CHAPTER 4

Configuring Additional Router Features

This chapter shows you how to enter basic configurations using command-line interface (CLI).

Contents

Configuring the Domain Name and Domain Name Server

Configure a domain name and Domain Name Server (DNS) for your router to contact other devices on your network efficiently. Use the following guidelines:

- To define a default domain name that the Cisco IOS XR software uses to complete unqualified hostnames (names without a dotted-decimal domain name), use the **domain-name** command in global configuration mode.
- To specify the address of one or more name servers to use for name and address resolution, use the **domain name-server** command in global configuration mode. If no name server address is specified, the default name server is 255.255.255.255 so the DNS lookup can be broadcast to the local network segment. If a DNS server is in the local network, it replies. If not, there might be a server that knows how to forward the DNS request to the correct DNS server.
- Use the **show hosts** command in EXEC mode to display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.

To configure the DNS and DNS server, complete the following steps:

SUMMARY STEPS

1. **configure**
2. **domain name** *domain-name-of-organization*
3. **domain name-server** *ipv4-address*
4. **commit**
or
end
5. **show hosts**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`configure`**
	Example:
	`RP/0/RSP0/CPU0:router# configure`
		Enters global configuration mode.

Step 2	**`domain name`** *`domain-name-of-organization`*
	Example:
	`RP/0/RSP0/CPU0:router(config)# domain name cisco.com`
		Defines a default domain name used to complete unqualified hostnames.

Step 3	**`domain name-server`** *`ipv4-address`*
	Example:
	`RP/0/RSP0/CPU0:router(config)# domain name-server 192.168.1.111`
		Specifies the address of a name server to use for name and address resolution (hosts that supply name information).
		Note You can enter up to six addresses, but only one for each command.

	Command or Action	Purpose

Step 4	**`end`**
	`or`
	`commit`
	
	Example:
	`RP/0/RSP0/CPU0:router(config)# end`
	`or`
	`RP/0/RSP0/CPU0:router(config)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)?`
		`[cancel]:`
		– Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		– Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		– Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Step 5	**`show hosts`**
	
	Example:
	`RP/0/RSP0/CPU0:router(config)# show hosts`
		Displays all configured name servers.

Examples

In the following example, the domain name and DNS are configured:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# domain name cisco.com
RP/0/RSP0/CPU0:router(config)# domain name-server 10.1.1.1
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router(config)# end
RP/0/RSP0/CPU0:router# show hosts

Default domain is cisco.com
Name/address lookup uses domain service
Name servers: 10.1.1.1
```

Configuring Telnet and XML Host Services

For security, some host services are disabled by default. You can enable Host services, such as Telnet and Extensible Markup Language (XML), using the commands in this section. Enabling the Telnet server allows users to log in to the router using IPv4 Telnet clients.

Prerequisites

Ensure the following prerequisites are met before configuring Telnet and XML host services:

- For the XML host services, the Manageability package must be installed and activated on the router.
- To enable the Secure Socket Layer (SSL) of the XML services, the Security package must be installed and activated on the router.

See *Cisco ASR 9000 Series Aggregation Series Router System Management Configuration Guide* for information on installing and activating packages.

Note This process enables the Telnet and XML host services on the Management Ethernet interfaces. For more information on how to enable these services on other inband interfaces, refer to the *Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*.

SUMMARY STEPS

1. **configure**
2. **telnet ipv4 server max-servers** *limit*
3. **end** or **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure** **Example:** RP/0/RSP0/CPU0:router# configure	Enters global configuration mode.
Step 2	**telnet ipv4 server max-servers** *limit* **Example:** RP/0/RSP0/CPU0:router(config)# telnet ipv4 server max-servers 5	Enables Telnet services on the router and specifies the maximum number of allowable Telnet servers.
Step 3	**end** or **commit** **Example:** RP/0/RSP0/CPU0:router(config)# end or RP/0/RSP0/CPU0:router(config)# commit	Saves configuration changes. • When you issue the **end** command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: – Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Examples

In the following example, the host services are enabled:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# telnet ipv4 server max-servers 5
RP/0/RSP0/CPU0:router(config)# http server
RP/0/RSP0/CPU0:router(config)# commit
```

Related Documents

Related Topic	Document Title
Installation and activation of the Manageability and Security Packages	*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*
Descriptions of the XML server commands	*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*

Managing Configuration History and Rollback

After each commit operation, the system saves a record of committed configuration changes. This record has only changes made during the configuration session; it does not contain the complete configuration. Each record is assigned a unique ID, a *commitID*. Using a commitID you can:

- Identify the previous configuration to which to return. Before rolling back the configuration to a specific commitID, consider the following:
  - You cannot roll back to a configuration removed because of package incompatibility. Configuration rollbacks only succeed when the configuration passes all compatibility checks with the active Cisco IOS XR Software release.
  - If the system finds an incompatible configuration during rollback, the operation fails and an error appears.
- Load configuration changes made during a configuration session
- Load configuration changes from multiple commitIDs
- Clear commitIDs

Cisco IOS XR automatically saves up to 100 of the most recent commitIDs.

The following sections describe how to manage configuration changes and roll back to a previously committed configuration:

- Viewing CommitIDs, page 4-7
- Viewing Configuration Changes Recorded in a CommitID, page 4-7
- Previewing Rollback Configuration Changes, page 4-8
- Rolling Back the Configuration to a Specific Rollback Point, page 4-8
- Rolling Back the Configuration over a Specified Number of Commits, page 4-9
- Loading CommitID Configuration Changes to the Target Configuration, page 4-9
- Loading Rollback Configuration Changes to the Target Configuration, page 4-10
- Deleting CommitIDs, page 4-11

Viewing CommitIDs

To view up to 100 of the most recent commitIDs, type the **show configuration commit list** command in EXEC or administration EXEC mode. Up to 100 of the most recent commitIDs are saved by the system. Each commitID entry shows the user who committed configuration changes, the connection used to execute the commit, and commitID time stamp.

The commitIDs are shown in the "Label/ID" column. The following example shows the **show configuration commit list** command display in EXEC and administration EXEC modes:

```
RP/0/RSP1/CPU0:router# show configuration commit list

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    1000000219  cisco     vty0        CLI         12:27:50 UTC Wed Mar 22 2008
2    1000000218  cisco     vty1        CLI         11:43:31 UTC Mon Mar 20 2008
3    1000000217  cisco     con0_RSP0_C  CLI         17:44:29 UTC Wed Mar 15 2008

RP/0/RSP1/CPU0:router# admin
RP/0/RSP1/CPU0:router(admin)# show configuration commit list

SNo. Label/ID    User      Line        Client      Time Stamp
~~~~ ~~~~~~~~    ~~~~      ~~~~        ~~~~~~      ~~~~~~~~~~
1    2000000022  cisco     vty1        CLI         15:03:59 UTC Fri Mar 17 2008
2    2000000021  cisco     con0_RSP0_C  CLI         17:42:55 UTC Wed Mar 15 2008
3    2000000020  SYSTEM    con0_RSP0_C  Setup Dial  17:07:39 UTC Wed Mar 15 2008
```

Viewing Configuration Changes Recorded in a CommitID

To view the configuration changes made during a specific commit session (commitID), go to EXEC or administration EXEC mode and type the **show configuration commit changes** command followed by a commitID number. The easiest way to determine the commitID is to type the **show configuration commit changes ?** command first. In the following example, the command help is used to display the available commitIDs, and then the changes for a specific commitID are displayed:

```
RP/0/RSP1/CPU0:router(admin)# show configuration commit changes ?

  last        Changes made in the most recent <n> commits
  since       Changes made since (and including) a specific commit
  2000000020  Commit ID
  2000000021  Commit ID
  2000000022  Commit ID

RP/0/RSP1/CPU0:router(admin)# show configuration commit changes 2000000020

Building configuration...
username cisco
 secret 5 $1$MgUH$xzUEW6jLfyAYLKJE.3p440
 group root-system
!
end
```

Previewing Rollback Configuration Changes

The **show configuration rollback changes** command allows you to preview the configuration changes that take place if you roll back the configuration to a specific commitID. For example, if you want to roll back the configuration to a specific point, all configuration changes made after that point must be undone. This rollback process is often accomplished by executing the **no** version of commands that must be undone.

To display the prospective rollback configuration changes from the current configuration to a specific commitID, go to EXEC or administration EXEC mode and type the **show configuration rollback changes to** *commitId* command. In the following example, the command help displays the available commitIDs, and then the rollback changes are displayed.

```
RP/0/RSP1/CPU0:router# show configuration rollback changes to ?

  1000000217  Commit ID
  1000000218  Commit ID
  1000000219  Commit ID

RP/0/RSP1/CPU0:router# show configuration rollback changes to 1000000218

Building configuration...
no interface Loopback100
interface Gi0/1/0/0
 no ipv4 nd dad attempts
!
!
no route-policy xx
end
```

To display the prospective rollback configuration changes from the current configuration to a specified number of previous sessions, go to EXEC or administration EXEC mode and type the **show configuration rollback changes last** *commit-range* command:

```
RP/0/RSP0/CPU0:router# show configuration rollback changes last 2

Building configuration...
interface Loopback3
no description
no ipv4 address 10.0.1.1 255.0.0.0
exit
interface Loopback4
no description
no ipv4 address 10.0.0.1 255.0.0.0
end
```

In the preceding example, the command display shows the proposed rollback configuration changes for the last two commit IDs.

Rolling Back the Configuration to a Specific Rollback Point

When you roll back the configuration to a specific rollback point, you undo all configuration changes made during the session identified by the commit ID for that rollback point, and you undo all configuration changes made after that point. The rollback process rolls back the configuration and commits the rolled-back configuration. The rollback process also creates a new rollback point so that you can roll back the configuration to the previous configuration.

Tip To preview the commands that undo the configuration during a rollback, use the **show configuration rollback changes** command.

To roll back the router configuration to a previously committed configuration, go to EXEC or administration EXEC mode and type the **rollback configuration to** *commitId* command:

```
RP/0/RSP1/CPU0:router# rollback configuration to 1000000220
Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.
2 items committed in 1 sec (1)items/sec
Updating.
Updated Commit database in 1 sec
Configuration successfully rolled back to '1000000220'.
```

Rolling Back the Configuration over a Specified Number of Commits

When you roll back the configuration over a specific number of commits, you do not have to enter a specific commit ID. Instead, you specify a number *x*, and the software undoes all configuration changes made in the last *x* committed configuration sessions. The rollback process rolls back the configuration, commits the rolled-back configuration, and creates a new commitID for the previous configuration.

Tip To preview the commands that undo the configuration during a rollback, use the **show configuration rollback changes** command.

To roll back to the last *x* commits made, go to EXEC or administration EXEC mode and type the **rollback configuration last** *x* command; *x* is a number ranging from 1 to the number of saved commits in the commit database.

In the following example, a request is made to roll back the configuration changes made during the previous two commits:

```
RP/0/RSP0/CPU0:router# rollback configuration last 2

Loading Rollback Changes.
Loaded Rollback Changes in 1 sec
Committing.
1 items committed in 1 sec (0)items/sec
Updating.
Updated Commit database in 1 sec
Configuration successfully rolled back 2 commits.
```

Loading CommitID Configuration Changes to the Target Configuration

If the changes saved for a specific commitID are close to what you want, but a rollback is not appropriate, you can load the configuration changes for a commitID into the target configuration, modify the target configuration, and then commit the new configuration. Unlike the rollback process, the loaded changes are not applied until you commit them.

Note Unlike the rollback process, loading the commitID configuration changes loads only the changes made during that commit operation. The load process does not load all changes made between the commitID and the current committed configuration.

To load commitID changes in the target configuration, go to global configuration or administration configuration mode and type the **load commit changes** command with the commitID number. In the following example, show commands are used to display the changes for a commitID, the commitID configuration is loaded into the target configuration, and the target configuration appears:

```
RP/0/RSP1/CPU0:router# show configuration commit changes ?

  last        Changes made in the most recent <n> commits
  since       Changes made since (and including) a specific commit
  1000000217  Commit ID
  1000000218  Commit ID
  1000000219  Commit ID
  1000000220  Commit ID
  1000000221  Commit ID

RP/0/RSP1/CPU0:router# show configuration commit changes 1000000219
Building configuration...
interface Loopback100
!
interface Gi0/1/0/0
 ipv4 nd dad attempts 50
!
end

RP/0/RSP1/CPU0:router# config

RP/0/RSP1/CPU0:router(config)# load commit changes 1000000219
Building configuration...
Loading.
77 bytes parsed in 1 sec (76)bytes/sec

RP/0/RSP1/CPU0:router(config)# show configuration

Building configuration...
interface Loopback100
!
interface Gi0/1/0/0
 ipv4 nd dad attempts 50
!
end
```

Loading Rollback Configuration Changes to the Target Configuration

If the changes for a specific rollback point are close to what you want, but a rollback is not appropriate, you can load the rollback configuration changes into the target configuration, modify the target configuration, and then commit the new configuration. Unlike the rollback process, the loaded changes are not applied until you commit them.

Tip To display the rollback changes, type the **show configuration rollback changes** command.

To load rollback configuration changes from the current configuration to a specific session, go to global configuration or administration configuration mode and type the **load rollback changes to** *commitId* command:

```
RP/0/RSP0/CPU0:router(config)# load rollback changes to 1000000068

Building configuration...
Loading.
233 bytes parsed in 1 sec (231)bytes/sec
```

To load rollback configuration changes from the current configuration to a specified number of previous sessions, go to global configuration or administration configuration mode and type the **load rollback changes last** *commit-range* command:

```
RP/0/RSP0/CPU0:router(config)# load rollback changes last 6

Building configuration...
Loading.
221 bytes parsed in 1 sec (220)bytes/sec
```

In the preceding example, the command loads the rollback configuration changes for the last six commitIDs.

To load the rollback configuration for a specific commitID, go to global configuration or administration configuration mode and type the **load rollback changes** *commitId* command:

```
RP/0/RSP0/CPU0:router(config)# load rollback changes 1000000060

Building configuration...
Loading.
199 bytes parsed in 1 sec (198)bytes/sec
```

Deleting CommitIDs

You can delete the oldest configuration commitIDs by entering the **clear configuration commit** command in EXEC or administration EXEC mode. The **clear configuration commit** command must be followed by either the amount of disk space you want to reclaim or number of commitIDs you want to delete. To reclaim disk space from the oldest commitIDs, type the **clear configuration commit** command followed by the keyword **diskspace** and number of kilobytes to reclaim:

```
RP/0/RSP0/CPU0:router# clear configuration commit diskspace 50

Deleting 4 rollback points '1000000001' to '1000000004'
64 KB of disk space will be freed. Continue with deletion?[confirm]
```

To delete a specific number of the oldest commitIDs, type the **clear configuration commit** command followed by the keyword **oldest** and number of commitIDs to delete:

```
RP/0/RSP0/CPU0:router# clear configuration commit oldest 5

Deleting 5 rollback points '1000000005' to '1000000009'
80 KB of disk space will be freed. Continue with deletion?[confirm]
```

Configuring Logging and Logging Correlation

System messages generated by the Cisco IOS XR software can be logged to a variety of locations based on the severity level of the messages. For example, you could direct information messages to the system console and also log debugging messages to a network server.

In addition, you can define correlation rules that group and summarize related events, generate complex queries for the list of logged events, and retrieve logging events through an XML interface.

The following sections describe logging and the basic commands used to log messages in Cisco IOS XR software:

- Logging Locations and Severity Levels, page 4-12
- Alarm Logging Correlation, page 4-13
- Configuring Basic Message Logging, page 4-13
- Disabling Console Logging, page 4-15

Logging Locations and Severity Levels

Error messages can be logged to a variety of locations, as shown in Table 4-1.

Table 4-1 Logging Locations for System Error Messages

Logging Destination	Command (Global Configuration Mode)
console	**logging console**
vty terminal	**logging monitor**
external syslog server	**logging trap**
internal buffer	**logging buffered**

You can log messages based on the severity level of the messages, as shown in Table 4-2.

Table 4-2 Logging Severity Levels for System Error Messages

Level	Description
Level 0—Emergencies	System has become unusable.
Level 1—Alerts	Immediate action needed to restore system stability.
Level 2—Critical	Critical conditions that may require attention.
Level 3—Errors	Error conditions that may help track problems.
Level 4—Warnings	Warning conditions that are not severe.
Level 5—Notifications	Normal but significant conditions that bear notification.
Level 6—Informational	Informational messages that do not require action.
Level 7—Debugging	Debugging messages are for system troubleshooting only.

Alarm Logging Correlation

Alarm logging correlation is used to group and filter similar messages to reduce the amount of redundant logs and isolate the root causes of the messages.

For example, the original message describing the online insertion and removal (OIR) and system state being up or down can be reported, and all subsequent messages reiterating the same event can be correlated. When you create correlation rules, a common root event that is generating larger volumes of follow-on error messages can be isolated and sent to the correlation buffer. An operator can extract all correlated messages for display later, should the need arise. See *Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide* for more information.

Configuring Basic Message Logging

Numerous options for logging system messages in Cisco IOS XR software are available. This section provides a basic example.

To configure basic message logging, complete the following steps:

SUMMARY STEPS

1. **configure**
2. **logging** {*ip-address* | *hostname*}
3. **logging trap** *severity*
4. **logging console** [*severity*]
5. **logging buffered** [*severity* | *buffer-size*]
6. **commit**
7. **end**
8. **show logging**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`configure`**
	Example:
	`RP/0/RSP0/CPU0:router# configure`
		Enters global configuration mode.

Step 2	**`logging`** `{`*`ip-address`*` | `*`hostname`*`}`
	Example:
	`RP/0/RSP0/CPU0:router(config)# logging 10.1.1.1`
		Specifies a syslog server host to use for system logging.

Step 3	**`logging trap`** *`severity`*
	Example:
	`RP/0/RSP0/CPU0:router(config)# logging trap debugging`
		Limits the logging of messages sent to syslog servers to only those messages at the specified level.
		• See Table 4-2 for a summary of the logging severity levels.

	Command or Action	Purpose
Step 4	**logging console** [*severity*] **Example:** `RP/0/RSP0/CPU0:router(config)# logging console emergencies`	Logs messages on the console. • When a severity level is specified, only messages at that severity level are logged on the console. • See Table 4-2 for a summary of the logging severity levels.
Step 5	**logging buffered** [*severity* | *buffer-size*] **Example:** `RP/0/RSP0/CPU0:router(config)# logging buffered 1000000`	Copies logging messages to an internal buffer. • Newer messages overwrite older messages after the buffer is filled. • Specifying a severity level causes messages at that level and numerically lower levels to be logged in an internal buffer. See Table 4-2 for a summary of the logging severity levels. • The buffer size is from 4096 to 4,294,967,295 bytes. Messages above the set limit are logged to the console.
Step 6	**commit** **Example:** `RP/0/RSP0/CPU0:router(config)# commit`	Commits the target configuration to the router running configuration.

Step 7	**end**
	Example:
	`RP/0/RSP0/CPU0:router(config)# end`
		Ends the configuration session and returns to EXEC mode.

Step 8	**show logging** **Example:** `RP/0/RSP0/CPU0:router# show logging`	Displays the messages that are logged in the buffer.

Examples

In the following example, basic message logging is configured:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# logging 10.1.1.1
RP/0/RSP0/CPU0:router(config)# logging trap debugging
RP/0/RSP0/CPU0:router(config)# logging console emergencies
RP/0/RSP0/CPU0:router(config)# logging buffered 1000000
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router(config)# end
RP/0/RSP0/CPU0:router# show logging

Syslog logging: enabled (162 messages dropped, 0 flushes, 0 overruns)
    Console logging: level emergencies, 593 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level debugging, 2 messages logged
    Logging to 10.1.1.1, 2 message lines logged
    Buffer logging: level debugging, 722 messages logged

Log Buffer (1000000 bytes):
```

```
RP/0/RSP0/CPU0:Apr  8 19:18:58.679 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
RP/0/RSP0/CPU0:Apr  8 19:19:01.287 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
RP/0/RSP0/CPU0:Apr  8 19:22:15.658 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
LC/0/1/CPU0:Apr  8 19:22:30.122 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_NOTIFICATION
LC/0/6/CPU0:Apr  8 19:22:30.160 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_NOTIFICATION
RP/0/RSP0/CPU0:Apr  8 19:22:30.745 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_NOTIFICATI
RP/0/RSP1/CPU0:Apr  8 19:22:32.596 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_NOTIFICATI
LC/0/1/CPU0:Apr  8 19:22:35.181 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_FINISHED : s
LC/0/6/CPU0:Apr  8 19:22:35.223 : sysmgr[74]: %OS-SYSMGR-7-INSTALL_FINISHED : s
RP/0/RSP0/CPU0:Apr  8 19:22:36.122 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_FINISHED :
RP/0/RSP1/CPU0:Apr  8 19:22:37.790 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_FINISHED :
RP/0/RSP0/CPU0:Apr  8 19:22:41.015 : schema_server[332]: %MGBL-SCHEMA-6-VERSIONC
RP/0/RSP0/CPU0:Apr  8 19:22:59.844 : instdir[203]: %INSTALL-INSTMGR-4-ACTIVE_SOF
RP/0/RSP0/CPU0:Apr  8 19:22:59.851 : instdir[203]: %INSTALL-INSTMGR-6-INSTALL_OP
 --More--
```

Related Documents

Related Topic	Document Title
Configuration of system logging	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Configuration Guide*
Commands used to configure logging	*Cisco ASR 9000 Series Aggregation Services Router System Monitoring Command Reference*
Configuration of alarm correlation and generating complex queries	*Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*
Commands used to configure alarm correlation	*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*
Retrieve logging events through an XML interface	*Cisco ASR 9000 Series Aggregation Services Router XML API Guide*

Disabling Console Logging

To disable console logging, type the **logging console disable** command in global configuration mode.

Creating and Modifying User Accounts and User Groups

In the Cisco IOS XR software, users are assigned individual usernames and passwords. Each username is assigned to one or more user groups, each of which defines display and configuration commands the user is authorized to execute. This authorization is enabled by default in the Cisco IOS XR software, and each user must log in to the system using a unique username and password.

The following sections describe the basic commands used to configure users and user groups:

- Viewing Details About User Accounts, User Groups, and Task IDs, page 4-16
- Configuring User Accounts, page 4-17
- Creating Users and Assigning Groups, page 4-17

For a summary of user accounts, user groups, and task IDs, see the "User Groups, Task Groups, and Task IDs" section on page 3-7

Note The management of user accounts, user groups, and task IDs is part of the authentication, authorization, and accounting (AAA) feature. AAA is a suite of security features in the Cisco IOS XR software. For more information on the AAA, see the *Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide* and *Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference.* For instructions to activate software packages, see *Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*.

Viewing Details About User Accounts, User Groups, and Task IDs

Table 4-3 summarizes the EXEC mode commands used to display details about user accounts, user groups, and task IDs.

Table 4-3 Commands to Display Details About Users and User Groups

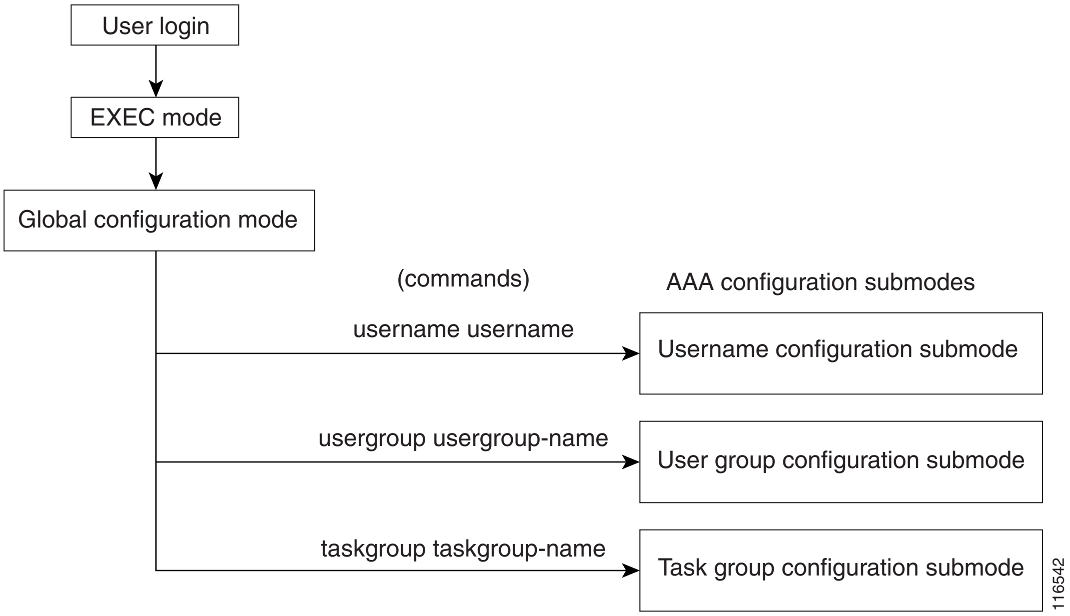
Command	Description
show aaa userdb *username*	Displays the task IDs and privileges assigned to a specific username. To display all users on the system, type the command without a username.
show aaa usergroup *usergroup-name*	Displays the task IDs and privileges that belong to a user group. To display all groups on the system, type the command without a group name.

Configuring User Accounts

User accounts, user groups, and task groups are created by entering the appropriate commands in one of the AAA configuration submodes, as shown in Figure 4-1.

This section describes the process to configure usernames. For instructions to configure user groups, task groups, and other AAA security features, see the *Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide.*

Figure 4-1 AAA Configuration Submodes


User login
EXEC mode
Global configuration mode
(commands)
AAA configuration submodes
username username
Username configuration submode
usergroup usergroup-name
User group configuration submode
taskgroup taskgroup-name
Task group configuration submode
116542

Creating Users and Assigning Groups

To create a user, assign a password, and assign the user to a group, perform the following procedure.

SUMMARY STEPS

1. **configure**
2. **username** *user-name*
3. **password** {**0** | **7**} *password*
   or
   secret {**0** | **5**} *password*
4. **group** *group-name*
5. Repeat Step 4 for each user group to be associated with the user specified in Step 2.
6. **commit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`configure`**
	Example:
	`RP/0/RSP0/CPU0:router# configure`
		Enters global configuration mode.

Step 2	**`username`** *`user-name`*
	Example:
	`RP/0/RSP0/CPU0:router(config)# username user1`
		Creates a name for a new user (or identifies a current user) and enters username configuration submode.
		• The *user-name* argument can be only one word. Spaces and quotation marks are not allowed.

Step 3	**`password`** `{`**`0`** `|` **`7`**`}` *`password`*
	or
	`secret` `{`**`0`** `|` **`5`**`}` *`password`*
	Example:
	`RP/0/RSP0/CPU0:router(config-un)# password 0 pwd1`
	or
	`RP/0/RSP0/CPU0:router(config-un)# secret 5 pwd1`
		Specifies a password for the user named in Step 2.
		• Use the **secret** command to create a secure login password for the user names specified in Step 2.
		• Entering **0** following the **password** command specifies that an unencrypted (clear-text) password follows. Entering **7** following the **password** command specifies that an encrypted password follows.
		• Entering **0** following the **secret** command specifies that a secure unencrypted (clear-text) password follows. Entering **5** following the **secret** command specifies that a secure encrypted password follows.
		• Type **0** is the default for the **password** and **secret** commands.

Step 4	**`group`** *`group-name`*
	Example:
	`RP/0/RSP0/CPU0:router(config-un)# group sysadmin`
		Assigns the user named in Step 2 to a user group.
		• The user takes on all attributes of the user group, as defined by the user group association to various task groups.
		• Each user must be assigned to at least one user group. A user may belong to multiple user groups.

Step 5	Repeat Step 4 for each user group to be associated with the user specified in Step 2.	—

Step 6	**`commit`**
	Example:
	`RP/0/RSP0/CPU0:router(config-un)# commit`
		Saves configuration changes and activates them as part of the running configuration.

Related Documents

Related Topic	Document Title
Create users, assign users to user groups, create and modify user groups, and configure remote AAA access	*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*

Configuring Software Entitlement

Certain software and hardware features are enabled using software entitlement, which is a system that consists of a license manager on a Cisco IOS XR device that manages licenses for various software and hardware features. The license manager parses and authenticates a license before accepting it. The software features on the router use the license manager APIs to check out and release licenses. Licenses are stored in persistent storage on the router.

All core routing features are available for use without any license. In Cisco IOS XR Software Release 3.7, the following features must be enabled with licenses:

- Layer 3 VPN
- Modular services card bandwidth

Refer to the *Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide* for more information on configuring software licenses.

Configuration Limiting

The Cisco IOS XR software places preset limits on the configurations you can apply to the running configuration of a router. These limits ensure that the router has sufficient system resources (such as RAM) for normal operations. Under most conditions, these preset limits are sufficient.

In some cases, for which a large number of configurations is required for a particular feature, it may be necessary to override the preset configuration limits. This override can be done only if configurations for another feature are low or unused.

Caution Overriding the default configuration limits can result in a low-memory condition.

The following sections describe the limits you can configure, default and maximum values, and commands for configuring and displaying the configuration limits:

- Static Route Configuration Limits, page 4-20
- IS-IS Configuration Limits, page 4-20
- OSPFv2 and v3 Configuration Limits, page 4-21
- Routing Policy Language Line and Policy Limits, page 4-23
- Multicast Configuration Limits, page 4-25
- MPLS Configuration Limits, page 4-26
- Other Configuration Limits, page 4-26

Static Route Configuration Limits

Table 4-4 summarizes the maximum limits for static routes, including the commands used to display and change the limits.

Table 4-4 Static Route Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Static Router Configuration Mode)	Show Current Settings Command (EXEC or Global Configuration Mode)
Maximum static IPv4 routes	4000	40,000	**maximum path ipv4** *n*	**show running-config router static**

Examples

In the following example, the maximum number of static IPv4 routes is changed to 5000 and the new configuration appears.

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router static
RP/0/RSP1/CPU0:router(config-static)# maximum path ipv4 5000
RP/0/RSP1/CPU0:router(config-static)# commit
RP/0/RSP1/CPU0:router(config-static)# show running-config router static

router static
 maximum path ipv4 5000
 address-family ipv4 unicast
  0.0.0.0/0 172.29.52.1
 !
!
```

IS-IS Configuration Limits

Table 4-5 summarizes the maximum limits for Intermediate System to Intermediate System (IS-IS) routing protocol, including the commands used to display and change the limits.

Table 4-5 IS-IS Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Address Family Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum number of prefixes redistributed into IS-IS	10,000	28,000	**maximum-redistributed-prefixes** *n*	**show isis adjacency**
Number of active parallel paths for each route on a Cisco ASR 9000 Series Router	8	32	**maximum-paths** *n*	**show isis route**

Examples

In the following example, the maximum number of active parallel paths for each route is increased to 10, and the maximum number of prefixes redistributed into IS-IS is increased to 12,000:

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router isis 100 address-family ipv4
RP/0/RSP1/CPU0:router(config-isis-af)# maximum-paths 10
RP/0/RSP1/CPU0:router(config-isis-af)# maximum-redistributed-prefixes 12000
RP/0/RSP1/CPU0:router(config-isis-af)# commit
RP/0/RSP1/CPU0:Mar 30 14:11:07 : config[65739]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'cisco'.   Use 'show configuration commit changes 1000000535' to view
the changes.
RP/0/RSP1/CPU0:router(config-isis-af)#
```

OSPFv2 and v3 Configuration Limits

Table 4-6 summarizes the maximum limits for Open Shortest Path First (OSPF) protocol, including the commands used to display and change the limits.

Table 4-6 OSPFv2 Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Router Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum number of interfaces that can be configured for an OSPF instance	255	1024	**maximum interfaces** *n*	**show ospf**
Maximum routes redistributed into OSPF	10,000	4294967295	**maximum redistributed-prefixes** *n*	**show ospf** **Note** The maximum number of redistributed prefixes appear only if redistribution is configured.
Maximum number of parallel routes (maximum paths) on Cisco ASR 9000 Series routers	32	32	**maximum paths** *n*	**show running-config router ospf** **Note** This command shows only changes to the default value. If the **maximum paths** command does not appear, the router is set to the default value.

Examples

The following examples illustrate OSPF configuration limits:

- Maximum Interfaces for Each OSPF Instance: Example, page 4-22
- Maximum Routes Redistributed into OSPF: Example, page 4-22
- Number of Parallel Links (max-paths): Example, page 4-23

Maximum Interfaces for Each OSPF Instance: Example

In the following example, the **show ospf** command is used to display the maximum number of OSPF interfaces:

```
RP/0/RSP1/CPU0:router# show ospf

 Routing Process "ospf 100" with ID 0.0.0.0
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 500 msecs
 Minimum hold time for LSA throttle 5000 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Maximum number of configured interfaces 255
--More--
```

The following example configures the maximum interface limit on a router:

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router ospf 100
RP/0/RSP1/CPU0:router(config-router)# maximum interfaces 600
RP/0/RSP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y

RP/0/RSP1/CPU0:Mar 30 16:12:39 : config[65740]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'cisco'.   Use 'show configuration commit changes 1000000540' to view
the changes.
RP/0/RSP1/CPU0:Mar 30 16:12:39 : config[65740]: %SYS-5-CONFIG_I : Configured from console
by cisco

RP/0/RSP1/CPU0:router# show ospf

 Routing Process "ospf 100" with ID 0.0.0.0
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 500 msecs
 Minimum hold time for LSA throttle 5000 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Maximum number of configured interfaces 600
--More--
```

Maximum Routes Redistributed into OSPF: Example

In the following example, the **maximum redistributed-prefixes** command is used to set the maximum routes redistributed into OSPF:

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router ospf 100
RP/0/RSP1/CPU0:router(config-router)# maximum redistributed-prefixes 12000
RP/0/RSP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y
```

```
RP/0/RSP1/CPU0:Mar 30 16:26:52 : config[65740]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'cisco'.   Use 'show configuration commit changes 1000000541' to view
the changes.
RP/0/RSP1/CPU0:Mar 30 16:26:52 : config[65740]: %SYS-5-CONFIG_I : Configured from console
by cisco
RP/0/RSP1/CPU0:router#
```

Number of Parallel Links (max-paths): Example

In the following example, the **maximum paths** command is used to set the maximum number of parallel routes:

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# router ospf 100
RP/0/RSP1/CPU0:router(config-router)# maximum paths 10
RP/0/RSP1/CPU0:router(config-router)# end
Uncommitted changes found, commit them? [yes]: y

RP/0/RSP1/CPU0:Mar 30 18:05:13 : config[65740]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'cisco'.   Use 'show configuration commit changes 1000000542' to view
the changes.
RP/0/RSP1/CPU0:Mar 30 18:05:13 : config[65740]: %SYS-5-CONFIG_I : Configured from console
by cisco
RP/0/RSP1/CPU0:router#
```

Routing Policy Language Line and Policy Limits

Two limits for Routing Policy Language (RPL) configurations exist:

1. Number of RPL lines: The number of configuration lines entered by the user, including the beginning and ending statements (that is “route-policy”). The number of configuration lines for sets is also included.
2. Number of RPL policies: The number of policies that can be configured on the router. Policies are counted only once: Multiple use of the same policy counts as a single policy toward the limit 1.

The limits for RPL lines and policies are summarized in Table 4-7. You can change the default values up to the absolute maximum, but you cannot change the value to a number less than the number of items that are currently configured.

Table 4-7 Maximum Lines of RPL: Configuration Limits and Commands

Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Global Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum number of RPL lines	65,536	131,072	**rpl maximum lines** *n*	**show rpl maximum lines**
Maximum number of RPL policies	3500	5000	**rpl maximum policies** *n*	**show rpl maximum policies**

Examples

In the following example, the **show rpl maximum** command is used in EXEC mode to display the current setting for RPL limits and number of each limit currently in use. A summary of the memory used by all of the defined policies is also shown below the limit settings.

```
RP/0/RSP1/CPU0:router# show rpl maximum

                             Current    Current       Max
                              Total      Limit       Limit
------------------------------------------------------------
Lines of configuration             0      65536     131072
Policies                           0       3500       5000
Compiled policies size (kB)        0
RP/0/RSP1/CPU0:router#
```

In the next example, the **rpl maximum** command changes the currently configured line and policy limits. The **show rpl maximum** command displays the new settings.

```
RP/0/RSP1/CPU0:router# configure
RP/0/RSP1/CPU0:router(config)# rpl maximum policies 4000
RP/0/RSP1/CPU0:router(config)# rpl maximum lines 80000
RP/0/RSP1/CPU0:router(config)# commit

RP/0/RSP1/CPU0:Apr  1 00:23:44.062 : config[65709]: %LIBTARCFG-6-COMMIT : Configuration
committed by user 'UNKNOWN'.   Use 'show configuration commit changes 1000000010' to view
the changes.
RP/0/RSP1/CPU0:router(config)# exit

RP/0/RSP1/CPU0:Apr  1 00:23:47.781 : config[65709]: %SYS-5-CONFIG_I : Configured from
console by console

RP/0/RSP1/CPU0:router# show rpl maximum

                             Current    Current       Max
                              Total      Limit       Limit
------------------------------------------------------------
Lines of configuration             0      80000     131072
Policies                           0       4000       5000
Compiled policies size (kB)        0
RP/0/RSP1/CPU0:router#
```

Multicast Configuration Limits

Table 4-8 summarizes the maximum limits for multicast configuration, including the commands used to display and change the limits.

Table 4-8 Multicast Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command	Show Current Settings Command (EXEC Mode)
Internet Group Management Protocol (IGMP) Limits				
Maximum number of groups used by IGMP and accepted by a router	50,000	75,000	**maximum groups** *n* (router IGMP configuration mode)	**show igmp summary**
Maximum number of groups for each interface accepted by a router	25,000	40,000	**maximum groups-per-interface** *n* (router IGMP interface configuration mode)	**show igmp summary**
Multicast Source Discovery Protocol (MSDP) Limits				
Maximum MSDP Source Active (SA) entries	20,000	75,000	**maximum external-sa** *n* (router MSDP configuration mode)	**show msdp summary**
Maximum MSDP SA entries that can be learned from MSDP peers	20,000	75,000	**maximum peer-external-sa** *n* (router MSDP configuration mode)	**show msdp summary**
Protocol Independent Multicast (PIM) Limits				
Maximum PIM routes supported	100,000	200,000	**maximum routes** *n* (router PIM configuration mode)	**show pim summary**
Maximum PIM egress states	300,000	600,000	**maximum route-interfaces** *n* (router PIM configuration mode)	**show pim summary**
Maximum PIM registers	20,000	75,000	**maximum register-states** *n* (router PIM configuration mode)	**show pim summary**
Maximum number of PIM group map ranges learned from Auto-RP	500	5000	**maximum group-mappings autorp** *n* (router PIM configuration mode)	**show pim summary**

MPLS Configuration Limits

Table 4-9 summarizes the maximum limits for Multiprotocol Label Switching (MPLS) configuration, including the commands used to display and change the limits.

Table 4-9 MPLS Configuration Limits and Commands

Limit Description	Default	Absolute Maximum Limit	Configuration Command (Global Configuration Mode)	Show Current Settings Command (EXEC Mode)
Maximum traffic engineer (TE) tunnels head	2500	65536	**mpls traffic-eng maximum tunnels** *n*	**show mpls traffic-eng maximum tunnels**

Other Configuration Limits

Table 4-10 summarizes the maximum limits for additional configuration limits, including the commands used to display and change the limits.

Table 4-10 Additional Configuration Limits and Commands

Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command (Global Configuration Mode)	Show Current Settings Command (EXEC Mode)
IPv4 ACL (access list and prefix list)	5000	16000	**ipv4 access-list maximum acl threshold** *n*	**show access-lists ipv4 maximum**
IPv4 ACE (access list and prefix list)	200,000	350,000	**ipv4 access-list maximum ace threshold** *n*	**show access-lists ipv4 maximum**