

MPLS LDP Lossless MD5 Session Authentication

The MPLS LDP Lossless MD5 Session Authentication feature enables a Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) session to be password-protected without tearing down and reestablishing the LDP session.

- Prerequisites for MPLS LDP Lossless MD5 Session Authentication, on page 1
- Restrictions for MPLS LDP Lossless MD5 Session Authentication, on page 2
- Information About MPLS LDP Lossless MD5 Session Authentication, on page 2
- How to Configure MPLS LDP Lossless MD5 Session Authentication, on page 5
- Configuration Examples for MPLS LDP Lossless MD5 Session Authentication, on page 13
- Additional References, on page 25
- Feature Information for MPLS LDP Lossless MD5 Session Authentication, on page 25

Prerequisites for MPLS LDP Lossless MD5 Session Authentication

The MPLS LDP Lossless MD5 Session Authentication feature is an enhancement to the MPLS LDP MD5 Global Configuration feature. Before configuring the MPLS LDP Lossless MD5 Session Authentication feature, see the "MPLS LDP MD5 Global Configuration" feature module for more information on how the message digest algorithm 5 (MD5) works with Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) to ensure that LDP segments remain properly protected.

Note The MPLS LDP Lossless MD5 Session Authentication feature must be configured before MPLS LDP is configured.

Configure the following features on the label switch router (LSR) before configuring the MPLS LDP Lossless MD5 Session Authentication feature:

- Distributed Cisco Express Forwarding
- Static or dynamic routing
- MPLS Virtual Private Network (VPN) routing and forwarding (VRFs) instances for MPLS VPNs
- MPLS LDP Lossless MD5 Session Authentication for the MPLS VPN VRFs

Note If a VRF is deleted, then the lossless MD5 session authentication for that VRF is automatically removed.

Restrictions for MPLS LDP Lossless MD5 Session Authentication

Message Digest 5 (MD5) protection applies to Label Distribution Protocol {LDP} sessions between peers. Tag Distribution Protocol (TDP) sessions between peers are not protected.

Information About MPLS LDP Lossless MD5 Session Authentication

How MPLS LDP Messages in MPLS LDP Lossless MD5 Session Authentication are Exchanged

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) messages (discovery, session, advertisement, and notification messages) are exchanged between LDP peers through two channels:

- LDP discovery messages are transmitted as User Datagram Protocol (UDP) packets to the well-known LDP port.
- Session, advertisement, and notification messages are exchanged through a TCP connection established between two LDP peers.

The MPLS LDP Lossless MD5 Session Authentication feature allows an LDP session to be password-protected without tearing down and reestablishing the LDP session. The Message Digest 5 (MD5) password can be implemented and changed without interrupting the LDP session.

The Evolution of MPLS LDP MD5 Password Features

The initial version of Label Distribution Protocol (LDP) Message Digest 5 (MD5) protection allowed authentication to be enabled between two LDP peers and each segment sent on the TCP connection was verified between the peers. Authentication was configured on both LDP peers using the same password; otherwise, the peer session was not established. The **mpls ldp neighbor** command was issued with the **password** keyword. When MD5 protection was enabled, the device tore down the existing LDP sessions and established new sessions with the neighbor device.

An improved MD5 protection feature, called MPLS LDP MD5 Global Configuration, was later introduced that allowed LDP MD5 to be enabled globally instead of on a per-peer basis. Using this feature, password requirements for a set of LDP neighbors could be configured. The MPLS LDP MD5 Global Configuration feature also improved the ability to maintain the LDP session. The LDP session with a peer was not automatically torn down when the password for that peer was changed. The new password was implemented the next time an LDP session was established with the peer.

The MPLS LDP Lossless MD5 Session Authentication feature is based on the MPLS LDP MD5 Global Configuration feature. However, the MPLS LDP Lossless MD5 Session Authentication feature provides the following enhancements:

- Activate or change LDP MD5 session authentication without interrupting the LDP session.
- Configure multiple passwords, so one password can be used now and other passwords later.
- Configure asymmetric passwords, which allows one password to be used for incoming TCP segments and a different password to be used for outgoing TCP segments.
- Configure passwords so that they overlap for a period of time. This functionality is beneficial when the clocks on two label switch routers (LRS) are not synchronized.

These enhancements are available by using the **key-chain** command, which allows different key strings to be used at different times according to the keychain configuration.

Keychains Use with MPLS LDP Lossless MD5 Session Authentication

The MPLS LDP Lossless MD5 Session Authentication feature allows keychains to be used to specify different Message Digest 5 (MD5) keys to authenticate Label Distribution Protocol (LDP) traffic exchanged in each direction.

In the following example, three passwords are configured:

```
key chain ldp-pwd
 key 1
  key-string lab
  send-lifetime 10:00:00 Nov 2 2008 10:00:00 Dec 2 2008
  accept-lifetime 00:00:00 Jan 1 1970 duration 1
 key 2
  key-string lab2
  send-lifetime 00:00:00 Jan 1 1970 duration 1
  accept-lifetime 10:00:00 Nov 2 2008 10:00:00 Nov 17 2008
 key 3
  key-string lab3
  send-lifetime 00:00:00 Jan 1 1970 duration 1
  accept-lifetime 10:00:00 Nov 17 2008 10:00:00 Dec 2 2008
!
mpls ldp password option 1 for nbr-acl key-chain ldp-pwd
```

- Key 1 specifies the lab password. The **send-lifetime** command enables the lab password to authenticate the outgoing TCP segments from November 2, 2008, at 10:00:00 a.m. until December 2, 2008, at 10:00:00 a.m. The **accept-lifetime** command is configured so that the lab password is never used to authenticate incoming TCP segments. The **accept-lifetime** command enables the lab password for 1 second on January 1, 1970. By setting the date to the past and by enabling a duration of 1 second, the password for incoming TCP segments immediately expires. If the **accept-lifetime** command is omitted from the keychain configuration, then the password is always valid for incoming TCP segments.
- Key 2 and key 3 specify the lab2 and lab3 passwords, respectively. The **send-lifetime** commands enable the passwords for 1 second on January 1, 1970. By setting the date to the past and by enabling a duration of 1 second, the passwords for outgoing TCP segments immediately expire. If the **send-lifetime** commands are omitted from the keychain configuration, the passwords are always valid for outgoing TCP segments. The **accept-lifetime** commands for key 2 and key 3 enable the passwords to authenticate the incoming TCP segments from November 2, 2008, at 10:00:00 a.m. until November 17, 2008, at 10:00:00 a.m. and from November 17, 2008, at 10:00:00 a.m. until December 2, 2008, at 10:00:00 a.m., respectively.

Application of Rules to Overlapping Passwords

Overlapping passwords can be useful when two label switch routers (LSRs) have clocks that are not synchronized. The overlapping passwords provide a window to ensure that TCP packets are not dropped. The following rules apply to overlapping passwords:

- If the send-lifetime value for the next password begins before the send-lifetime value of the current password expires, the password with the shorter key ID is used during the overlap period. The send-lifetime value of the current password can be shortened by configuring a shorter send-lifetime value. Similarly, the send-lifetime value of the current password can be lengthened by configuring a longer send-lifetime value.
- If the accept-lifetime value for the next password begins before the accept-lifetime value of the current password expires, both the next password and the current password are used concurrently. The next password information is passed to TCP. If TCP fails to authenticate the incoming segments with the current password, it tries authenticating with the next password. If TCP authenticates a segment using the new password, it discards the current password and uses the new password from that point on.
- If a password for incoming or outgoing segments expires and no additional valid password is configured, one of the following actions take place:
  - If a password is required for the neighbor, the Label Distribution Protocol (LDP) drops the existing session.
  - If a password is not required for the neighbor, LDP attempts to roll over to a session that does not require authentication. This attempt also fails unless the password expires on both LSRs at the same time.

Password Rollover Period Guidelines

Both old and new passwords are valid during a rollover period. This ensures a smooth rollover when clocks are not synchronized between two Label Distribution Protocol (LDP) neighbors. When passwords are configured using a keychain, the rollover period is equal to the accept-lifetime overlap between two successive receive passwords.

The minimum rollover period (the duration between two consecutive Message Digest 5 (MD5) key updates) must be longer than the value of the LDP keepalive interval time to ensure an update of new MD5 authentication keys. If LDP session hold time is configured to its default value of 3 minutes, the LDP keepalive interval is 1 minute. The minimum rollover period should be 5 minutes. However, we recommend that the minimum rollover period is set to between 15 and 30 minutes.

To ensure a seamless rollover, follow these guidelines:

- Ensure that the local time on the peer label switch routers (LSRs) is the same before configuring the keychain.
- Check for error messages (TCP-6-BADAUTH) that indicate keychain misconfiguration.
- Validate the correct keychain configuration by checking for the following password messages:

```
%LDP-5-PWDCFG: Password configuration changed for 10.1.1.1:0
%LDP-5-PWDRO: Password rolled over for 10.1.1.1:0
```

Resolving LDP Password Problems

The Label Distribution Protocol (LDP) displays error messages when an unexpected neighbor attempts to open an LDP session, or the LDP password configuration is invalid. Some existing LDP debugs also display password information.

When a password is required for a potential LDP neighbor, but no password is configured for it, the label switch router (LSR) ignores LDP hello messages from that neighbor. When the LSR processes the hello message and tries to establish a TCP connection with the neighbor, it displays the error message and stops establishing the LDP session with the neighbor. The error is rate-limited and has the following format:

```
00:00:57: %LDP-5-PWD: MD5 protection is required for peer 10.2.2.2:0(glbl), no password
configured
```

When passwords do not match between LDP peers, TCP displays the following error message on the LSR that has the lower router ID; that is, the device that has the passive role in establishing TCP connections:

```
00:01:07: %TCP-6-BADAUTH: Invalid MD5 digest from 10.2.2.2(11051) to 10.1.1.1(646)
```

If one peer has a password configured and the other one does not, TCP displays the following error messages on the LSR that has a password configured:

```
00:02:07: %TCP-6-BADAUTH: No MD5 digest from 10.1.1.1(646) to 10.2.2.2(11099)
```

How to Configure MPLS LDP Lossless MD5 Session Authentication

Configuring MPLS LDP Lossless MD5 Session Authentication Using a Keychain

Perform the following task to configure the MPLS LDP Lossless MD5 Session Authentication feature using a keychain. Keychains allow a different key string to be used at different times according to the keychain configuration. Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) queries the appropriate keychain to obtain the current live key and key ID for the specified keychain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} {*type-code wildcard-mask* | *ip-address mask*}
4. **key chain** *name-of-chain*
5. **key** *key-id*
6. **key-string** *string*
7. **accept-lifetime** {*start-time* | **local** *start-time*} {**duration** | *seconds end-time* | **infinite**}
8. **send-lifetime** {*start-time* | **local** *start-time*} {**duration** *seconds end-time* | **infinite**}
9. **exit**
10. **exit**
11. **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* {**key-chain** *keychain-name* | [**0** | **7**] *password*}

12. **exit**
13. **show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter the password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**permit** | **deny**} {*type-code wildcard-mask* | *ip-address mask*} **Example:** `Device(config)# access-list 10 permit 10.2.2.2`	Creates an access list.
Step 4	**key chain** *name-of-chain* **Example:** `Device(config)# key chain ldp-pwd`	Enables authentication for routing protocols and identifies a group of authentication keys. • Enters keychain configuration mode.
Step 5	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Identifies an authentication key on a keychain. • The *key-id* value must be a numeral. • Enters keychain key configuration mode.
Step 6	**key-string** *string* **Example:** `Device(config-keychain-key)# key-string pwd1`	Specifies the authentication string for a key. • The *string* value can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral.
Step 7	**accept-lifetime** {*start-time* | **local** *start-time*} {**duration** | *seconds end-time* | **infinite**} **Example:** `Device(config-keychain-key)# accept-lifetime 10:00:00 Jan 13 2007 10:00:00 Jan 13 2009`	Specifies the time period during which the authentication key on a keychain can be used for verifying incoming TCP segments. The *start-time* argument identifies the time to start and the local *start-time* argument identifies the time to start in the local time zone. Both arguments have the same parameters: **Note**

	Command or Action	Purpose
		The time reference depends on the clock time zone configuration on the device. If no time zone configured, then the default time zone uses the Coordinated Universal Time (UTC) time. If it is configured, either the Eastern Standard Time (EST) or Pacific Standard Time (PST) time zone is used. • *hh:mm:ss* is the time format. • Enter the number of days from 1 to 31. • Enter the name of the month. • Enter the year from the present to 2035. Once the start time is entered, select from the following: • The **duration** keyword sets the key lifetime duration in seconds. • The *end-time* argument sets the time to stop. These parameters are the same as those used for the *start-time* argument. • The **infinite** keyword allows the accept-lifetime period to never expire. If the **no accept-lifetime** value is defined, the associated receive password is valid for authenticating incoming TCP segments.
Step 8	**send-lifetime** {*start-time* | **local** *start-time*} {**duration** *seconds end-time* | **infinite**} **Example:** `Device(config-keychain-key)# send-lifetime 10:00:00 Jan 13 2007 10:00:00 Jan 13 2009`	Specifies the time period during which the authentication key on a keychain can be used for verifying outgoing TCP segments. The *start-time* argument identifies the time to start and the local *start-time* argument identifies the time to start in the local time zone. Both arguments have the same parameters: **Note** The time reference depends on the clock time zone configuration on the device. If no time zone configured, then the default time zone uses the UTC time. If it is configured, either the EST or PST time zone is used. • *hh:mm:ss* is the time format. • Enter the number of days from 1 to 31. • Enter the name of the month. • Enter the year from 1993 to 2035. Once the start time is entered, select from the following:

	Command or Action	Purpose
		• The **duration** keyword sets the send lifetime duration in seconds. • The *end-time* argument sets the time to stop. These parameters are the same as those used for the *start-time* argument. • The **infinite** keyword allows the send lifetime period to never expire. If the **no send-lifetime** value is defined, the associated send password is valid for authenticating outgoing TCP segments.
Step 9	**exit** **Example:** `Device(config-keychain-key)# exit`	Returns to keychain configuration mode.
Step 10	**exit** **Example:** `Device(config-keychain)# exit`	Returns to global configuration mode.

Step 11	**mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* {**key-chain** *keychain-name* | [**0** | **7**] *password*}
	Example:
	`Device(config)# mpls ldp password option 1 for 10 keychain ldp-pwd`
		Configures a Message Digest 5 (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 virtual routing and forwarding (VRF) configured on the label switch router (LSR).
		• The *number* argument defines the order in which the access lists are evaluated in the determination of a neighbor password. The range is 1 to 32767.
		• The **for** *acl* keyword and argument 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 to 99) can be used for the *acl* argument.
		• The **key-chain** *keychain-name* keyword and argument specifies the name of the keychain to use.
		• The **0** and **7** keywords specify whether the password that follows is hidden (encrypted);
		  • **0** specifies an unencrypted password.
		  • **7** specifies an encrypted password.
		• The *password* argument specifies the MD5 password to be used for the specified LDP sessions.

	Command or Action	Purpose
Step 12	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Step 13	**show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]
	Example:
	`Device# show mpls ldp neighbor detail`
		Displays the status of LDP sessions.
		• The **vrf** *vrf-name* keyword and argument displays the LDP neighbors for the specified VRF instance.
		• The *ip-address* argument identifies the neighbor with the IP address for which password protection is configured.
		• The *interface* argument identifies 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/not required)
		  • The password source (neighbor/fallback/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.

Enabling the Display of MPLS LDP Password Rollover Changes and Events

When a password is required for a neighbor, but no password is configured for the neighbor, the following debug message is displayed:

```
00:05:04: MDSym5 protection is required for peer 10.2.2.2:0(glbl), but no password configured.
```

To enable the display of events related to configuration changes and password rollover events, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp logging password configuration** [**rate-limit** *number*]

4. **mpls ldp logging password rollover** [**rate-limit** *number*]
5. **exit**
6. **debug mpls ldp transport events**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ldp logging password configuration** [**rate-limit** *number*] **Example:** `Device(config)# mpls ldp logging password configuration rate-limit 30`	Enables the display of events related to configuration changes. • The output displays events when a new password is configured or an existing password has been changed or deleted. A rate limit of 1 to 60 messages a minute can be specified.
Step 4	**mpls ldp logging password rollover** [**rate-limit** *number*] **Example:** `Device(config)# mpls ldp logging password rollover rate-limit 25`	Enables the display of events related to password rollover events. • Events are displayed when a new password is used for authentication or when authentication is disabled. A rate limit of 1 to 60 messages a minute can be specified.
Step 5	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 6	**debug mpls ldp transport events** **Example:** `Device# debug mpls ldp transport events`	Displays notifications when a session TCP Message Digest 5 (MD5) option is changed. • You can also use the **debug mpls ldp transport connections** command to display notifications when the MD5 option is changed.

Changing MPLS LDP Lossless MD5 Session Authentication Passwords

The MPLS LDP Lossless MD5 Session Authentication feature allows Message Digest 5 (MD5) passwords to be changed for Label Distribution Protocol (LDP) session authentication without having to close and reestablish an existing LDP session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp** [**vrf** *vrf-name*] **password rollover duration** *minutes*
4. **mpls ldp** [**vrf** *vrf-name*] **password fallback** {**key-chain** *keychain-name* | [**0** | **7**] *password*}
5. **no mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** *password*
6. **exit**
7. **show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter the password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ldp** [**vrf** *vrf-name*] **password rollover duration** *minutes* **Example:** `Device(config)# mpls ldp password rollover duration 7`	Configures the duration before the new password takes effect. • The **vrf** *vrf-name* keyword and argument specifies a virtual routing and forwarding (VRF) configured on the label switch router (LSR). • The *minutes* argument specifies the number of minutes from 5 to 65535 before the password rollover occurs on this device.
Step 4	**mpls ldp** [**vrf** *vrf-name*] **password fallback** {**key-chain** *keychain-name*	[**0**	**7**] *password*} **Example:** `Device(config)# mpls ldp password fallback key-chain fallback`	Configures an MD5 password for LDP sessions with peers. • The **vrf** *vrf-name* keyword and argument specifies a VRF configured on the LSR. • The **key-chain** *keychain-name* keyword and argument specifies the name of the keychain used to specify the

	Command or Action	Purpose

		MD5 key that authenticates the exchange of bidirectional LDP traffic.
		• The **0** and **7** keywords specify whether the password that follows is hidden (encrypted);
		  • **0** specifies an unencrypted password.
		  • **7** specifies an encrypted password.
		• The *password* argument specifies the MD5 password to be used for the specified LDP sessions.

Step 5	**no mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** *password* **Example:** `Device(config)# no mpls ldp neighbor 10.11.11.11 password lab1`	Disables the configuration of a password for computing MD5 checksums for the session TCP connection with the specified neighbor. • The **vrf** *vrf-name* keyword and argument optionally specifies the VRF instance for the specified neighbor. • The *ip-address* argument identifies the neighbor router ID. • The **password** *password* keyword and argument is necessary so that the device computes MD5 checksums for the session TCP connection with the specified neighbor.
Step 6	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Step 7	**show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]
	Example:
	`Device# show mpls ldp neighbor detail`
		Displays the status of LDP sessions.
		• The **vrf** *vrf-name* keyword argument displays the LDP neighbors for the specified VRF instance.
		• The *ip-address* argument identifies the neighbor with the IP address for which password protection is configured.
		• The *interface* argument lists 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/not required)
		  • The password source (neighbor/fallback/number [option number])

	Command or Action	Purpose
		• 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.

Configuration Examples for MPLS LDP Lossless MD5 Session Authentication

Example: Configuring MPLS LDP Lossless MD5 Session Authentication Using a Keychain (Symmetrical)

The following example shows a configuration of two peer label switch routers (LSRs) that use symmetrical Message Digest 5 (MD5) keys:

LSR1

```
access-list 10 permit 10.2.2.2
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
 key 1
  key-string pwd1
  send-lifetime 10:00:00 Jan 1 2009 10:00:00 Feb 1 2009
  accept-lifetime 09:00:00 Jan 1 2009 11:00:00 Feb 1 2009
!
interface loopback0
  ip address 10.1.1.1 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 10.0.1.1 255.255.255.254
  mpls label protocol ldp
  mpls ip
```

LSR2

```
access-list 10 permit 10.1.1.1
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
 key 1
  key-string pwd1
  send-lifetime 10:00:00 Jan 1 2009 10:00:00 Feb 1 2009
  accept-lifetime 09:00:00 Jan 1 2009 11:00:00 Feb 1 2009
!
```

```
interface loopback0
  ip address 10.2.2.2 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 10.0.1.2 255.255.255.254
  mpls label protocol ldp
  mpls ip
```

Example: Configuring MPLS LDP Lossless MD5 Session Authentication Using a Keychain (Asymmetrical)

The following example shows a configuration of two peer label switch routers (LSRs) that use asymmetrical MD5 keys:

LSR1

```
access-list 10 permit 10.2.2.2
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
 key 1
  key-string pwd1
  accept-lifetime 00:00:00 Jan 1 2005 duration 1
  send-lifetime 10:00:00 Jan 1 2009 10:00:00 Feb 1 2009
 key 2
  key-string pwd2
  accept-lifetime 09:00:00 Jan 1 2009 11:00:00 Feb 1 2009
  send-lifetime 00:00:00 Jan 1 2005 duration 1
!
interface loopback0
  ip address 10.1.1.1 255.255.255.255
!
interface FastEthernet0/0/0
  ip address 10.0.1.1 255.255.255.254
  mpls label protocol ldp
  mpls ip
```

LSR2

```
access-list 10 permit 10.1.1.1
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
 key 1
  key-string pwd2
  accept-lifetime 00:00:00 Jan 1 2005 duration 1
  send-lifetime 10:00:00 Jan 1 2009 10:00:00 Feb 1 2009
 key 2
  key-string pwd1
  accept-lifetime 09:00:00 Jan 1 2009 11:00:00 Feb 1 2009
  send-lifetime 00:00:00 Jan 1 2005 duration 1
!
interface loopback0
  ip address 10.2.2.2 255.255.255.255
!
interface FastEthernet0/0/0
```

```
ip address 10.0.1.2 255.255.255.254
mpls label protocol ldp
mpls ip
```

Examples: Changing MPLS LDP Lossless MD5 Session Authentication Password

The following example shows the existing password configuration for LSR A, LSR B, and LSR C:

LSR A Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.11.11.11 password lab1
mpls ldp neighbor 10.12.12.12 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.10.10.10 255.255.255.255
!
interface FastEthernet1/0/0
ip address 10.2.0.1 255.255.0.0
mpls ip
!
interface FastEthernet2/0/0
ip address 10.0.0.1 255.255.0.0
mpls ip
```

LSR B Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.11.11.11 255.255.255.255
!
interface FastEthernet1/0/0
ip address 10.2.0.2 255.255.0.0
mpls ip
```

LSR C Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.12.12.12 255.255.255.255
!
interface FastEthernet2/0/0
ip address 10.0.0.2 255.255.0.0
mpls ip
!
```

The following example shows how the lossless password change is configured using the **mpls ldp password rollover duration** command for LSR A, LSR B, and LSR C so there is enough time to change all the passwords on all of the devices:

LSR A New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.11.11.11 password lab1
no mpls ldp neighbor 10.12.12.12 password lab1
```

LSR B New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.10.10.10 password lab1
```

LSR C New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.10.10.10 password lab1
```

After 10 minutes has elapsed, the password changes. The following system logging message for LSR A confirms that the password rollover was successful:

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0
```

Examples: Changing MPLS LDP Lossless MD5 Session Authentication Password Using a Rollover Without Keychain

The MPLS LDP Lossless MD5 Session Authentication password can be changed in a lossless way (without tearing down an existing Label Distribution Protocol [LDP] session) by using a password rollover without a keychain.

The following example shows the existing password configuration for LSR A and LSR B:

LSR A Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.11.11.11 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.10.10.10 255.255.255.255
!
interface FastEthernet1/0/0 ip address 10.2.0.1 255.255.0.0
mpls ip
```

LSR B Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.11.11.11 255.255.255.255
```

```
!
interface FastEthernet1/0/0
ip address 10.2.0.2 255.255.0.0
mpls ip
```

The following example shows the new password configuration for LSR A and LSR B:



Note The rollover duration should be large enough so that the passwords can be changed on all impacted devices.

LSR A New Configuration

```
mpls ldp password rollover duration 10
mpls ldp neighbor 10.11.11.11 password lab2
```

LSR B New Configuration

```
mpls ldp password rollover duration 10
mpls ldp neighbor 10.10.10.10 password lab2
```

After 10 minutes (rollover duration), the password changes and the following system logging message confirms the password rollover at LSR A:

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
```

Example: Changing MPLS LDP Lossless MD5 Session Authentication Password Using a Rollover with a Keychain

The MPLS LDP Lossless MD5 Session Authentication password can be changed in a lossless way by using a password rollover with a keychain. The following configuration example shows the new password keychain configuration for LSR A, LSR B, and LSR C, in which the new password is ldp-pwd.

In the example, the desired keychain is configured first. The first pair of keys authenticate incoming TCP segments (recv key) and compute Message Digest 5 (MD5) digests for outgoing TCP segments (xmit key). These keys should be the same keys as those currently in use; that is, in lab 1. The second recv key in the keychain should be valid after a few minutes. The second xmit key becomes valid at a future time.



Note The rollover duration should be large enough so that the passwords can be changed on all impacted devices.

LSR A New Configuration

```
mpls ldp password rollover duration 10
access-list 10 permit 10.11.11.11
access-list 10 permit 10.12.12.12
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
```

```
accept-lifetime 10:00:00 Jan 1 2009 10:45:00 Jan 1 2009
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2009 10:30:00 Feb 1 2009
accept-lifetime 10:15:00 Jan 1 2009 10:45:00 Feb 1 2009
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009
accept-lifetime 10:15:00 Feb 1 2009 10:45:00 Mar 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
no mpls ldp neighbor 10.11.11.11 password lab1
no mpls ldp neighbor 10.12.12.12 password lab1
```

LSR B New Configuration

```
mpls ldp password rollover duration 10
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
accept-lifetime 10:00:00 Jan 1 2009 10:45:00 Jan 1 2009
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2009 10:30:00 Feb 1 2009
accept-lifetime 10:15:00 Jan 1 2009 10:45:00 Feb 1 2009
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009
accept-lifetime 10:15:00 Feb 1 2009 10:45:00 Mar 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
no mpls ldp neighbor 10.10.10.10 password lab1
```

LSR C New Configuration

```
mpls ldp password rollover duration 10
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
accept-lifetime 10:00:00 Jan 1 2009 10:45:00 Jan 1 2009
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2009 10:30:00 Feb 1 2009
accept-lifetime 10:15:00 Jan 1 2009 10:45:00 Feb 1 2009
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009
accept-lifetime 10:15:00 Feb 1 2009 10:45:00 Mar 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
no mpls ldp neighbor 10.10.10.10 password lab1
```

After 10 minutes, the password changes and the following system logging message confirms the password rollover at LSR A.

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0
```

Examples: Changing MPLS LDP Lossless MD5 Session Authentication Password Using a Fallback Password with a Keychain

The MPLS LDP Lossless MD5 Session Authentication password can be changed in a lossless way by using a fallback password when doing a rollover with a keychain.



Note The fallback password is used only when there is no other keychain configured. If there is a keychain configured, then the fallback password is not used.

The following example shows the existing password configuration for LSR A, LSR B, and LSR C:

LSR A Existing Configuration

```
mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.10.10.10 255.255.255.255
!
interface FastEthernet1/0/0
ip address 10.2.0.1 255.255.0.0
mpls ip
!
interface FastEthernet2/0/0
ip address 10.0.0.1 255.255.0.0
mpls ip
!
access-list 10 permit 10.11.11.11
access-list 10 permit 10.12.12.12
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
accept-lifetime 10:00:00 Jan 1 2009 10:45:00 Jan 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR B Existing Configuration

```
mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.11.11.11 255.255.255.255
!
interface FastEthernet1/0/0
ip address 10.2.0.2 255.255.0.0
mpls ip
!
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
```

```
accept-lifetime 10:00:00 Jan 1 2009 10:45:00 Jan 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR C Existing Configuration

```
mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.12.12.12 255.255.255.255
!
interface FastEthernet2/0/0
ip address 10.0.0.2 255.255.0.0
mpls ip
!
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
accept-lifetime 10:00:00 Jan 1 2009 10:45:00 Jan 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```



Note The fallback keychain is not used unless the keychain *ldp-pwd* is removed using the **no mpls ldp password option 5 for 10 key-chain ldp-pwd** command.

The following example shows the new configuration for LSR A, LSR B, and LSR C, where one keychain is configured with the name *ldp-pwd* and another keychain is configured with the name *fallback* for the fallback password.



Note The rollover duration should be large enough so that the passwords can be changed on all impacted devices.

LSR A New Configuration

```
mpls ldp password rollover duration 10
!
key chain fallback
key 10
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR B New Configuration

```
mpls ldp password rollover duration 10
!
key chain fallback
key 10
```

```
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR C New Configuration

```
mpls ldp password rollover duration 10
key chain fallback
key 10
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd
```

After 10 minutes, the password changes and the following system logging message confirms the password rollover at LSR A:

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0
```

Examples: Changing MPLS LDP Lossless MD5 Session Authentication Common Misconfiguration

The following sections describe common misconfiguration examples that can occur when the MPLS LDP Lossless MD5 Session Authentication password is migrated in a lossless way. Misconfigurations can lead to undesired behavior in a Label Distribution Protocol (LDP) session.

Examples: Incorrect Keychain LDP Password Configuration

Possible misconfigurations can occur when keychain-based commands are used with the **mpls ldp password option for key-chain** command. If the **accept-lifetime** or **send-lifetime** command is not specified in this configuration, then a misconfiguration can occur when more than two keys are in a keychain.

The following example shows an incorrect keychain configuration with three passwords for LSR A and LSR B in the keychain:

LSR A Incorrect Keychain LDP Password Configuration

```
access-list 10 permit 10.11.11.11
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2009 10:30:00 Feb 1 2009
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR B Incorrect Keychain LDP Password Configuration

```
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2009 10:30:00 Feb 1 2009
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

In the example, for both LSR A and LSR B, during the period of the third **send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009** command, all three configured keys are valid as receive keys, and only the last configured key is valid as a transmit key. The keychain resolution rules dictate that keys 10 and 11 are used as receive keys, and only the last key 12 can be used as the transmit key. Because the transmit and receive keys are mismatched, the Label Distribution Protocol (LDP) session will not stay active.



Note When more than two passwords are configured in a keychain, the configuration needs to have both **accept-lifetime** and **send-lifetime** commands configured correctly for effective rollovers.

The following example shows the correct keychain configuration with multiple passwords in the keychain:

LSR A Correct Keychain LDP Password Configuration

```
access-list 10 permit 10.11.11.11
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
accept-lifetime 10:00:00 Jan 1 2009 10:45:00 Jan 1 2009
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2009 10:30:00 Feb 1 2009
accept-lifetime 10:15:00 Jan 1 2009 10:45:00 Feb 1 2009
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009
accept-lifetime 10:15:00 Feb 1 2009 10:45:00 Mar 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR B Correct Keychain LDP Password Configuration

```
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2009 10:30:00 Jan 1 2009
accept-lifetime 10:00:00 Jan 1 2009 10:45:00 Jan 1 2009
key 11
```

```
key-string lab2
send-lifetime 10:30:00 Jan 1 2009 10:30:00 Feb 1 2009
accept-lifetime 10:15:00 Jan 1 2009 10:45:00 Feb 1 2009
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009
accept-lifetime 10:15:00 Feb 1 2009 10:45:00 Mar 1 2009
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

In the example above, for both LSR A and LSR B, during the period of the third **send-lifetime 10:30:00 Feb 1 2009 10:30:00 Mar 1 2009** command, only the last key 12 is valid as transmit and receive keys. Therefore, the LDP session remains active.

Avoiding Access List Configuration Problems

Use caution when modifying or deleting an access list. Any empty access list implies "permit any" by default. So when either the **mpls ldp password option for key-chain** command or the **mpls ldp password option** command is used for MPLS LDP MD5 session authentication, if the access list specified in the command becomes empty as a result of a modification or deletion, then all Label Distribution Protocol (LDP) sessions on the device expect a password. This configuration may cause undesired behavior in LDP sessions. To avoid this scenario, ensure that the proper access list is specified for each label switch router (LSR).

Examples: Changing MPLS LDP Lossless MD5 Session Authentication Using a Second Key to Avoid LDP Session Failure

The MPLS LDP Lossless MD5 Session Authentication feature works when a specified rollover period is configured. Typically, one rollover period overlaps the two accept lifetime values that are configured for two consecutive receive keys. The Label Distribution Protocol (LDP) process requests an update from the keychain manager for the latest valid transmit and receive keys once every minute. LDP compares the latest key set with the keys from the previous update in its database to determine if a key was removed, changed, or rolled over. When the rollover occurs, the LDP process detects the rollover and programs TCP with the next receive key.

The LDP session can fail if LDP is configured to use two keys for the MPLS LDP Lossless MD5 Session Authentication feature where the first key uses a send and accept lifetime value and the second key is not configured. The configuration creates a special case where there are two rollovers but there is only one rollover period.

The following sections provide an example of this problem and a solution:

Example: TCP Authentication and LDP Sessions Can Fail When a Second Rollover Period Is Missing

In the following configuration, the first rollover is from "secondpass" to "firstpass." The second rollover is from "firstpass" back to "secondpass." The only rollover period in this configuration is the overlapping between the "firstpass" and "secondpass." Because one rollover period is missing, LDP performs only the first rollover and not the second rollover, causing TCP authentication to fail and the Label Distribution Protocol (LDP) session to fail.

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 01:03:00 Sep 10 2009 01:10:00 Sep 10 2009
   send-lifetime 01:05:00 Sep 10 2009 01:08:00 Sep 10 2009
```

```
 key 2
   key-string secondpass
```

TCP authentication and LDP sessions can also fail if the second key has send and accept lifetime configured. In this case the accept lifetime of the first key is a subset of the accept lifetime of the second key. For example:

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 01:03:00 Sep 10 2009 01:10:00 Sep 10 2009
   send-lifetime 01:05:00 Sep 10 2009 01:08:00 Sep 10 2009
 key 2
   key-string secondpass
   accept-lifetime 01:03:00 Sep 9 2009 01:10:00 Sep 11 2009
   send-lifetime 01:05:00 Sep 9 2009 01:08:00 Sep 11 2009
```

Examples: Reconfigure a Keychain to Prevent TCP Authentication and LDP Session Failures

If the configuration needs to specify the last key in the keychain to always be valid, then configure the keychain to have at least two keys. Each key must be configured with both the send and accept lifetime period. For example:

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 01:03:00 Sep 10 2008 01:10:00 Sep 10 2008
   send-lifetime 01:05:00 Sep 10 2008 01:08:00 Sep 10 2008
 key 2
   key-string secondpass
   accept-lifetime 01:06:00 Sep 10 2008 01:17:00 Sep 10 2008
   send-lifetime 01:08:00 Sep 10 2008 01:15:00 Sep 10 2008
 key 3
   key-string thirdpass
```

If the configuration needs to specify the first keychain for the time interval, then switch to use the second key forever after that interval. This is done by configuring the start time for the second key to begin shortly before the end time of the first key, and by configuring the second key to be valid forever after that interval. For example:

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 00:03:00 Sep 10 2008 01:10:00 Sep 10 2008
   send-lifetime 00:05:00 Sep 10 2008 01:08:00 Sep 10 2008
 key 2
   key-string secondpass
   accept-lifetime 01:06:00 Sep 10 2008 infinite
   send-lifetime 01:08:00 Sep 10 2008 infinite
```

If the configuration needs to specify the two keys in the order of the second key, first key, and second key again, then specify three keys in that order with the proper rollover period. For example:

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 00:03:00 Sep 10 2008 01:10:00 Sep 10 2008
   send-lifetime 00:05:00 Sep 10 2008 01:08:00 Sep 10 2008
 key 2
   key-string secondpass
   accept-lifetime 01:06:00 Sep 10 2008 01:17:00 Sep 10 2008
```

```
  send-lifetime 01:08:00 Sep 10 2008 01:15:00 Sep 10 2008
key 3
  key-string firstpass
  accept-lifetime 01:13:00 Sep 10 2008 infinite
  send-lifetime 01:15:00 Sep 10 2008 infinite
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
MPLS Label Distribution Protocol	"MPLS Label Distribution Protocol" module in the *MPLS Label Distribution Protocol Configuration Guide*
LDP implementation enhancements for the MD5 password	"MPLS LDP MD5 Global Configuration" module in the *MPLS Label Distribution Protocol Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MPLS LDP Lossless MD5 Session Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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