration feature to configure passwords for LDP neighbors.

You must understand how LDP determines the password for an LDP session between peers before you configure MD5 password protection for your network. LDP determines the passwords for its sessions based on the commands that you enter.

You can enter an **mpls ldp password vrf** *vrf-name* **required** [**for** *acl*] command, either with an optional *acl* argument that permits the LDP router ID of the neighbor or without an *acl* argument. Make sure that you enter a command that configures a password. Otherwise, LDP might not establish a session with the neighbor in question.

For the commands in the following password-determining process, *A.B.C.D:N* represents the LDP neighbor in VRF vpn1 and the neighbor LDP ID:

- *A.B.C.D* is the neighbor router ID.
- *N* is the neighbor label space ID.

To determine the password for an LDP session for the neighbor label space *A.B.C.D:N*, LDP looks at the password commands in the order indicated by the following statements:

- If you configured this command:

  mpls ldp neighbor vrf vpn1 *A.B.C.D* **password** *pwd-nbr*

  The LDP session password is *pwd-nbr*. LDP looks no further and uses the password you specify.

- Otherwise, LDP looks to see if you configured one or more **mpls ldp vrf vpn1 password option** commands. LDP considers the commands in order of the ascending *number* arguments (*number-1st to number-n*). For example:

  mpls ldp vrf vpn1 password option *number-1st* **for** *acl-1st pwd-1st*

LDP compares the peer router ID of the neighbor (*A.B.C.D)* with this command. If *A.B.C.D* is permitted by the command access list *acl-1st*, the session password is the command password, that is, *pwd-1st*.

If A.B.C.D is not permitted by *acl-1st*, LDP looks at the command with the next ascending *number* argument (*number-2nd*):

mpls ldp vrf vpn1 password option *number-2nd* **for** *acl-2nd pwd-2nd*

If *A.B.C.D* is permitted by the command access list *acl-2nd*, the session password is *pwd-2nd*.

If *A.B.C.D* is not permitted by the access list *acl-2nd*, LDP continues checking *A.B.C.D* against access lists until LDP:

- Finds *A.B.C.D* permitted by an access list. Then the command password is the session password.
- Has processed the *number-nth* argument of this command (*n* being the highest *number* argument you configured for this command).

- If the **mpls ldp vrf vpn1 password option** *number-nth* **for** *acl-nth pwd-nth* command produces no match and, therefore no password, LDP looks to see if you configured the following command:

  mpls ldp password vrf vpn1 fallback *pwd-fback*

  If you configured this command, the session password is *pwd-fback*.

- Otherwise, if LDP has not found a password, you did not configure a password for the session. LDP does not use MD5 protection for the session TCP connection.

LDP MD5 Password Configuration for Routing Tables

The MPLS—LDP MD5 Global Configuration feature introduces commands that can establish password protection for LDP sessions between LDP neighbors or peers. These commands can apply to routes in the global routing table or in a VRF.

By default, if the **vrf** keyword is not specified in the command, the command applies to the global routing table. The following sample commands would apply to routes in the global routing table:

```
Router# mpls ldp password required
Router# mpls ldp password option 15 for 99 pwd-acl
Router# mpls ldp password fallback pwd-fbck
```

You can configure LDP MD5 password protection for routes in a VRF only when the VRF is configured on the LSR. If you specify a VRF name and a VRF with that name is not configured on the LSR, LDP prints out a warning and discards the command. If you remove a VRF, LDP deletes the password configuration for that VRF. The following sample commands would apply to routes in a VRF, for example, VRF vpn1:

```
Router# mpls ldp vrf vpn1 password required
Router# mpls ldp vrf vpn1 password option 15 for 99 pwd-acl
Router# mpls ldp vrf vpn1 password fallback pwd-flbk
```

How to Configure the MPLS—LDP MD5 Global Configuration Feature

Perform the following tasks to configure the MPLS—LDP MD5 Global Configuration feature:

- Identifying LDP Neighbors for LDP MD5 Password Protection, page 5 (required)
- Configuring an LDP MD5 Password for LDP Sessions, page 7 (required)
- Verifying the LDP MD5 Configuration, page 14 (optional)

Password Requirements for LDP Sessions

You might require password protection for a certain set of neighbors for security reasons (for example, to prevent LDP sessions being established with unauthorized peers, or to block spoofed TCP messages). To enforce this security, you can configure a password requirement for LDP sessions with those neighbors that must have MD5 protection (TCP session uses a password).

If you configure a password requirement for a neighbor and you did not configure a password for the neighbor, LDP tears down the LDP sessions with the neighbor. LDP also tears down the LDP sessions with the neighbor if you configured a password requirement and a password and the password is not used in the LDP sessions.

If a password is required for a neighbor and the LDP sessions with the neighbor are established to use a password, any configuration that removes the password for the neighbor causes the LDP sessions to be torn down.

To avoid unnecessary LDP session flapping, you should perform the task as described in this section and use caution when you change LDP passwords.

Identifying LDP Neighbors for LDP MD5 Password Protection

Perform the following task to identify LDP neighbors for LDP MD5 password protection.

Prerequites

Before you start to configure passwords for LDP sessions, you must identify neighbors or groups of peers for which you want to provide MD5 protection. For example:

- You might have several customers that all use the same core routers. To ensure security you might want to provide each customer with a different password.
- You could have defined several departmental VRFs in your network. You could provide password protection for each VRF.
- Certain groups of peers might require password protection for security reasons. Password protection prevents unwanted LDP sessions.

Before you start to configure passwords for LDP sessions, you must identify neighbors or groups of peers for which you want to provide LDP MD5 password protection. This task uses the network in Figure 1 to show how you might identify LDP neighbors for LDP MD5 protection.

After you identify LDP neighbors or a group of peers for LDP MD5 protection, you must decide if password protection is mandatory and what password commands to use for each peer.

SUMMARY STEPS

1. Identify LDP neighbors or groups of peers for LDP MD5 password protection.
2. Decide what LDP MD5 protection is required for each neighbor or group of peers.

DETAILED STEPS

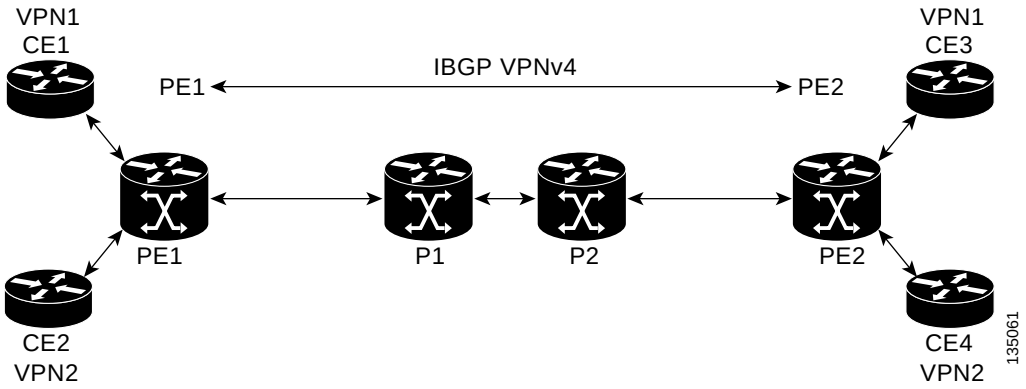
Step 1 Identify LDP neighbors or groups of peers for LDP MD5 password protection.

This task uses the network in Figure 1 to show how you might identify LDP neighbors for LDP MD5 protection.

Figure 1 shows a sample network that has the following topology:

- Carrier Supporting Carrier (CSC) is configured between provider edge (PE) router PE1 and customer edge (CE) router CE1 and between PE1 and CE2.
- Internal Border Gateway Protocol (IBGP) Virtual Private Network (VPN) IPv4 (VPNv4) to support Layer 3 VPNs is configured between PE1 and PE2.
- CE1 and CE3 are in VRF VPN1. CE2 and CE4 are in a different VRF, VPN2.

Figure 1 Sample Network: Identifying LDP Neighbors for LDP MD5 Protection



For the sample network in Figure 1, you could configure separate passwords on PE1 for the following:

- VRF VPN1
- VRF VPN2

You could also configure a password requirement on PE1 for P1, P2, CE1 and CE2.

Step 2 Decide what LDP MD5 protection is required for each neighbor or group of peers.

- If you need to set up a password for an LDP session with one peer or neighbor, for example, from PE1 to CE1, you could use the **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password-string* command, where *ip-address* is the router ID of the neighbor. See the "Configuring an LDP MD5 Password for LDP Sessions" section on page 7 for instructions.
- If you need to set up an LDP session password for a set of peers, for example for P1 and P2, you could set up an access list that permits access to these routers and denies access to all others. See the "Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers" section on page 12 for instructions.

- If you want to require a password for communication among VRF vpn1 members, you can configure a password requirement and password for VRF vpn1. If your network contains several VRFs, you can configure a password for each VRF. See the "Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF" section on page 10 for instructions.

Configuring an LDP MD5 Password for LDP Sessions

This section contains information about and instructions for configuring an LDP MD5 password for LDP sessions. You configure an LDP MD5 password to protect your routers from unwanted LDP sessions and provide LDP session security. You can provide LDP session security for a specific neighbor, or for LDP peers from a specific VRF or from the global routing table, or for a specific set of LDP neighbors.

After you have identified the LDP neighbor, LDP neighbors, or LDP peers in your network for which you want LDP MD5 password protection, perform the following procedures, as you require, to configure an LDP MD5 password for LDP sessions:

- Configuring an LDP MD5 Password for a Specified Neighbor, page 7
- Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF, page 10
- Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers, page 12

Configuring an LDP MD5 Password for a Specified Neighbor

Perform the following task to configure an LDP MD5 password for a specified neighbor.

LDP looks first for a password between the router and neighbor that is configured with the **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** *pwd-string* command. If a password is configured with this command, LDP uses that password before checking passwords configured by other commands.

You must add a configuration command for each neighbor or peer for which you want password protection.

Prerequisites

Identify the LDP neighbor or peer for which you want MD5 password protection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password-string*
4. **end**
5. **show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]
6. **show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] **password** [**pending** | **current**]
7. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password-string* **Example:** `Router(config)# mpls ldp neighbor vrf vpn1 10.1.1.1 password nbrce1pwd`	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor. • The **vrf** *vrf-name* keyword-argument pair specifies the VPN routing and forwarding instance for the specified neighbor. • The *ip-address* argument specifies the router ID (IP address) that identifies a neighbor. • The [**0** | **7**] keywords specify whether the password that follows is encrypted: – **0** specifies a clear-text (nonencrypted) password. – **7** specifies a Cisco proprietary encrypted password. • The *password-string* argument defines the password key to be used for computing MD5 checksums for the session TCP connection with the specified neighbor.
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | *interface*] [**detail**] [**graceful-restart**] **Example:** `Router# show mpls ldp neighbor vrf vpn1 detail`	Displays the status of LDP sessions. • The **vrf** *vrf-name* keyword-argument pair displays the LDP neighbors for the specified VRF instance (*vrf-name*). • The **all** keyword displays LDP neighbor information for all VPNs, including those in the default routing domain. • The *ip-address* argument identifies the neighbor with the IP address for which you configured password protection. • The *interface* argument defines the LDP neighbors accessible over this interface. • The **detail** keyword displays information in long form, including password information for this neighbor. Here are the items displayed: – An indication as to whether a password is mandatory for this neighbor (required or not required) – The password source (neighbor, fallback or number [option number]) – An indication as to whether the latest configured password for this neighbor is used by the TCP session (in use) or the TCP session uses an old password (stale) • The **graceful-restart** keyword displays per-neighbor graceful restart information.

	Command or Action	Purpose
Step 6	**show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] **password** [**pending** | **current**] **Example:** `Router# show mpls ldp neighbor vrf vpn1 password`	Displays password information used in established LDP sessions. • The **vrf** *vrf-name* keyword-argument pair displays the LDP neighbors for the specified VRF instance (*vrf-name*). • The *ip-address* argument identifies the neighbor with the IP address for which you configured password protection. • The *interface* argument defines the LDP neighbors accessible over this interface. • The **pending** keyword displays LDP sessions whose passwords are different from that in the current configuration. • The **current** keyword displays LDP sessions whose password is the same as that in current configuration. If you do not specify an optional keyword for this command, password information for all established LDP sessions is displayed.
Step 7	**show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**] **Example:** `Router# show mpls ldp discovery vrf vpn1 detail`	Displays the status of the LDP discovery process. • The **vrf** *vrf-name* keyword-argument pair displays the neighbor discovery information for the specified VRF instance (*vrf-name*). • The **all** keyword displays LDP discovery information for all VPNs, including those in the default routing domain. • The **detail** keyword displays detailed information about all LDP discovery sources on an LSR.

Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF

Perform the following task to configure an LDP MD5 password for LDP sessions with peers from a specified VRF. You can also use this task to configure an LDP MD5 password for LDP sessions with peers from the global routing table.

This task provides you with LDP session protection with peers from a particular VRF or the global routing table. If you want a password requirement, you can use the **mpls ldp password required** command.

If only LDP sessions with a set of LDP neighbors need MD5 protection, configure a standard IP access list that10 permits the desired set of LDP neighbors and denies the rest. See the "Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers" section on page 12.

Prerequisites

Identify LDP peers for which you want MD5 password protection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp** [**vrf** *vrf-name*] **password fallback** [**0** | **7**] *password*
4. **mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*]
5. **end**
6. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls ldp** [**vrf** *vrf-name*] **password fallback** [**0** | **7**] *password* **Example:** `Router(config)# mpls ldp vrf vpn1 password fallback 0 vrfpwdvppn1`	Configures an MD5 password for LDP sessions with peers. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The [**0** | **7**] keywords specify whether the password that follows is encrypted: – **0** specifies a clear-text (nonencrypted) password. – **7** specifies a Cisco proprietary encrypted password. • The *password* argument specifies the MD5 password to be used for the LDP sessions with peers whose connections are established through a named VRF or the global routing table. The example sets up an MD5 password for a VRF.
Step 4	**mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*] **Example:** `Router(config)# mpls ldp vrf vpn1 password required`	Specifies that LDP must use a password when establishing a session between LDP peers. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The **for** *acl* keyword-argument pair names an access list that specifies that a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the *acl* argument.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.
Step 6	**show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**] **Example:** `Router# show mpls ldp discovery detail`	Displays the status of the LDP discovery process. • The **vrf** *vrf-name* keyword-argument pair displays the neighbor discovery information for the specified VPN routing and forwarding instance (*vrf-name*). • The **all** keyword displays LDP discovery information for all VPNs, including those in the default routing domain. • The **detail** keyword displays detailed information about all LDP discovery sources on an LSR. Use this command to verify that password configuration is correct for all LDP neighbors.

Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers

Perform the following task to configure an LDP MD5 password for LDP sessions with a selected group of peers.

If only LDP sessions with a selected group of peers need MD5 protection, configure a standard IP access list that permits sessions with the desired group of peers (identified by LDP router IDs) and denies session with the rest. Configuring a password and password requirement for these neighbors or peers provides security by preventing LDP sessions from being established with unauthorized peers.

Prerequisites

Identify the groups of peers for which you want MD5 password protection and define an access list that permits LDP sessions with the group of peers you require.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0** | **7**] *password*
4. **mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*]
5. **end**
6. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0** | **7**] *password* **Example:** `Router(config)# mpls ldp password option 25 for 10 aclpwdfor10`	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The *number* argument defines the order in which the access lists are evaluated in the determination of a neighbor password. The valid range is 1–32767. • The **for** *acl* keyword-argument pair specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access list values (1–99) can be used for the *acl* argument. • The [**0** | **7**] keywords specifies whether the password that follows is encrypted: – **0** specifies a clear-text (nonencrypted) password. – **7** specifies a Cisco proprietary encrypted password. • The *password* argument specifies the MD5 password to be used for the specified LDP sessions.
Step 4	**mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*] **Example:** `Router(config)# mpls ldp password required for 10`	Specifies that LDP must use a password when establishing a session between LDP peers. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The **for** *acl* keyword-argument pair names an access list. The access list specifies a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the *acl* argument.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.
Step 6	**show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**] **Example:** `Router# show mpls ldp discovery detail`	Displays the status of the LDP discovery process. • The **vrf** *vrf-name* keyword-argument pair displays the neighbor discovery information for the specified VPN routing and forwarding instance (*vrf-name*). • The **all** keyword displays LDP discovery information for all VPNs, including those in the default routing domain. • The **detail** keyword displays detailed information about all LDP discovery sources on an LSR. Use this command to verify password configuration is correct for all LDP neighbors.

Verifying the LDP MD5 Configuration

Perform the following task to verify that the LDP MD5 secure sessions are as you configured for all LDP neighbors.

SUMMARY STEPS

1. **enable**
2. **show mpls ldp discovery detail**
3. **show mpls ldp neighbor detail**
4. **show mpls ldp neighbor password** [**pending** | **current**]
5. **exit**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

Step 2 **show mpls ldp discovery detail**

Use this command to verify that the LDP MD5 password information is as you configured for each neighbor. For example:

```
Router# show mpls ldp discovery detail

 Local LDP Identifier:
    10.1.1.1:0
    Discovery Sources:
    Interfaces:
```

```
    Ethernet1/0 (ldp): xmit/recv
        Hello interval: 5000 ms; Transport IP addr: 10.1.1.1
        LDP Id: 10.4.4.4:0
          Src IP addr: 10.0.20.4; Transport IP addr: 10.4.4.4
          Hold time: 15 sec; Proposed local/peer: 15/15 sec
          Password: not required, none, stale
Targeted Hellos:
    10.1.1.1 -> 10.3.3.3 (ldp): passive, xmit/recv
        Hello interval: 10000 ms; Transport IP addr: 10.1.1.1
        LDP Id: 10.3.3.3:0
          Src IP addr: 10.3.3.3; Transport IP addr: 10.3.3.3
          Hold time: 90 sec; Proposed local/peer: 90/90 sec
          Password: required, neighbor, in use
```

The Password field might display any of the following for the status of the password:

- Required or not required—Indicates whether password configuration is required.
- Neighbor, none, option #, or fallback—Indicates the password source when the password was configured.
- In use (current) or stale (previous)—Indicates the current LDP session password usage status.

Look at the output of the command to verify your configuration.

Step 3 **show mpls ldp neighbor detail**

Use this command to verify that the password information for a neighbor is as you configured. For example:

```
Router# show mpls ldp neighbor detail

    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 167/167; Downstream; Last TIB rev sent 9
        Up time: 02:24:02; UID: 5; Peer Id 3;
        LDP discovery sources:
          Targeted Hello 10.1.1.1 -> 10.3.3.3, passive;
            holdtime: 90000 ms, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
          10.3.3.3         10.0.30.3
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 9/9; Downstream; Last TIB rev sent 9
        Up time: 00:05:35; UID: 6; Peer Id 1;
        LDP discovery sources:
          Ethernet1/0; Src IP addr: 10.0.20.4
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          10.0.40.4       10.4.4.4         10.0.20.4
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

Step 4 **show mpls ldp neighbor password** [**pending** | **current**]

Use this command to verify that LDP sessions are using the password configuration that you expect, either the same as or different from that in the current configuration. The **pending** keyword displays information for LDP sessions whose password is different from that in the current configuration. The **current** keyword displays information for LDP sessions whose password is the same as that in the current configuration.

For example:

```
Router# show mpls ldp neighbor password

    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 57/57
    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 216/215

Router# show mpls ldp neighbor password pending

    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 57/57

Router# show mpls ldp neighbor password current

    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 216/215
```

This command displays password information used in established LDP sessions. If you do not enter an optional **pending** or **current** keyword for the command, password information for all established LDP sessions is displayed.

Step 5 **exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

Configuration Examples for Configuring the MPLS—LDP MD5 Global Configuration Feature

This section contains the following example for configuring the MPLS—LDP MD5 Global Configuration feature:

- Configuring an LDP MD5 Password for LDP Sessions: Examples, page 16

Configuring an LDP MD5 Password for LDP Sessions: Examples

The section contains the following examples for configuring an LDP MD5 password for LDP sessions:

- Configuring an LDP MD5 Password for LDP Sessions for a Specified Neighbor: Example, page 17
- Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF: Example, page 17

- Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers: Example, page 17

Configuring an LDP MD5 Password for LDP Sessions for a Specified Neighbor: Example

The following example shows how to configure an LDP MD5 password for LDP sessions for a specified neighbor:

```
enable
configure terminal
mpls ldp vrf vpn1 10.1.1.1 password nbrscrtpwd
end
```

This sets up nbrscrtpwd as the password to use for LDP sessions for the neighbor whose LDP router ID is 10.1.1.1. Communication with this neighbor is through VRF vpn1.

Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF: Example

The following example shows how to configure an LDP MD5 password for LDP sessions with peers from a specified VRF. The password vrfpwdvpn1 is configured for use with LDP peers that communicate using VRF vpn1. A password is required; otherwise, LDP tears down the session.

```
enable
configure terminal
mpls ldp vrf vpn1 password fallback vrfpwdvpn1
mpls ldp vrf vpn1 password required
end
```

The following example shows how to configure a password that is used for sessions for peers that communicate using the global routing table:

```
enable
configure terminal
mpls ldp password fallback vrfpwdvppn1
end
```

Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers: Example

The following example shows how to configure an LDP MD5 password for LDP sessions with a selected group of peers. The required password aclpwdfor10 is configured for access list 10. Only those LDP router IDs permitted in access list 10 are required to use the password.

```
enable
configure terminal
mpls ldp password option 25 for 10 aclpwdfor10
mpls ldp password required for 10
end
```

Access list 10 might look something like this:

```
enable
configure terminal
access-list 10 permit 10.1.1.1
access-list 10 permit 10.3.3.3
access-list 10 permit 10.4.4.4
access-list 10 permit 10.1.1.1
access-list 10 permit 10.2.2.2
end
```

Additional References

The following sections provide references related to the MPLS—LDP MD5 Global Configuration feature.

Related Documents

Related Topic	Document Title
Configuration tasks for LDP	"MPLS Label Distribution Protocol" chapter, *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4
Configuration tasks for SNMP LDP MIB	"MPLS Label Distribution Protocol MIB Version 8 Upgrade" module, *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

- **mpls ldp password fallback**
- **mpls ldp password option**
- **mpls ldp password required**
- **show mpls ldp discovery**
- **show mpls ldp neighbor**
- **show mpls ldp neighbor password**

mpls ldp password fallback

To configure a Message Digest 5 (MD5) password for Label Distribution Protocol (LDP) sessions with peers, use the **mpls ldp password fallback** command in global configuration mode. To remove the MD5 password, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password fallback** [**0** | **7**] *password*

no mpls ldp [**vrf** *vrf-name*] **password fallback**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance configured on the label switch router (LSR).
0 | **7**	(Optional) Specifies whether the *password* that follows is encrypted: • **0** specifies a clear-text (nonencrypted) password. • **7** specifies a Cisco proprietary encrypted password.
password	Specifies the MD5 password to be used for the LDP sessions with peers whose connections are established through a named VRF or the global routing table.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command specifies the default password for the VRF routing table. The VRF routing table name is specified by the *vrf-name* argument when you configure the **vrf** keyword for the command. If you do not include the **vrf** keyword in the command, the command specifies the default password for the global routing table. The password configured by this command is the password used for sessions between peers, if neither of the following commands applies: the **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** *pwd-nbr* command or the **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl password* command.

If you configure a type 7 (encrypted) password, the password is saved in encrypted form.

If you configure a type 0 (clear-text) password, it can be saved in clear-text form or encrypted form, depending on the status of the **service password-encryption** command:

- If the **service password-encryption** command is enabled, the type 0 password is converted and saved in encrypted form.

- If the **service password-encryption** command is not enabled, the type 0 password is saved in clear-text (nonencrypted) form.

When you enter a **show running-config** command, if the global **service password-encryption** command is enabled, a password saved in clear-text form is converted into encrypted form, and displayed and saved in encrypted form.

Examples

The following example shows how to configure an MD5 password for an LDP session with peers in VRF vpn1:

```
Router> enable
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls ldp vrf vpn1 password fallback password1
Router(config)# exit
Router#
```

The password, password1, would be encrypted. It is shown here as you would enter it on the command line.

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router ID are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
service password-encryption	Encrypts passwords.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password option

To configure a Message Digest 5 (MD5) password for Label Distribution Protocol (LDP) sessions with neighbors whose LDP router IDs are permitted by a specified access list, use the **mpls ldp password option** command in global configuration mode. To disable an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0** | **7**] *password*

no mpls ldp [**vrf** *vrf-name*] **password option** *number*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing/forwarding instance (VRF) configured on the label switch router (LSR).
number	The option number. A comparison of the *number* argument from several commands by the software sets up the order in which LDP evaluates access lists in the definition of a password for the neighbor. The valid range is 1 to 32767.
for *acl*	Specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access lists can be used for the *acl* argument.
0 | **7**	(Optional) Specifies whether the *password* that follows is encrypted: • **0** specifies a clear-text (nonencrypted) password. • **7** specifies a Cisco proprietary encrypted password.
password	Specifies the MD5 password to be used for the specified LDP sessions.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.0(32)SRB.

Usage Guidelines

This command specifies the *password* argument as the MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by an access list specified in the *acl* argument. This password is used if a password is not specified by the **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** *pwd-nbr* command.

When a configuration includes multiple **mpls ldp password option** commands, the *number* argument defines the order in which the command access lists are evaluated.

A configuration for a VRF can include zero, one, or more **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl password* commands.

You can specify the passwords in a clear-text format (type 0) or a Cisco-proprietary encrypted format (type 7). If you configure a type 7 (encrypted) password, the password is saved in encrypted form. If you configure a type 0 (clear-text) password, it can be saved in clear-text form or encrypted form, depending on the status of the **service password-encryption** command:

- If the **service password-encryption** command is enabled, the type 0 password is converted and saved in encrypted form.

  When you enter a **show running-config** command, if the global **service password-encryption** command is enabled, a password saved in clear-text form is converted into encrypted form, and displayed and saved in encrypted form.
- If the **service password-encryption** command is not enabled, the type 0 password is saved in clear-text (nonencrypted) form.

Examples

The following example shows how to configure an MD5 password for an LDP session with neighbors whose LDP router IDs are permitted by access list 10:

```
Router> enable
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls ldp password option 6 for 10 password1
Router(config)# exit
Router#
```

The password, *password1*, would be in clear-text (nonencrypted).

Related Commands

Command	Description
mpls ldp neighbor password	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor.
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.
service password-encryption	Encrypts passwords.
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

mpls ldp password required

To specify that Label Distribution Protocol (LDP) must use a password for an attempt to establish a session between LDP peers, use the **mpls ldp password required** command in global configuration mode. To remove the requirement that a password be used for a session with LDP, use the **no** form of this command.

mpls ldp [**vrf** *vrf-name*] **password required** [**for** *acl*]

no mpls ldp [**vrf** *vrf-name*] **password required** [**for** *acl*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a Virtual Private Network (VPN) routing and forwarding (VRF) instance configured on the label switch router (LSR).
for *acl*	(Optional) Access list that specifies a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the *acl* argument.

Defaults

If the **vrf** keyword is not specified in the command, the command applies to the global routing table.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command specifies that LDP must always use a password for an attempt to establish a session. If LDP cannot determine the password to use for an LDP session with a neighbor, an LDP session is not established.

The **vrf** keyword is available when you have configured a VRF on the LSR. If you specify a *vrf-name* argument and a VRF with that name is not configured on the LSR, a warning message is displayed and the command is discarded. If you remove a VRF, you also delete the password configured for that VRF.

Each VRF or global routing table can have zero or one **mpls ldp password required** command.

Examples

The following example shows how to specify that LDP must use a password for an attempt to establish a session between LDP peers:

```
Router> enable
Router# configure terminal
Router(config)# mpls ldp password required
```

Related Commands

Command	Description
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.

show mpls ldp discovery

To display the status of the Label Distribution Protocol (LDP) discovery process, use the **show mpls ldp discovery** command in user EXEC or privileged EXEC mode.

show mpls ldp discovery [**vrf** *vrf-name* | **all**] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the neighbor discovery information for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*).
all	(Optional) When the **all** keyword is specified alone in this command, the command displays LDP discovery information for all VPNs, including those in the default routing domain.
detail	(Optional) Displays detailed information about all LDP discovery sources on a label switch router (LSR).

Defaults

This command displays neighbor discovery information for the default routing domain if an optional **vrf** keyword is not specified.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST. The command was modified to comply with Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified for MPLS VPN support for LDP. The **vrf** and **all** keywords were added.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(8)T	This command was modified for MPLS VPN support for LDP. The **vrf** and **all** keywords were added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(14)T	The **detail** keyword was added to the command to display information related to the LDP Autoconfiguration feature.
12.2(28)SB	The **detail** keyword was updated to display information related to LDP Message Digest 5 (MD5) password configuration.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

This command displays neighbor discovery information for LDP or Tag Distribution Protocol (TDP). It generates a list of interfaces over which the LDP discovery process is running.

Examples

The following is sample output from the **show mpls ldp discovery** command:

```
Router# show mpls ldp discovery

Local LDP Identifier:
    10.1.1.1:0
Discovery Sources:
    Interfaces:
        Ethernet1/1/3 (ldp): xmit/recv
            LDP Id: 172.23.0.77:0
            LDP Id: 10.144.0.44:0
            LDP Id: 10.155.0.55:0
        ATM3/0.1 (ldp): xmit/recv
            LDP Id: 10.203.0.7:2
        ATM0/0.2 (tdp): xmit/recv
            TDP Id: 10.119.0.1:1
Targeted Hellos:
        10.8.1.1 -> 10.133.0.33 (ldp): active, xmit/recv
            LDP Id: 10.133.0.33:0
        10.8.1.1 -> 192.168.7.16 (tdp): passive, xmit/recv
            TDP Id: 10.133.0.33:0
Router#
```

The following is sample output from the **show mpls ldp discovery all** command, which shows the interfaces engaged in LDP discovery activity for all the VPN routing and forwarding instances, including those in the default routing domain. In this example, note that the same neighbor LDP ID (10.14.14.14) appears in all the listed VRF interfaces, highlighting the fact that the same IP address can coexist in different VPN routing and forwarding instances.

```
Router# show mpls ldp discovery all

Local LDP Identifier:
    10.12.12.12:0
    Discovery Sources:
    Interfaces:
        ATM1/1/0.1 (tdp):xmit/recv
            TDP Id:10.11.11.11:0
VRF vpn1:Local LDP Identifier:
    172.30.7.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.1 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn2:Local LDP Identifier:
    172.30.13.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.2 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn3:Local LDP Identifier:
    172.30.15.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.3 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn4:Local LDP Identifier:
    172.30.17.2:0
    Discovery Sources:
```

```
    Interfaces:
        ATM3/0/0.4 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn5:Local LDP Identifier:
    172.30.19.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.5 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn6:Local LDP Identifier:
    172.30.21.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.6 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn7:Local LDP Identifier:
    172.23.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.7 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn8:Local LDP Identifier:
    172.30.25.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.8 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn9:Local LDP Identifier:
    172.30.27.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.9 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn10:Local LDP Identifier:
    172.30.29.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.10 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn11:Local LDP Identifier:
    172.30.31.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.11 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn12:Local LDP Identifier:
    172.30.33.2:0
    Discovery Sources:
    Interfaces:
        ATM3/0/0.12 (ldp):xmit/recv
            LDP Id:10.14.14.14:0
VRF vpn13:Local LDP Identifier:

Router#
```

Table 1 describes the significant fields shown in the display.

Table 1 show mpls ldp discovery Field Descriptions

Field	Description
Local LDP Identifier	The LDP identifier for the local router. An LDP identifier is 6-bytes displayed in the form “IP address:number.” By convention, the first four bytes of the LDP identifier constitute the router ID; integers, starting with 0, constitute the final two bytes of the IP address:number construct.
Interfaces	Lists the interfaces that are engaging in LDP discovery activity: • The xmit field—Indicates that the interface is sending LDP discovery hello packets. • The recv field—Indicates that the interface is receiving LDP discovery hello packets. • The (LDP) or (TDP) field—Indicates the label distribution protocol configured for the interface. The LDP (or TDP) identifiers indicate the LDP (or TDP) neighbors discovered on the interface.
Targeted Hellos	Lists the platforms to which targeted hello messages are being sent: • The xmit, recv, (ldp), and (tdp) fields are as described for the Interfaces field. • The active field indicates that this LSR has initiated targeted hello messages. • The passive field indicates that the neighbor LSR has initiated targeted hello messages and that this LSR is configured to respond to the targeted hello messages from the neighbor. **Note** The entry for a given target platform may indicate both active and passive.

The following is sample output from the **show mpls ldp discovery detail** command showing that LDP was enabled by the **mpls ip** command and the **mpls ldp autoconfig** command:

```
Router# show mpls ldp discovery detail

Local LDP Identifier:
    10.11.11.11:0
    Discovery Sources:
    Interfaces:
        Serial2/0 (ldp): xmit/recv
            Enabled: Interface config, IGP config;
            Hello interval: 5000 ms; Transport IP addr: 10.11.11.11
            LDP Id: 10.10.10.10:0
              Src IP addr: 172.20.0.1; Transport IP addr: 10.10.10.10
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
```

Table 2 describes the significant fields shown in the display.

Table 2 show mpls ldp discovery detail Field Descriptions

Field	Description
Local LDP Identifier	The LDP identifier for the local router. An LDP identifier is a 6-byte construct displayed in the form “IP address:number.” By convention, the first four bytes of the LDP identifier constitute the router ID; integers, starting with 0, constitute the final two bytes of the IP address:number construct.
Interfaces	Lists the interfaces that are engaging in LDP discovery activity: • The xmit field—Indicates that the interface is sending LDP discovery hello packets. • The recv field—Indicates that the interface is receiving LDP discovery hello packets. • The LDP (or TDP) field—Indicates the label distribution protocol configured for the interface. The LDP (or TDP) identifiers indicate the LDP (or TDP) neighbors discovered on the interface.
Interface config; IGP config;	Describes how LDP is enabled: • Interface config—Enabled by the **mpls ip** command. • IGP config—Enabled by the **mpls ldp autoconfig** command. • Interface config; IGP config;—Enabled by the **mpls ip** command and the **mpls ldp autoconfig** command.
Hello interval	Period of time (in milliseconds) between the sending of consecutive hello messages.
Transport IP addr	Specifies that the interface address should be advertised as the transport address in the LDP discovery hello messages.
LDP Id	LDP ID of the peer router.
Src IP addr	Source IP address of the local router.
Transport IP addr	Specifies that the named IP address should be advertised as the transport address in the LDP discovery hello messages sent on an interface.
Hold time	Period of time (in seconds) a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor.
Proposed local/peer	Hold times (in seconds) proposed for LDP hello timer by the local router and the peer router. LDP uses the lower of these two values as the hold time.

The following is sample output from the **show mpls ldp discovery detail** command that displays information related to LDP MD5 passwords. Information related to MD5 passwords is pointed out in bold text in the output.

```
Router# show mpls ldp discovery detail

 Local LDP Identifier:
    10.10.10.10:0
    Discovery Sources:
    Interfaces:
```

```
    Ethernet1/0 (ldp): xmit/recv
        Hello interval: 5000 ms; Transport IP addr: 10.10.10.10
        LDP Id: 10.4.4.4:0
          Src IP addr: 10.0.20.4; Transport IP addr: 10.4.4.4
          Hold time: 15 sec; Proposed local/peer: 15/15 sec
          Password: not required, none, stale       <-- LDP MD5 password information
Targeted Hellos:
    10.10.10.10 -> 10.3.3.3 (ldp): passive, xmit/recv
        Hello interval: 10000 ms; Transport IP addr: 10.10.10.10
        LDP Id: 10.3.3.3:0
          Src IP addr: 10.3.3.3; Transport IP addr: 10.3.3.3
          Hold time: 90 sec; Proposed local/peer: 90/90 sec
          Password: required, neighbor, in use     <-- LDP MD5 password information
```

Password information displayed by this command includes:

- Password requirement for the neighbor (required or not required).
- Password source in the current configuration. The source is described by one of the following:
  - neighbor—This indicates that the password for the neighbor is retrieved from the **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password* command. The *ip-address* argument is the router ID of the neighbor.
  - num—This indicates that the password for the neighbor is retrieved from **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0** | **7**] *password* command. The *number* argument is a number from 1 to 32767. The *acl* argument is the name or number of an IP standard access list that permits the neighbor router ID.
  - fallback—The password for the neighbor is retrieved from **mpls ldp** [**vrf** *vrf-name*] **fallback** *password* command.
  - none—No password is configured for this neighbor.
- Password used by LDP sessions established with the neighbor is from current or previous configuration (in use or stale).

Related Commands

Command	Description
mpls label protocol (global configuration)	Specifies the label distribution protocol (LDP or TDP) to be used on a platform.
mpls label protocol (interface configuration)	Specifies the label distribution protocol (LDP or TDP) to be used on a given interface.
show mpls interfaces	Displays information about one or more interfaces that have been configured for label switching.
show mpls ldp neighbor	Displays the status of LDP sessions.

show mpls ldp neighbor

To display the status of Label Distribution Protocol (LDP) sessions, use the **show mpls ldp neighbor** command in user EXEC or privileged EXEC mode.

show mpls ldp neighbor [**vrf** *vrf-name* | **all**] [*address* | *interface*] [**detail**] [**graceful-restart**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*).
all	(Optional) Displays LDP neighbor information for all VPNs, including those in the default routing domain.
address	(Optional) Identifies the neighbor with this IP address.
interface	(Optional) Defines the LDP neighbors accessible over this interface.
detail	(Optional) Displays information in long form.
graceful-restart	(Optional) Displays per-neighbor graceful restart information.

Defaults

This command displays information about LDP neighbors for the default routing domain if you do not specify the optional **vrf** keyword.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	The command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP and the **vrf** and **all** keywords were added.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(26)S	The **detail** keyword was updated to display information about inbound filtering.
12.2(25)S	The **graceful-restart** keyword was added.
12.3(14)T	The command output was updated so that the **detail** keyword displays information about MPLS LDP Session Protection.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(28)SB	The **detail** keyword was updated to include Message Digest 5 (MD5) password information and the command was implemented on the Cisco 10000 Series Routers.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

The **show mpls ldp neighbor** command can provide information about all LDP neighbors, or the information can be limited to the following:

- Neighbor with specific IP address
- LDP neighbors known to be accessible over a specific interface

Note This command displays information about LDP and Tag Distribution Protocol (TDP) neighbor sessions.

Examples

For explanations of the significant fields shown in the displays, see Table 3.

The following is sample output from the **show mpls ldp neighbor** command:

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.0.7.7:2; Local LDP Ident 10.1.1.1:1
        TCP connection: 10.0.7.7.11032 - 10.1.1.1.646
        State: Oper; Msgs sent/rcvd: 5855/6371; Downstream on demand
        Up time: 13:15:09
        LDP discovery sources:
          ATM3/0.1
Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.1.1.1.646 - 10.1.1.1.11006
        State: Oper; Msgs sent/rcvd: 4/411; Downstream
        Up time: 00:00:52
        LDP discovery sources:
          Ethernet1/0/0
        Addresses bound to peer LDP Ident:
          10.0.0.29       10.1.1.1        10.0.0.199      10.10.1.1
          10.205.0.9
```

The following is sample output from the **show mpls ldp neighbor** command, in which duplicate addresses are detected. They indicate an error because a given address should be bound to only one peer.

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.0.7.7:2; Local LDP Ident 10.1.1.1:1
        TCP connection: 10.0.7.7.11032 - 10.1.1.1.646
        State: Oper; Msgs sent/rcvd: 5855/6371; Downstream on demand
        Up time: 13:15:09
        LDP discovery sources:
          ATM3/0.1
Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.1.1.1.646 - 10.1.1.1.11006
        State: Oper; Msgs sent/rcvd: 4/411; Downstream
        Up time: 00:00:52
        LDP discovery sources:
          Ethernet1/0/0
        Addresses bound to peer LDP Ident:
          10.0.0.29 10.1.1.1 10.0.0.199 10.10.1.1
          10.205.0.9
        Duplicate Addresses advertised by peer:
          10.10.8.111
```

The following is sample output from the **show mpls ldp neighbor vrf vpn10** command, which displays the LDP neighbor information for the specified VPN routing and forwarding instance named vpn10:

```
Router# show mpls ldp neighbor vrf vpn10

Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.29.0.2:0
        TCP connection:10.14.14.14.646 - 10.29.0.2.11384
        State:Oper; Msgs sent/rcvd:1423/800; Downstream
        Up time:02:38:11
        LDP discovery sources:
          ATM3/0/0.10
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
```

The following shows sample output from the **show mpls ldp neighbor detail** command, which displays information about inbound filtering:

```
Router# show mpls ldp neighbor vrf vpn1 detail

 Peer LDP Ident: 10.13.13.13:0; Local LDP Ident 10.33.0.2:0
   TCP connection: 10.13.13.13.646 - 10.33.0.2.31581
   State: Oper; Msgs sent/rcvd: 11/10; Downstream; Last TIB rev sent 13
   Up time: 00:02:25; UID: 26; Peer Id 0;
   LDP discovery sources:
    Ethernet1/0/2; Src IP addr: 10.33.0.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.3.105.1       10.13.13.13     10.33.0.1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl:1
 Peer LDP Ident: 10.14.14.14:0; Local LDP Ident 10.33.0.2:0
   TCP connection: 10.14.14.14.646 - 10.33.0.2.31601
   State: Oper; Msgs sent/rcvd: 10/9; Downstream; Last TIB rev sent 13
   Up time: 00:01:17; UID: 29; Peer Id 3;
   LDP discovery sources:
    Ethernet1/0/3; Src IP addr: 10.33.0.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.3.104.1       10.14.14.14     10.32.0.1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl:1
```

The following is sample output from the **show mpls ldp neighbor all** command, which displays the LDP neighbor information for all VPN routing and forwarding instances, including those in the default routing domain. In this example, note that the same neighbor LDP ID (10.14.14.14) appears in all the listed VRF interfaces, highlighting the fact that the same IP address can coexist in different VPN routing and forwarding instances.

```
Router# show mpls ldp neighbor all

Peer TDP Ident:10.11.11.11:0; Local TDP Ident 10.12.12.12:0
        TCP connection:10.11.11.11.711 - 10.12.12.12.11003
        State:Oper; PIEs sent/rcvd:185/187; Downstream
        Up time:02:40:02
        TDP discovery sources:
          ATM1/1/0.1
        Addresses bound to peer TDP Ident:
          10.3.38.3        10.1.0.2        10.11.11.11
VRF vpn1:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.7.0.2:0
        TCP connection:10.14.14.14.646 - 10.7.0.2.11359
        State:Oper; Msgs sent/rcvd:952/801; Downstream
        Up time:02:38:49
        LDP discovery sources:
          ATM3/0/0.1
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn2:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.13.0.2:0
        TCP connection:10.14.14.14.646 - 10.13.0.2.11361
        State:Oper; Msgs sent/rcvd:964/803; Downstream
        Up time:02:38:50
        LDP discovery sources:
          ATM3/0/0.2
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn3:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.15.0.2:0
        TCP connection:10.14.14.14.646 - 10.15.0.2.11364
        State:Oper; Msgs sent/rcvd:1069/800; Downstream
        Up time:02:38:52
        LDP discovery sources:
          ATM3/0/0.3
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.17.0.1       10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
```

```
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn4:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.17.0.2:0
        TCP connection:10.14.14.14.646 - 10.17.0.2.11366
        State:Oper; Msgs sent/rcvd:1199/802; Downstream
```

The following example shows the Graceful Restart status of the LDP neighbors:

```
Router# show mpls ldp neighbor graceful-restart

Peer LDP Ident: 10.20.20.20:0; Local LDP Ident 10.17.17.17:0
   TCP connection: 10.20.20.20.16510 - 10.17.17.17.646
    State: Oper; Msgs sent/rcvd: 8/18; Downstream
    Up time: 00:04:39
    Graceful Restart enabled; Peer reconnect time (msecs): 120000
Peer LDP Ident: 10.19.19.19:0; Local LDP Ident 10.17.17.17:0
    TCP connection: 10.19.19.19.11007 - 10.17.17.17.646
    State: Oper; Msgs sent/rcvd: 8/38; Downstream
    Up time: 00:04:30
    Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

The following sample output from the **show mpls ldp neighbor detail** command displays information about the MD5 password configuration:

```
Router# show mpls ldp neighbor detail

    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 167/167; Downstream; Last TIB rev sent 9
        Up time: 02:24:02; UID: 5; Peer Id 3;
        LDP discovery sources:
          Targeted Hello 10.1.1.1 -> 10.3.3.3, passive;
            holdtime: 90000 ms, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
          10.3.3.3        10.0.30.3
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 9/9; Downstream; Last TIB rev sent 9
        Up time: 00:05:35; UID: 6; Peer Id 1;
        LDP discovery sources:
          Ethernet1/0; Src IP addr: 10.0.20.4
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          10.0.40.4       10.4.4.4        10.0.20.4
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

Table 3 describes the significant fields shown in the displays.

Table 3 show mpls ldp neighbor Field Descriptions

Field	Description
Peer LDP Ident	LDP (or TDP) identifier of the neighbor (peer) for this session.
Local LDP Ident	LDP (or TDP) identifier for the local label switch router (LSR) for this session.
TCP connection	TCP connection used to support the LDP session, shown in the following format: • peer IP address.peer port • local IP address.local port
Password	Indicates if password protection is being used. Password status is as follows: • Required or not required—Indicates whether password configuration is required. • Neighbor, none, option #, or fallback—Indicates the password source when the password was configured. • In use (current) or stale (previous)—Indicates the current LDP session password usage status.
State	State of the LDP session. Generally, this is Oper (operational), but transient is another possible state.
Msgs sent/rcvd	Number of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintenance of the LDP session.
Downstream on demand	Indicates that the Downstream on Demand method of label distribution is being used for this LDP session. When the Downstream on Demand method is used, an LSR advertises its locally assigned (incoming) labels to its LDP peer only when the peer requests them.
Downstream	Indicates that the downstream method of label distribution is being used for this LDP session. When the downstream method is used, an LSR advertises all of its locally assigned (incoming) labels to its LDP peer (subject to any configured access list restrictions).
Up time	Length of time (in hours, minutes, seconds) the LDP session has existed.
Graceful Restart enabled	Indicates whether the LDP session has Graceful Restart enabled.
Peer reconnect time	The length of time, in milliseconds (msecs), the peer router waits for a router to reconnect.
LDP discovery sources	Sources of LDP discovery activity that led to the establishment of this LDP session.
Targeted Hello	Lists the platforms to which targeted hello messages are being sent: • The active field indicates that this LSR has initiated targeted hello messages. • The passive field indicates that the neighbor LSR has initiated targeted hello messages and that this LSR is configured to respond to the targeted hello messages from the neighbor.

Table 3 show mpls ldp neighbor Field Descriptions (continued)

Field	Description
holdtime	Period of time, in milliseconds (ms), a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor.
hello interval	Period of time, in milliseconds (ms), between the sending of consecutive hello messages.
Addresses bound to peer LDP Ident	Known interface addresses of the LDP session peer. These are addresses that might appear as “next hop” addresses in the local routing table. They are used to maintain the Label Forwarding Information Base (LFIB).
Duplicate Addresses advertised by peer	IP addresses that are bound to another peer. They indicate an error because a given address should be bound to only one peer.
Peer holdtime	The time, in milliseconds (ms), that the neighbor session is retained without the receipt of an LDP message from the neighbor.
KA Interval	Keep Alive Interval. The amount of time, in milliseconds (ms), that a router lets pass without sending an LDP message to its neighbor. If this time elapses and the router has nothing to send, it sends a Keep Alive message.
Peer state	State of the peer; estab means established.
LDP inbound filtering accept acl:1	Access list that is permitted for inbound label binding filtering.

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.

show mpls ldp neighbor password

To display password information used in established Label Distribution Protocol (LDP) sessions, use the **show mpls ldp neighbor password** command in user EXEC mode or privileged EXEC mode.

show mpls ldp neighbor [**vrf** *vrf-name*] [*ip-address* | *interface*] **password** [**pending** | **current**] [**all**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*).
ip-address	(Optional) Identifies the neighbor that has this IP address.
interface	(Optional) Defines the LDP neighbors accessible over this interface.
pending	(Optional) Displays LDP sessions whose password is different from that in the current configuration.
current	(Optional) Displays LDP sessions whose password is the same as that in the current configuration.
all	(Optional) When the **all** keyword is specified alone in this command, the command displays LDP password information for all neighbors in all VPNs, including those in the global routing table.

Defaults

If you do not configure an optional keyword for this command, password information for all established LDP sessions is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use this command to display password information for established LDP sessions. If you do not specify an option, password information for all established LDP sessions is displayed. To display LDP sessions whose password is the same as that in the current configuration, use the **current** keyword with the command. To display LDP sessions whose password is different from that in the current configuration, use the **pending** keyword with the command.

Examples

The following is sample output from the **show mpls ldp neighbor password** command that displays information for all established LDP sessions:

```
Router# show mpls ldp neighbor password

    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.10.01.10.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 57/57
    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 216/215
```

The following is sample output from the **show mpls ldp neighbor password pending** command that displays information for LDP sessions whose passwords are different from those in the current configuration:

```
Router# show mpls ldp neighbor password pending

    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 57/57
```

The following is sample output from the **show mpls ldp neighbor password current** command that displays information for LDP sessions whose passwords are the same as those in the current configuration:

```
Router# show mpls ldp neighbor password current

    Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 216/215
```

Table 4 describes the significant fields shown in the displays.

Table 4 show mpls ldp neighbor password Field Descriptions

Field	Description
Peer LDP Ident	LDP identifier of the neighbor (peer) for this session.
Local LDP Ident	LDP identifier for the local label switch router (LSR) for this session.
TCP connection	TCP connection used to support the LDP session, shown in the following format: • peer IP address.peer port • local IP address.local port

Table 4 show mpls ldp neighbor password Field Descriptions (continued)

Field	Description
Password	Indicates the password source and status. • Required or not required indicates whether password configuration is required or not. • Neighbor, none, option #, or fallback indicates the password source when the password was configured. None indicates that no password was configured. • In use (current) or stale (previous) is the usage status of the current LDP session password.
State	State of the LDP session. Generally this is Oper (operational), but transient is another possible state.
Msgs sent/rcvd	Numbers of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintaining the LDP session.

Related Commands

Command	Description
mpls ldp password fallback	Configures an MD5 password for LDP sessions with peers.
mpls ldp password option	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.
mpls ldp password required	Specifies that LDP must use a password when establishing a session between LDP peers.

Feature Information for MPLS—LDP MD5 Global Configuration

Table 5 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 5 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 5 Feature Information for MPLS—LDP MD5 Global Configuration

Feature Name	Releases	Feature Information
MPLS—LDP MD5 Global Configuration	12.2(28)SB 12.0(32)SY 12.2(33)SRB	The MPLS—LDP MD5 Global Configuration feature provides enhancements to the Label Distribution Protocol (LDP) implementation of the Message Digest 5 (MD5) password. This feature allows you to enable LDP MD5 globally instead of on a per-peer basis. Using this feature you can set up password requirements for a set of LDP neighbors to help prevent unauthorized peers from establishing LDP sessions and to block spoofed TCP messages. In 12.2(28)SB, this feature was introduced. In 12.0(32)SY, this feature was integrated into Cisco IOS Release 12.0(32)SY. The following sections provide information about this feature: • Enhancements to LDP MD5 Protection for LDP Messages Between Peers, page 2 • LDP MD5 Password Configuration Information, page 3 • LDP MD5 Password Configuration for Routing Tables, page 4 • Password Requirements for LDP Sessions, page 5 • Identifying LDP Neighbors for LDP MD5 Password Protection, page 5 • Identifying LDP Neighbors for LDP MD5 Password Protection, page 5 • Configuring an LDP MD5 Password for LDP Sessions, page 7 • Verifying the LDP MD5 Configuration, page 14 The following commands were modified by this feature: **mpls ldp password fallback**, **mpls ldp password option**, **mpls ldp password required**, **show mpls ldp discovery**, **show mpls ldp neighbor**, **show mpls ldp neighbor password**. This feature was integrated into Cisco IOS Release 12.2(33)SRB.

Glossary

BGP—Border Gateway Protocol. An interdomain routing protocol that replaces External Gateway Protocol (EGP). BGP systems exchange reachability information with other BGP systems. BGP is defined by RFC 1163.

EGP—Exterior Gateway Protocol. An internet protocol for exchanging routing information between autonomous systems. EGP is documented in RFC 904. EGP is not to be confused with the general term exterior gateway protocol. EGP is an obsolete protocol that was replaced by Border Gateway Protocol (BGP).

CE router—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

CSC—Carrier Supporting Carrier. A situation where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

LDP—Label Distribution Protocol. A standard protocol between Multiprotocol Label Switching (MPLS)-enabled routers that is uses in the negotiation of the labels used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

LDP peer—A label switch router (LSR) that is the receiver of label space information from another LSR. If an LSR has a label space to advertise to another LSR, or to multiple LSRs, one Label Distribution Protocol (LDP) session exists for each LSR (LDP peer) receiving the label space information.

MD5—Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. SNMP v.2 uses MD5 for message authentication, to verify the integrity of the communication, to authenticate the message origin, and to check its timeliness.

MPLS—Multiprotocol Label Switching. A switching method that forwards IP traffic through use of labels. Each label instructs the routers and the switches in the network where to forward a packet based on preestablished IP routing information.

PE router—provider edge router. A router that is part of a service provider's network connected to a customer edge (CE) router. All Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) processing occurs in the PE router.

VPN—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic forwarded from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

VRF—A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

Note See the *Internetworking Terms and Acronyms* for terms not included in this glossary.