Locking the Configuration

First Published: February 28, 2005
Last Updated: March 19, 2010

Cisco IOS software provides the user an option to lock the running configuration and prevent other users from concurrently accessing the Cisco IOS configuration. This module contains information and configuration tasks for locking the configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Locking the Configuration" section on page 11.

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

Information About Locking the Configuration

To lock the configuration, you should understand the following concepts:

Exclusive Configuration Change Access and Access Session Locking

Devices running Cisco IOS software maintain a running configuration that determines the configuration state of the device. Changes to the running configuration alter the behavior of the device. Because Cisco IOS software allows multiple users to change the running configuration via the device CLI (including the device console and telnet Secure Shell (SSH)), in some operating environments it would be beneficial to prevent multiple users from making concurrent changes to the Cisco IOS running configuration. Temporarily limiting access to the Cisco IOS running configuration prevents inadvertent conflicts or cases where two users attempt to configure the same portion of the running configuration.

The Exclusive Configuration Change Access feature (also called the “Configuration Lock” feature) allows you to have exclusive change access to the Cisco IOS running configuration, preventing multiple users from making concurrent configuration changes.

This feature provides exclusive change access to the Cisco IOS running configuration from the time you enter global configuration mode by using the **configure terminal** command. This gives the effect of a “configuration lock,” preventing other users from changing the Cisco IOS running configuration. The configuration lock is automatically released when the user exits Cisco IOS configuration mode.

The Exclusive Configuration Change Access feature is enabled using the **configuration mode exclusive** command in global configuration mode. Exclusive configuration change access can be set to **auto**, so that the Cisco IOS configuration mode is locked whenever anyone uses the **configure terminal** command, or it can be set to **manual**, so that the Cisco IOS configuration mode is locked only when the **configure terminal lock** command is issued.

The Exclusive Configuration Change Access feature is complementary with the locking mechanism for the Configuration Replace and Configuration Rollback feature introduced in Cisco IOS Release 12.2(25)S and 12.3(7)T.

Access Session Locking

The Access Session Locking feature extends the Exclusive Configuration Change Access feature such that **show** and **debug** commands entered by the user holding the configuration lock always have execution priority. This feature prevents concurrent configuration access and also provides an option to prevent simultaneous processes, such as a **show** command entered by another user, from executing while other configuration commands are being executed. When this feature is enabled, the commands entered by the user with the configuration lock (such as configuration commands) always have priority over commands entered by other users.

Parser Concurrency and Locking Improvements

In order to overcome the following limitations posed by the Exclusive Configuration Change Access feature, the Parser Concurrency and Locking Improvements feature was introduced in Cisco IOS Release 12.2(33)SRE:

- The Exclusive Configuration Change Access feature locks the configuration to other users. The lock is automatically released when the lock holder exits from the configuration mode. Any other user in the configuration mode will be returned to the EXEC mode when the lock is acquired. Also, any user can execute the **clear configuration lock** command and forcibly remove the lock and allow normal access to all users.
- The router can reload when multiple write processes belonging to the same client simultaneously access the Cisco IOS configurations in a shared mode.
- The router can reload when EXEC commands concurrently access the data structure.

Effective from Cisco IOS Release 12.2(33)SRE, the Concurrency and Locking Improvements feature is the primary locking mechanism used to prevent concurrent configuration of Cisco IOS software by multiple users.

The Parser Concurrency and Locking Improvements feature provides a common interface that ensures that exclusive access is granted to the requested process and prevents others from concurrently accessing the Cisco IOS configuration. It allows access only to the user holding the lock and prevents other clients from accessing the configuration.

Effective from Cisco IOS Release 12.2(33)SRE, the **configuration mode exclusive** {**auto** | **manual**} command will not be available to enable single-user access functionality for the Cisco IOS CLI. Use the **parser command serializer** command to enable configuration access only to the users holding the lock and prevent other clients from accessing the configuration.

How to Configure Configuration Lock

This section contains the following procedures:

- Enabling Exclusive Configuration Change Access and Access Session Locking, page 3 (required)
- Obtaining Exclusive Configuration Change Access, page 4 (optional)
- Enabling Parser Concurrency and Locking Improvements, page 5 (required)
- Monitoring and Troubleshooting Configuration Locking, page 6 (optional)

Enabling Exclusive Configuration Change Access and Access Session Locking

Note Effective with Cisco IOS Release 12.2(33)SRE, the Exclusive Configuration Change Access and Access Session Locking feature is not available in Cisco IOS software. Use the Parser Concurrency and Locking Improvements feature instead of this feature. See the "Enabling Parser Concurrency and Locking Improvements" section on page 5 for more information.

Perform this task to enable the Exclusive Configuration Change Access and Access Session Locking feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **configuration mode exclusive** {**auto** | **manual**}
4. **end**

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	**configuration mode exclusive** {**auto** | **manual**} **Example:** `Router(config)# configuration mode exclusive auto`	Enables exclusive configuration change access (configuration lock feature). • When the command is enabled, configuration sessions are performed in single-user (exclusive) mode. • The **auto** keyword automatically locks the configuration session whenever the **configure terminal** command is used. This is the default. • The **manual** keyword allows you to choose to lock the configuration session manually or leave it unlocked. If you use the **manual** keyword, you must perform the task described in the "Obtaining Exclusive Configuration Change Access" section on page 4.
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration session and returns the CLI to privileged EXEC mode.

Obtaining Exclusive Configuration Change Access

Perform this task to obtain exclusive configuration change access for the duration of your configuration session. Use of the **lock** keyword with the **configure terminal** command is necessary only if the exclusive configuration mode has been set to **manual** (see the "Enabling Exclusive Configuration Change Access and Access Session Locking" section).

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **configure terminal lock**
4. Configure the system by entering your changes to the running configuration.
5. **end**
   or
   exit

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	**configure terminal lock** **Example:** `Router(config)# configure terminal lock`	(Optional) Locks the Cisco IOS software in exclusive (single-user) mode. • This command can be used only if you have previously enabled configuration locking by using the **configuration mode exclusive** command. • This command is available in Cisco IOS Release 12.3(14)T or later releases.
Step 4	Configure the system by entering your changes to the running configuration.	—

Step 5	**end**
	or
	exit
	
	Example:
	`Router(config)# end`
	or
	
	Example:
	`Router(config)# exit`
		Ends your configuration session, automatically releases the session lock obtained in Step 1, and exits to privileged EXEC mode.
		Note Either the **end** command, the **exit** command, or the Ctrl-Z key combination releases the configuration lock. Use of the **end** command is recommended.

Enabling Parser Concurrency and Locking Improvements

Perform this task to enable configuration access only to the users holding a configuration lock and to prevent other clients from accessing the running configuration.

Restrictions

The Parser Cconcurrency and Locking Improvements feature does not allow two or more processes to exist simultaneously within the critical section of Cisco IOS configurations.

This feature flags a command to prevent its serialization if an excessive amount of time is required to generate its output or if its use produces more than 10 kilobytes of output. Examples of commands that would not be serialized are the **show terminal** and **show running-config** commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parser command serializer**
4. **exit**

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	**parser command serializer** **Example:** `Router(config)# parser command serializer`	Introduces an exclusive lock to serialize access to Cisco IOS configurations.
Step 4	**exit** **Example:** `Router(config)# exit`	(Optional) Exits global configuration mode.

Monitoring and Troubleshooting Configuration Locking

Perform either or both steps in this task to monitor or troubleshoot the Exclusive Configuration Change Access and Access Session Locking feature.

SUMMARY STEPS

1. **show configuration lock**
2. **debug configuration lock**

DETAILED STEPS

Step 1 **show configuration lock**

Use this command to display the status and details of any current configuration locks, including the owner, user, terminal, lock state, and lock class.

If you cannot enter global configuration mode, you can use this command to determine if the configuration session is locked by another user, and who that user is.

```
Router# show configuration lock

Parser Configure Lock
-----------------------------------------------------
Owner PID                          : 3
User                               : unknown
TTY                                : 0
Type                               : EXCLUSIVE
State                              : LOCKED
Class                              : EXPOSED
Count                              : 1
Pending Requests                   : 0
User debug info                    : configure terminal
Session idle state                 : TRUE
No of exec cmds getting executed   : 0
No of exec cmds blocked            : 0
Config wait for show completion    : FALSE
Remote ip address                  : Unknown
Lock active time (in Sec)          : 6
Lock Expiration timer (in Sec)     : 593
Router(config)#
```

Step 2 **debug configuration lock**

Use this command to enable debugging of Cisco IOS configuration locks (exposed class locks or rollback class locks):

```
Router# debug configuration lock

Session1 from console
==========================

Router# configure terminal lock

Configuration mode locked exclusively. The lock will be cleared once you exit out of
configuration mode using end/exit
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Parser : LOCK REQUEST in EXCLUSIVE mode
Parser: <configure terminal lock> - Config. Lock requested by process <3> client <PARSER
Client>
Parser: <configure terminal lock> - Config. Lock acquired successfully !
Router(config)#
```

Configuration Examples for Locking the Configuration

This section provides the following configuration examples:

Configuring an Exclusive Lock in Auto Mode: Example

The following example shows how to enable the exclusive lock in auto mode for single-user auto configuration mode using the **configuration mode exclusive auto** command. Once the Cisco IOS configuration file is locked exclusively, you can verify this configuration by using the **show configuration lock** command.

```
Router# configure terminal
Router(config)# configuration mode exclusive auto
Router(config)# exit

Router# configure terminal

! Locks configuration mode exclusively.

Router# show configuration lock

Parser Configure Lock

Owner PID        :  10
User             :  User1
TTY              :  3
Type             :  EXCLUSIVE
State            :  LOCKED
Class            :  Exposed
Count            :  0
Pending Requests :  0
User debug info  :  0
```

Configuring an Exclusive Lock in Manual Mode: Example

The following example shows how to enable the exclusive locking feature in manual mode by using the **configuration mode exclusive manual** command. Once you have configured manual exclusive mode, you can lock the configuration mode by using the **configure terminal lock** command. In this mode, the **configure terminal** command will not automatically lock the parser configuration mode.

```
Router# configure terminal
Router(config)# configuration mode exclusive manual
Router(config)# exit

Router# configure terminal lock

Enter configuration commands, one per line.  End with CNTL/Z.

*Mar 25 17:02:45.928:  Configuration mode locked exclusively. The lock will be cleared
once you exit out of configuration mode using end/exit
```

Configuring Parser Concurrency and Locking Improvements: Example

The following example shows how to enable the Parser Concurrency and Locking Improvements feature by using the **parser command serializer** command:

```
Router# configure terminal
Router(config)# parser command serializer
Router(config)# exit
```

Additional References

The following sections provide references related to locking the configuration.

Related Documents

Related Topic	Document Title
Commands for managing configuration files	*Cisco IOS Configuration Management Command Reference*
Information about managing configuration files	*Managing Configuration Files*

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. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Locking the Configuration

Table 1 lists the features in this module and provides links to specific configuration information.

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 1 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 1 Feature Information for Locking the Configuration

Feature Name	Releases	Feature Information
Exclusive Configuration Change Access and Access Session Locking	12.3(14)T 12.0(31)S 12.2(33)SRA 12.4(11)T 12.2(33)SXH 12.2(33)SB	The Exclusive Configuration Change Access feature (also called the "Configuration Lock" feature) allows you to have exclusive change access to the Cisco IOS running configuration, preventing multiple users from making concurrent configuration changes. The Access Session Locking addition to this feature extends the Exclusive Configuration Change Access feature such that **show** and **debug** commands entered by the user holding the configuration lock always have execution priority; **show** and **debug** commands entered by other users are allowed to run only after the processes initiated by the configuration lock owner have finished. The Exclusive Configuration Change Access feature is complementary with the locking mechanism for the Configuration Replace and Configuration Rollback feature ("rollback lock"). The Configuration Lock feature feature was integrated into Release 12.0S, and the Access Session Locking feature extension was implemented. The **configuration mode exclusive** command was extended to include the following keyword options: **config_wait**, **expire**, **interleave**, **lock-show**, **retry_wait**, and **terminate**. The output of the **show configuration lock** command was improved. The extended feature was integrated into Releases 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and 12.2(33)SB. The following sections provide information about this feature: • Information About Locking the Configuration • How to Configure Configuration Lock The following commands were introduced or modified: **clear configuration lock**, **configuration mode exclusive**, and **configure terminal lock**.
Parser Concurrency and Locking Improvements	12.2(33)SRE 15.1(1)T	The Parser Concurrency and Locking Improvements feature provides a common interface that ensures that exclusive access is granted to the requested process and prevents others from concurrently accessing the Cisco IOS configuration. It allows access only to the user holding the lock and prevents other clients from accessing the configuration. The following sections provide information about this feature: • Parser Concurrency and Locking Improvements • Enabling Parser Concurrency and Locking Improvements The following commands were introduced or modified: **parser command serializer** and **test parser session-lock**.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.