udld

To enable aggressive or normal mode in UDLD and to set the configurable message timer time, use the **udld** command. See the "Usage Guidelines" section for using the **no** form of this command.

udld {**enable** | **aggressive**}

no udld {**enable** | **aggressive**}

udld message time *message-timer-time*

no udld message time

Syntax Description

udld enable	Enables UDLD in normal mode by default on all fiber interfaces.
udld aggressive	Enables UDLD in aggressive mode by default on all fiber interfaces.
message time *message-timer-time*	Sets the period of time between UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional; valid values are from 7 to 90 seconds.

Defaults

The defaults are as follows:

- UDLD is disabled on all fiber interfaces.
- *message-timer-time* is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

Use the **no** form of this command to do the following:

- Disable normal mode UDLD on all fiber ports by default.
- Disable aggressive mode UDLD on all fiber ports by default.
- Disable the message timer.

If you enable aggressive mode, after all the neighbors of a port age out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to try to get resynchronized with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

This command affects fiber interfaces only. Use the **udld port** interface configuration mode command in Release 12.1(13)E and later releases to enable UDLD on other interface types. To enable UDLD on other interface types, use the **udld enable** interface configuration mode command in releases prior to Release 12.1(13)E.

Examples

This example shows how to enable UDLD on all fiber interfaces:

```
Router(config)# udld enable
Router(config)#
```

Related Commands

show udld
udld port

udld port

To enable UDLD on the interface or enable UDLD in aggressive mode on the interface, use the **udld port** command. Use the **no** form of this command to return to the default settings.

udld port [**aggressive**]

no udld port [**aggressive**]

Syntax Description

aggressive	(Optional) Enables UDLD in aggressive mode on this interface; see the "Usage Guidelines" section for additional information.

Defaults

The defaults for Release 12.1(13)E and later releases are as follows:

- Fiber interfaces are in the state of the global **udld** (**enable** or **aggressive**) command.
- Nonfiber interfaces have UDLD disabled.

The defaults for releases prior to Release 12.1(13)E are as follows:

- Fiber interfaces is neither **udld enable**, **udld aggressive**, nor **udld disable**. For this reason, fiber interfaces enable UDLD as per the state of the global **udld** (**enable** or **aggressive**) command.
- Nonfiber interfaces have UDLD disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(13)E	This command was changed from **udld** to **udld port**.

Usage Guidelines

This command does not appear in the CLI unless a GBIC is installed in the port you are trying to enable.

In Release 12.1(13)E and later releases, use the following syntax to enable or disable UDLD on an interface:

udld port [**aggressive**]

no udld port [**aggressive**]

Use the following guideline in Release 12.1(13)E and later releases:

- Use the **udld port** and **udld port aggressive** commands on fiber ports to override the setting of the global **udld** (**enable** or **aggressive**) command. Use the **no** form on fiber ports to remove this setting and return control of UDLD enabling back to the global **udld** command, or in the case of nonfiber ports, to disable UDLD.

In releases prior to Release 12.1(13)E, use the following syntax:

udld {**enable** | **aggressive** | **disable**}

no udld {**enable** | **aggressive** | **disable**}

Use the following guidelines in releases prior to Release 12.1(13)E:

- Use the **no udld enable** command on fiber ports to return control of UDLD to the global **udld enable** command, or in the case of nonfiber ports, to disable UDLD.
- Use the **udld aggressive** command on fiber ports to override the setting of the global **udld** (**enable** or **aggressive**) command. Use the **no** form on fiber ports to remove this setting and return control of the UDLD enabling back to the global **udld** command, or in the case of nonfiber ports, to disable UDLD.
- The **disable** keyword is supported on fiber ports with a GBIC installed only. Use the **no** form of this command to remove this setting and return control of UDLD to the global **udld** command.

If you enable aggressive mode, after all the neighbors of a port age out either in the advertisement or in the detection phase, UDLD restarts the linkup sequence to try to get resynchronized with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

If the port changes from fiber to nonfiber or vice versa, all configurations are maintained because of a change of module or a GBIC change detected by the platform software.

Examples

This example shows how to cause any port interface to enable UDLD regardless of the current global **udld** setting:

- In Release 12.1(13)E and later releases:

```
Router(config-if)# udld port
Router(config-if)#
```

- In releases prior to Release 12.1(13)E:

```
Router(config-if)# udld enable
Router(config-if)#
```

This example shows how to cause any port interface to enable UDLD in aggressive mode regardless of the current global **udld** (**enable** or **aggressive**) setting:

- In Release 12.1(13)E and later releases:

```
Router(config-if)# udld port aggressive
Router(config-if)#
```

- In releases prior to Release 12.1(13)E:

```
Router(config-if)# udld aggressive
Router(config-if)#
```

This example shows how to cause a fiber port interface to disable UDLD regardless of the current global **udld** setting:

- In Release 12.1(13)E and later releases:

```
Router (config-if)# no udld port
Router (config-if)#
```

- In releases prior to Release 12.1(13)E:

```
Router (config-if)# udld disable
Router (config-if)#
```

Related Commands **show udld**
udld

udld reset

To reset all the ports that are shut down by UDLD and permit traffic to begin passing through them again (although other features, such as spanning tree, PAGP, and DTP, will behave normally if enabled), use the **udld reset** command.

udld reset

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports will begin to run UDLD again and may shut down for the same reason if the reason for the shutdown has not been corrected.

Examples

This example shows how to reset all ports shut down by UDLD:

```
Router# udld reset
```

Related Commands

show udld

undelete

To recover a file that is marked “deleted” on a Flash file system, use the **undelete** command.

undelete *index* [*filesystem***:**]

Syntax Description

index	Number to index the file in the **dir** command output; valid values are from 1 to 1024.
*filesystem***:**	(Optional) A file system containing the file to undelete, followed by a colon; valid values are **bootflash:**, **slot0:**, **flash:**, or **sup-bootflash:**.

Defaults

The default file system is specified when you enter the **cd** command.

Command Modes

EXEC

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

For Class A and B Flash file systems, when you delete a file, the Cisco IOS software simply marks the file as deleted, but it does not erase the file. This command allows you to recover a “deleted” file on a specified Flash memory device. You must undelete a file by its index because you could have multiple deleted files with the same name. For example, the “deleted” list could contain multiple configuration files with the name router-config. You undelete by index to indicate which of the many router-config files from the list to undelete. Use the **dir** command to learn the index number of the file you want to undelete.

The **bootflash:**, **flash:**, **slot0:**, and **sup-bootflash:** keywords designate Class A file systems.

You cannot undelete a file if a valid (undeleted) file with the same name exists. Instead, you first delete the existing file and then undelete the file you want. For example, if you had an undeleted version of the router-config file and you wanted to use a previous, deleted version instead, you could not simply undelete the previous version by index. You would first delete the existing router-config file and then undelete the previous router-config file by index. You can delete and undelete a file up to 15 times.

On Class A Flash file systems, if you try to recover the configuration file pointed to by the CONFIG_FILE environment variable, the system prompts you to confirm recovery of the file. This prompt reminds you that the CONFIG_FILE environment variable points to an undeleted file. To permanently delete all files marked “deleted” on a Flash memory device, use the **squeeze** EXEC command.

On Class B Flash file systems, you must use the **erase** EXEC command to recover any space that is taken by deleted files.

Examples

This example shows how to recover the deleted file whose index number is 1 to the Flash PC card inserted in slot 0:

```
Router# undelete 1 slot0:
```

```
Router#
```

Related Commands

delete (refer to the *Cisco IOS Release 12.1 Command Reference*)
dir (refer to the *Cisco IOS Release 12.1 Command Reference*)
squeeze

upgrade rom-monitor

To set the execution preference on a ROMMON, use the **upgrade rom-monitor** command.

upgrade rom-monitor {**slot** *num*} {**sp** | **rp**} {**file** *filename*}

upgrade rom-monitor {**slot** *num*} {**sp | rp**} {{**invalidate** | **preference**} {**region1** | **region2**}}

Syntax Description

slot *num*	Slot number of the ROMMON to be upgraded.
sp	Upgrades the ROMMON of the switch processor.
rp	Upgrades the ROMMON of the route processor.
file *filename*	Specifies the name of the SREC file; see the "Usage Guidelines" section for valid values.
invalidate	Invalidates the ROMMON of the selected region.
preference	Sets the execution preference on a ROMMON of the selected region.
region1	Selects the ROMMON in region 1.
region2	Selects the ROMMON in region 2.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.
12.1(8a)EX	This command was changed to support all the devices accessible from the RP console when specifying the file path.
12.1(11b)E	This command was changed to support all the devices accessible from the SP console when specifying the file path.

Usage Guidelines

Caution If you enter the **upgrade rom-monitor** command with no parameters, service may be interrupted.

Caution If you enter the **upgrade rom-monitor** command from a Telnet session instead of a console connection, service may be interrupted.

Note Releases 12.1(8a)EX and earlier do not support the field-upgradable ROMMON feature on a Supervisor Engine 2. If you revert to a release prior to 12.1(8a)EX on a Supervisor Engine 2, the previously upgraded ROMMON will be invalidated and returned to run the ROMMON stored on the PROM. If you wish to use releases prior to 12.1(8a)EX on a Supervisor Engine 2, but upgrade your ROMMON, you must physically replace a ROMMON PROM with a ROMMON PROM programmed with the new ROMMON image. Contact Cisco TAC for additional information.

The **slot** *num* is required for this command to function properly.

The **sp** keyword is required only if a supervisor engine is installed in the specified slot.

Valid values for **file** *filename* include the following:

- **bootflash:**
- **disk0:**
- **flash:**
- **ftp:**
- **rtp:**
- **slot0:**
- **sup-bootflash:**
- **sup-slot0:**
- **tftp:**

Examples

This example shows how to upgrade the new ROMMON image to the Flash device on a Supervisor Engine 2:

```
Router# upgrade rom-monitor slot 1 sp file tftp://dirt/tftpboot-users/A2_71059.srec
ROMMON image upgrade in progress
   Erasing flash
   Programming flash
   Verifying new image
   ROMMON image upgrade complete
   The card must be reset for this to take effect
Router#
```

Related Commands

show rom-monitor

username

To establish a username-based authentication system, use the **username** command.

username *name* **secret** {**0** | **5**} *password*

Syntax Description

name	User ID.
secret 0 | **5**	Specifies the secret; valid values are **0** (text immediately following is not encrypted) and **5** (text immediately following is encrypted using an MD5-type encryption method).
password	Password.

Defaults

No username-based authentication system is established.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E3	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

Use this command to enable Enhanced Password Security for the specified, unretrievable username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method. You cannot use MD5 encryption with protocols such as CHAP that require clear-text passwords.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an “info” username that does not require a password but connects the user to a general purpose information service.

The **username** command provides username and/or secret authentication for login purposes only.

The *name* argument can be only one word. White spaces and quotation marks are not allowed.

Multiple **username** commands can be used to specify options for a single user.

For information about additional **username** commands, refer to the *Cisco IOS Release 12.1 Command Reference* publication.

Examples

This example shows how to specify an MD5 encryption on a password (warrior) for a username (xena);

```
Router(config)# username xena secret 5 warrior
Router(config)#
```

Related Commands

enable password (refer to the *Cisco IOS Release 12.1 Command Reference*)
enable secret (refer to the *Cisco IOS Release 12.1 Command Reference*)