



# Configuring Additional Router Features

---

This chapter contains instructions and information for entering basic configurations using the command-line interface (CLI).

## Contents

- [Configuring the Domain Name and Domain Name Server, page 79](#)
- [Configuring Telnet, HTTP, and XML Host Services, page 81](#)
- [Managing Configuration History and Rollback, page 85](#)
- [Configuring Logging and Logging Correlation, page 90](#)
- [Creating and Modifying User Accounts and User Groups, page 94](#)
- [Configuring Software Entitlement, page 97](#)
- [Configuration Limiting, page 98](#)

## 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, follow these steps:

## SUMMARY STEPS

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

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure</b>  <b>Example:</b> RP/0/RSP0/CPU0:router# configure	Enters global configuration mode.
Step 2	<b>domain name</b> <i>domain-name-of-organization</i>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# domain name cisco.com	Defines a default domain name used to complete unqualified hostnames.
Step 3	<b>domain name-server</b> <i>ipv4-address</i>  <b>Example:</b> 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).  <b>Note</b> You can enter up to six addresses, but only one for each command.
Step 4	<b>end</b> or <b>commit</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# end or RP/0/RSP0/CPU0:router(config)# commit	Saves configuration changes.  <ul style="list-style-type: none"> <li>• When you issue the <b>end</b> command, the system prompts you to commit changes:  Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> <li>– Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>– Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>– Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> </ul> </li> <li>• Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

	Command or Action	Purpose
Step 5	<b>show hosts</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# show hosts	Displays all configured name servers.

## Examples

The following example shows how 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
```

## Related Documents

Related Topic	Document Title
Complete descriptions of the domain services commands	<i>Implementing Host Services and Applications on Cisco IOS XR Software module in Cisco ASR 9000 Series Aggregation Services RouterIP Addresses and Services Configuration Guide</i>

# Configuring Telnet, HTTP, and XML Host Services

For security reasons, some host services are disabled by default. You can enable Host services, such as Telnet, XML, and HTTP by using the commands described in this section. Host services provide the following features:

- Enabling the Telnet server allows users to log in to the router using IPv4 or IPv6 Telnet clients.
- Enabling the XML agent enables XML Common Object Request Broker Architecture (CORBA) agent services so that you can manage and configure the router using an XML interface.

## Prerequisites

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

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

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

**Note**

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

**SUMMARY STEPS**

1. **configure**
2. **interface MgmtEth interface-path-id**  
**ipv4 address ipv4-address subnetmask**
3. **ipv4 virtual address ipv4-address subnetmask**
4. **end** or **commit**
5. **exit**
6. **configure**
7. **telnet {ipv4 | ipv6} server max-servers limit**
8. **http server**
9. **xml agent**
10. **end** or **commit**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>configure</b>  <b>Example:</b> RP/0/RSP0/CPU0:router# configure	Enters global configuration mode.
<b>Step 2</b>	<b>interface MgmtEth interface-path-id</b> <b>ipv4 address ipv4-address subnetmask</b>  <b>Example:</b> <b>Active RP</b> RP/0/RSP0/CPU0:router(config)# interface MgmtEth0/RP0/CPU0/0 RP/0/RSP0/CPU0:router(config-if)# ipv4 address 172.29.52.75 255.255.255.0 RP/0/RP0/CPU0:router(config-if)# no shut RP/0/RP0/CPU0:router(config-if)# exit  <b>Standby RP</b> RP/0/RSP0/CPU0:router(config)# interface MgmtEth0/RP1/CPU0/0 RP/0/RSP0/CPU0:router(config-if)# ipv4 address 172.29.52.76 255.255.255.0 RP/0/RSP0/CPU0:router(config-if)# no shut RP/0/RSP0/CPU0:router(config-if)# exit	Configures the Management Ethernet ports on the active and standby RPs.

	Command or Action	Purpose
Step 3	<pre> <b>ipv4 virtual address</b> <i>ipv4-address subnetmask</i>  RP/0/RSP0/CPU0:router(config)# <b>ipv4 virtual</b> <b>address</b> 172.29.52.77 255.255.255.0 </pre>	Defines an IPv4 virtual address for the Management Ethernet interface.
Step 4	<pre> <b>end</b> or <b>commit</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# <b>end</b> or RP/0/RSP0/CPU0:router(config)# <b>commit</b> </pre>	<p>Saves configuration changes.</p> <ul style="list-style-type: none"> <li>When you issue the <b>end</b> command, the system prompts you to commit changes: <pre> Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: </pre> <ul style="list-style-type: none"> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> </ul> </li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>
Step 5	<pre> <b>exit</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# <b>exit</b> </pre>	Exits global configuration mode.
Step 6	<pre> <b>configure</b>  <b>Example:</b> RP/0/RSP0/CPU0:router# <b>configure</b> </pre>	Enters global configuration mode.
Step 7	<pre> <b>telnet ipv4 server max-servers</b> <i>limit</i> or <b>telnet ipv6 server max-servers</b> <i>limit</i>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# <b>telnet ipv4</b> <b>server max-servers</b> 5 </pre>	Enables Telnet services on the router and specifies the maximum number of allowable Telnet servers.
Step 8	<pre> <b>http server</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# <b>http server</b> </pre>	Enables HTTP server on the router.

	Command or Action	Purpose
Step 9	<b>xml agent</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# <b>xml agent</b> RP/0/RSP0/CPU0:router(config)# <b>xml agent tty</b>	Enables XML requests on the router.
Step 10	<b>end</b> or <b>commit</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# <b>end</b> or RP/0/RSP0/CPU0:router(config)# <b>commit</b>	Saves configuration changes. <ul style="list-style-type: none"> <li>When you issue the <b>end</b> command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> <li>Entering <b>yes</b> saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.</li> <li>Entering <b>no</b> exits the configuration session and returns the router to EXEC mode without committing the configuration changes.</li> <li>Entering <b>cancel</b> leaves the router in the current configuration session without exiting or committing the configuration changes.</li> </ul> </li> <li>Use the <b>commit</b> command to save the configuration changes to the running configuration file and remain within the configuration session.</li> </ul>

## Examples

The following example shows how the host services are enabled:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface MgmtEth0/RP0/CPU0/0
RP/0/RSP0/CPU0:router(config)# ipv4 address 172.29.52.75 255.255.255.0
RP/0/RSP0/CPU0:router(config)# ipv4 virtual address 172.29.52.77 255.255.255.0
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router(config)# exit
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)# xml agent
RP/0/RSP0/CPU0:router(config)# commit
```

## Related Documents

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

# Managing Configuration History and Rollback

After each commit operation, the system saves a record of the committed configuration changes. This record contains only the changes made during the configuration session; it does not contain the complete configuration. Each record is assigned a unique ID, known as a *commit ID*.

When multiple commit IDs are present, you can use a commit ID to identify a previous configuration to which to return, or you can use the commit ID to load the configuration changes made during that configuration session. You can also load configuration changes from multiple commit IDs, and you can clear commit IDs. If you are thinking about rolling back the configuration to a specific commit ID, consider the following guidelines:

- You cannot roll back to a configuration that was removed because of package incompatibility. Configuration rollbacks can succeed only when the configuration passes all compatibility checks with the currently active Cisco IOS XR Software release.
- If the system finds an incompatible configuration during rollback, the operation fails and an error appears.

The Cisco IOS XR software automatically saves up to 100 of the most recent commit IDs. The following sections describe how to manage configuration changes and roll back to a previously committed configuration:

- [Displaying the Commit IDs, page 86](#)
- [Displaying the Configuration Changes Recorded in a Commit ID, page 86](#)
- [Previewing Rollback Configuration Changes, page 87](#)
- [Rolling Back the Configuration to a Specific Rollback Point, page 87](#)
- [Rolling Back the Configuration over a Specified Number of Commits, page 88](#)
- [Loading Commit ID Configuration Changes to the Target Configuration, page 88](#)
- [Loading Rollback Configuration Changes to the Target Configuration, page 89](#)
- [Deleting Commit IDs, page 90](#)

## Displaying the Commit IDs

To display a history of up to 100 of the most recent commit IDs, enter the **show configuration commit list** command in EXEC or administration EXEC mode. Up to 100 of the most recent commit IDs are saved by the system. Each commit ID entry shows the user who committed configuration changes, the connection used to execute the commit, and commit ID time stamp.

The commit IDs 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

## Displaying the Configuration Changes Recorded in a Commit ID

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

```
RP/0/RSP0/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/RSP0/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 commit ID. 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 commit ID, go to EXEC or administration EXEC mode and enter the **show configuration rollback changes to *commit ID*** command. In the following example, the command help displays the available commit IDs, 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 enter the **show configuration rollback changes last *commit-range*** command:

```
RP/0/RSP1/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 enter the **rollback configuration to *commit ID*** 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 commit ID 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 enter 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/RSP1/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 Commit ID Configuration Changes to the Target Configuration

If the changes saved for a specific commit ID are close to what you want, but a rollback is not appropriate, you can load the configuration changes for a commit ID 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 commit ID configuration changes loads only the changes made during that commit operation. The load process does not load all changes made between the commit ID and the current committed configuration.

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

```
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
ipv6 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
ipv6 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, enter 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 enter the **load rollback changes to *commit ID*** command:

```
RP/0/RSP0/CPU0:router(config)# load rollback changes to 100000068

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 enter 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 commit IDs.

To load the rollback configuration for a specific commit ID, go to global configuration or administration configuration mode and enter the **load rollback changes *commit ID*** command:

```
RP/0/RSP0/CPU0:router(config)# load rollback changes 100000060

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

## Deleting Commit IDs

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

```
RP/0/RSP0/CPU0:router# clear configuration commits 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 commit IDs, enter the **clear configuration commits** command followed by the **oldest** keyword and number of commit IDs to delete:

```
RP/0/RSP0/CPU0:router# clear configuration commits 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 91](#)
- [Alarm Logging Correlation, page 91](#)
- [Configuring Basic Message Logging, page 92](#)
- [Disabling Console Logging, page 94](#)

## Logging Locations and Severity Levels

Table 10 shows error messages that can be logged to a variety of locations.

**Table 10** Logging Locations for System Error Messages

Logging Destination	Command (Global Configuration Mode)
console	<b>logging console</b>
vt terminal	<b>logging monitor</b>
external syslog server	<b>logging trap</b>
internal buffer	<b>logging buffered</b>

Table 11 shows how you can log messages based on the severity level of the messages.

**Table 11** 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. For more information, see [Cisco ASR 9000 Series Aggregation Services Router \*System Management Configuration Guide\*](#) .

## 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, follow these 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	<b>configure</b>  <b>Example:</b> RP/0/RSP0/CPU0:router# configure	Enters global configuration mode.
Step 2	<b>logging</b> { <i>ip-address</i>   <i>hostname</i> }  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# logging 10.1.1.1	Specifies a syslog server host to use for system logging.
Step 3	<b>logging trap</b> <i>severity</i>  <b>Example:</b> 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. <ul style="list-style-type: none"> <li>• <a href="#">Table 11</a> shows a summary of the logging severity levels.</li> </ul>
Step 4	<b>logging console</b> [ <i>severity</i> ]  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# logging console emergencies	Logs messages on the console. <ul style="list-style-type: none"> <li>• When a severity level is specified, only messages at that severity level are logged on the console.</li> <li>• <a href="#">Table 11</a> shows a summary of the logging severity levels.</li> </ul>

	Command or Action	Purpose
Step 5	<b>logging buffered</b> [ <i>severity</i>   <i>buffer-size</i> ]  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# logging buffered 1000000	Copies logging messages to an internal buffer. <ul style="list-style-type: none"> <li>• Newer messages overwrite older messages after the buffer is filled.</li> <li>• Specifying a severity level causes messages at that level and numerically lower levels to be logged in an internal buffer. See <a href="#">Table 11</a> for a summary of the logging severity levels.</li> <li>• The buffer size is from 4096 to 4,294,967,295 bytes. Messages above the set limit are logged to the console.</li> </ul>
Step 6	<b>commit</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# commit	Commits the target configuration to the router running configuration.
Step 7	<b>end</b>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# end	Ends the configuration session and returns to EXEC mode.
Step 8	<b>show logging</b>  <b>Example:</b> RP/0/RSP0/CPU0:router# show logging	Displays the messages that are logged in the buffer.

## Examples

The following example shows how the 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_NOTIFICATION
RP/0/RSP0/CPU0:Apr  8 19:22:32.596 : sysmgr[79]: %OS-SYSMGR-7-INSTALL_NOTIFICATION
```

```
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/RSP0/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--
```

## Disabling Console Logging

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

## Related Documents

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

## 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 group, 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. For a summary of user accounts, user groups, and task IDs, see the “[User Groups, Task Groups, and Task IDs](#)” section on page 53.

- [Displaying Details About User Accounts, User Groups, and Task IDs, page 95](#)
- [Configuring User Accounts, page 95](#)
- [Creating Users and Assigning Groups, page 96](#)

For a summary of user accounts, user groups, and task IDs, see [User Groups, Task Groups, and Task IDs](#).



### 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 included in the Cisco IOS XR software. For more information on the AAA concepts and configuration tasks, see the *Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide* and the *Cisco*



*ASR 9000 Series Aggregation Services Router System Security Command Reference* . For instructions to activate software packages, see the *Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide* .

## Displaying Details About User Accounts, User Groups, and Task IDs

Table 12 summarizes the EXEC mode commands used to display details about user accounts, user groups, and task IDs.

**Table 12** Commands to Display Details About Users and User Groups

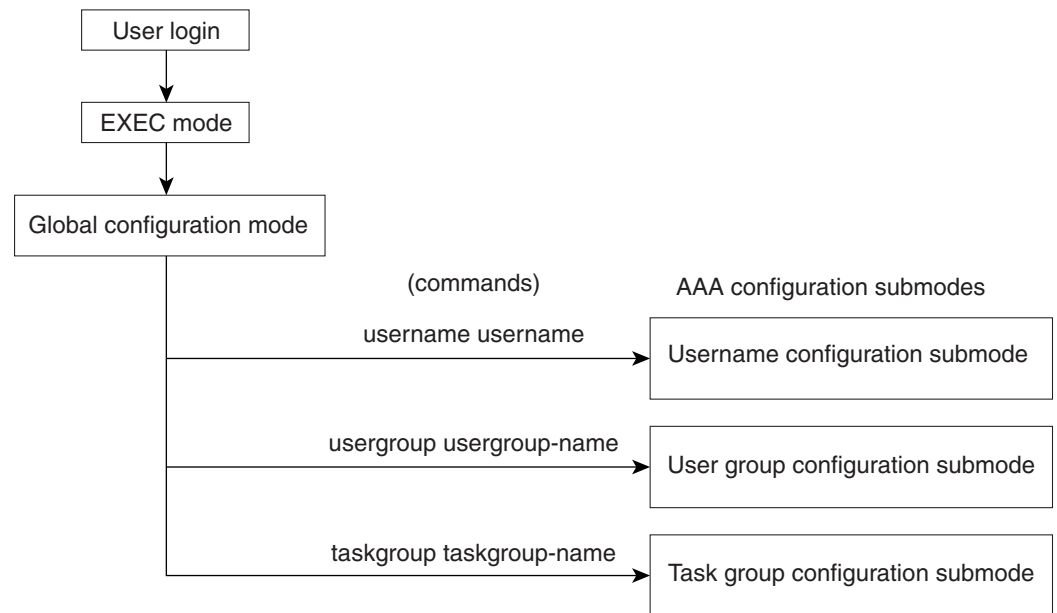
Command	Description
<code>show aaa userdb <i>username</i></code>	Displays the task IDs and privileges assigned to a specific username. To display all users on the system, type the command without a username.
<code>show aaa usergroup <i>usergroup-name</i></code>	Displays the task IDs and privileges that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

## Configuring User Accounts

Figure 23 shows how user accounts, user groups, and task groups are created by entering the appropriate commands in one of the AAA configuration submodes.

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

**Figure 23** AAA Configuration Submodes



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	<b>configure</b>  <b>Example:</b> RP/0/RSP0/CPU0:router# configure	Enters global configuration mode.
Step 2	<b>username</b> <i>user-name</i>  <b>Example:</b> RP/0/RSP0/CPU0:router(config)# username user1	Creates a name for a new user (or identifies a current user) and enters username configuration submenu. <ul style="list-style-type: none"> <li>• The <i>user-name</i> argument can be only one word. Spaces and quotation marks are not allowed.</li> </ul>
Step 3	<b>password</b> {0   7} <i>password</i> or <b>secret</b> {0   5} <i>password</i>  <b>Example:</b> 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 <a href="#">Step 2</a> . <ul style="list-style-type: none"> <li>• Use the <b>secret</b> command to create a secure login password for the user names specified in <a href="#">Step 2</a>.</li> <li>• Entering <b>0</b> following the <b>password</b> command specifies that an unencrypted (clear-text) password follows. Entering <b>7</b> following the <b>password</b> command specifies that an encrypted password follows.</li> <li>• Entering <b>0</b> following the <b>secret</b> command specifies that a secure unencrypted (clear-text) password follows. Entering <b>5</b> following the <b>secret</b> command specifies that a secure encrypted password follows.</li> <li>• Type <b>0</b> is the default for the <b>password</b> and <b>secret</b> commands.</li> </ul>

	Command or Action	Purpose
Step 4	<p><code>group group-name</code></p> <p><b>Example:</b>  RP/0/RSP0/CPU0:router(config-un)# group sysadmin</p>	<p>Assigns the user named in <a href="#">Step 2</a> to a user group.</p> <ul style="list-style-type: none"> <li>The user takes on all attributes of the user group, as defined by the user group association to various task groups.</li> <li>Each user must be assigned to at least one user group. A user may belong to multiple user groups.</li> </ul>
Step 5	Repeat <a href="#">Step 4</a> for each user group to be associated with the user specified in <a href="#">Step 2</a> .	—
Step 6	<p><code>commit</code></p> <p><b>Example:</b>  RP/0/RSP0/CPU0:router(config-un)# commit</p>	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	<i>Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide.</i>

# 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 4.0, the following features must be enabled with licenses:

- Layer 3 VPN Routing and Forwarding (VRF)
- G.709 support for supported 10-Gigabit Ethernet line cards (LCs)
- Video Monitoring (Vid-Mon) for Chassis
- Infrastructure VRF

## Examples

The following example shows the supported license features:

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router(admin)#show license features
Tue Jun 29 10:06:46.296 pst
```

```
Platform Feature ID:
  A9K-ADV-OPTIC-LIC
  A9K-ADV-VIDEO-LIC
```

```
A9K-ivrf-LIC
A9K-AIP-LIC-B
A9K-AIP-LIC-E
```

The following example shows how the permanent license is acquired for a feature that you have purchased:

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router(admin)# show license

Mon May 31 22:17:35.958 DST

FeatureID: A9K-ADV-OPTIC-LIC (Slot based, Permanent)
Total licenses 1
Available for use      1
Allocated to location  0
Active                 0
Store name             Permanent
Store index            1
Pool: Owner
  Total licenses in pool: 1
  Status: Available    1   Operational:    0
```

## Adding a License to a Router

Go to the license tool on Cisco.com at <http://www.cisco.com/go/license> and enter the Product Authorization Key (PAK) of the feature and the UDI of the chassis.

Copy the license file to your TFTP server accessible from your router.

Enter administration EXEC mode on the router to which you want to add the license:

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router(admin)# license add tftp://192.10.10.10/mylicenses/lc40g_lic
RP/0/RSP0/CPU0:router(admin)# exit
```

For more information on configuring software licenses, see *Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*.

## 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 99](#)
- [IS-IS Configuration Limits, page 100](#)

- [OSPFv2 and v3 Configuration Limits, page 100](#)
- [Routing Policy Language Line and Policy Limits, page 103](#)
- [Platform-Independent Multicast Configuration Limits, page 104](#)
- [Cisco ASR 9000 Series Router Multicast Configuration Limits, page 105](#)
- [MPLS Configuration Limits, page 105](#)
- [Video Monitoring Limits, page 106](#)
- [L2VPN Configuration Limits, page 107](#)

## Static Route Configuration Limits

Table 13 summarizes the maximum limits for static routes, including the commands used to display and change the limits.

**Table 13** *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	<code>maximum path ipv4 n</code>	<code>show running-config router static</code>

### Examples

The following example shows 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 14 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 14** 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	20,000 <sup>1</sup>	<b>maximum-redistributed-prefixes</b> <i>n</i>	<b>show isis adjacency</b>
Number of active parallel paths for each route on a Cisco ASR 9000 Series Router	8	8	<b>maximum-paths</b> <i>n</i>	<b>show isis route</b>

1. This limit is for ASR 9000 Ethernet LCs. The actual number differs depending on the LC on the system.

## Examples

The following example shows 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 15 summarizes the maximum limits for Open Shortest Path First (OSPF) protocol, including the commands used to display and change the limits.

Table 15 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	<b>maximum interfaces</b> <i>n</i>	<b>show ospf</b>
Maximum routes redistributed into OSPF	10,000	20,000 <sup>1</sup>	<b>maximum redistributed-prefixes</b> <i>n</i>	<b>show ospf</b> <b>Note</b> The maximum number of redistributed prefixes appear only if redistribution is configured.
Maximum number of parallel routes (maximum paths) on Cisco ASR 9000 Series Router routers	8	8	<b>maximum paths</b> <i>n</i>	<b>show running-config router ospf</b> <b>Note</b> This command shows only changes to the default value. If the <b>maximum paths</b> command does not appear, the router is set to the default value.

1. This limit is for ASR 9000 Ethernet LCs. The actual number differs depending on the LC on the system.

## Examples

The following examples show OSPF configuration limits:

- [Maximum Interfaces for Each OSPF Instance: Example, page 101](#)
- [Maximum Routes Redistributed into OSPF: Example, page 102](#)
- [Number of Parallel Links \(max-paths\): Example, page 103](#)

### Maximum Interfaces for Each OSPF Instance: Example

The following example shows how the **show ospf** command is used to display the maximum number of OSPF interfaces:

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

```
Mon May 31 22:20:15.618 DST
```

```
Routing Process "ospf 100" with ID 10.144.144.144
NSR (Non-stop routing) is Enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 50 msec
Minimum hold time between two consecutive SPFs 200 msec
Maximum wait time between two consecutive SPFs 5000 msec
Initial LSA throttle delay 50 msec
Minimum hold time for LSA throttle 200 msec
Maximum wait time for LSA throttle 5000 msec
Minimum LSA interval 200 msec. Minimum LSA arrival 100 msec
```

```

LSA refresh interval 1800 seconds
Flood pacing interval 33 msec. Retransmission pacing interval 66 msec
Adjacency stagger enabled; initial (per area): 2, maximum: 64
  Number of neighbors forming: 0, 5 full
Maximum number of configured interfaces 255
Number of external LSA 3. Checksum Sum 0x00f54e
Number of opaque AS LSA 0. Checksum Sum 00000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
--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

Mon May 31 22:23:35.401 DST

Routing Process "ospf 100" with ID 10.144.144.144
NSR (Non-stop routing) is Enabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 50 msec
Minimum hold time between two consecutive SPFs 200 msec
Maximum wait time between two consecutive SPFs 5000 msec
Initial LSA throttle delay 50 msec
Minimum hold time for LSA throttle 200 msec
Maximum wait time for LSA throttle 5000 msec
Minimum LSA interval 200 msec. Minimum LSA arrival 100 msec
LSA refresh interval 1800 seconds
Flood pacing interval 33 msec. Retransmission pacing interval 66 msec
Adjacency stagger enabled; initial (per area): 2, maximum: 64
  Number of neighbors forming: 0, 5 full
Maximum number of configured interfaces 600
--More--

```

## Maximum Routes Redistributed into OSPF: Example

The following example shows how 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

The following example shows how 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:

- 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.
- 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 16](#). 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 16** 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	<b>rpl maximum lines</b> <i>n</i>	<b>show rpl maximum lines</b>
Maximum number of RPL policies	3500	5000	<b>rpl maximum policies</b> <i>n</i>	<b>show rpl maximum policies</b>

### Examples

The following example shows how 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

Mon May 31 22:28:25.602 DST
                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#

```

The following example shows how 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

Mon May 31 23:25:24.444 DST
                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#

```

## Platform-Independent Multicast Configuration Limits

Table 17 summarizes the maximum limits for multicast configuration, including the commands used to display and change the limits. These limits are applicable to any platform.

**Table 17** Multicast Configuration Limits and Commands

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command	Show Current Settings Command (EXEC Mode)
<b>Internet Group Management Protocol (IGMP) Limits</b>				
Maximum number of groups used by IGMP and accepted by a router	50,000	75,000	<b>maximum groups</b> <i>n</i> (router IGMP configuration mode)	<b>show igmp summary</b>
Maximum number of groups for each interface accepted by a router	25,000	40,000	<b>maximum groups-per-interface</b> <i>n</i> (router IGMP interface configuration mode)	<b>show igmp summary</b>
<b>Multicast Source Discovery Protocol (MSDP) Limits</b>				
Maximum MSDP Source Active (SA) entries	20,000	75,000	<b>maximum external-sa</b> <i>n</i> (router MSDP configuration mode)	<b>show msdp summary</b>

**Table 17** Multicast Configuration Limits and Commands (continued)

Feature Limit Description	Default Maximum Limit	Absolute Maximum Limit	Configuration Command	Show Current Settings Command (EXEC Mode)
Maximum MSDP SA entries that can be learned from MSDP peers	20,000	75,000	<b>maximum peer-external-sa</b> <i>n</i> (router MSDP configuration mode)	<b>show msdp summary</b>
<b>Protocol Independent Multicast (PIM) Limits</b>				
Maximum PIM routes supported	100,000	200,000	<b>maximum routes</b> <i>n</i> (router PIM configuration mode)	<b>show pim summary</b>
Maximum PIM egress states	300,000	600,000	<b>maximum route-interfaces</b> <i>n</i> (router PIM configuration mode)	<b>show pim summary</b>
Maximum PIM registers	20,000	75,000	<b>maximum register-states</b> <i>n</i> (router PIM configuration mode)	<b>show pim summary</b>
Maximum number of PIM group map ranges learned from Auto-RP	500	5000	<b>maximum group-mappings autorp</b> <i>n</i> (router PIM configuration mode)	<b>show pim summary</b>

## Cisco ASR 9000 Series Router Multicast Configuration Limits

[Table 18](#) summarizes the maximum multicast scale supported by the Cisco ASR 9000 Series Router. These limits take precedence over the limits specified in the [Table 17](#).

**Table 18** Multicast Scale Limits on Cisco ASR 9000 Series Router

Limit Description	Per System	Per Linecard
Multicast Routes	16,384	16,384
Multicast Subscriber Interfaces	Configuration Limits <sup>1</sup>	16,000

1. Refer to Platform Independent Multicast configuration limits as specified in [Table 17](#).

## MPLS Configuration Limits

[Table 19](#) summarizes the maximum limits for Multiprotocol Label Switching (MPLS) configuration, including the commands used to display and change the limits.


**Table 19** 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	4096	65536	<b>mpls tr maxabs tunnels</b> <i>n</i>	<b>show mpls traffic-eng maximum tunnels</b>

## Video Monitoring Limits

Table 20 summarizes the maximum values for video monitoring configuration, monitored flows, and their performance metrics.

**Table 20** Video Monitoring Limits

Category	Maximum Value	Comments
Class Maps	1024 per policy map 1024 per system	The maximum value is valid when the keyword is traffic.
Policy Maps	256 per system	The maximum value is valid when the keyword is performance-traffic.
Video Monitoring service policies	One policy per interface	The maximum values is valid when the keyword is performance-traffic.
Monitored Flows	4096 per Network Processor (NP) 4096 per class map 4096 per policy map (8192 per policy map when attached to a bundle interface.)	Includes both static and dynamic flows.
Flow Rate at Layer 3	280 kpps per flow	Equivalent to uncompressed high definition (HD) video streams. The absolute configuration maximum value is 1 Mpps per flow.
Flow Rate at Media Layer	3 Gbps per flow	Equivalent to uncompressed high definition (HD) video streams.
Delay Factor (DF) Precision	1 millisecond	—
Media Rate Variation (MRV) range	999.999%	Minimum range is -100%
Flow History	60 intervals per flow	Default value is 10 intervals per flow.
Interval Duration	300 seconds per interval	Default value is 30 seconds per interval. Minimum value is 10 seconds that can be incremented by 5 seconds.
Reacts	14 reacts per class map	 <p><b>Note</b> This value is specific to <i>Cisco ASR 9000 Series Aggregation Series Router</i> running Cisco IOS XR Software Release 4.0.</p>



**Note**

For more information about each category, see the “Implementing Video Monitoring Service on Cisco ASR 9000 Series Routers” chapter in *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*.

## Other Configuration Limits

Table 21 summarizes the maximum limits for additional configuration limits, including the commands used to display and change the limits.

**Table 21** Additional Configuration Limits and Commands

Limit Description	Absolute Maximum Limit	Show Current Settings Command (EXEC Mode)
IPv4 ACL (access list and prefix list)	10,000	<code>show access-lists ipv4 maximum</code>
IPv4 ACE (access list and prefix list)	350,000	<code>show access-lists ipv4 maximum</code>

## L2VPN Configuration Limits

Table 0-22 summarizes the scale limitations on the Cisco ASR 9000 Series Routers.

**Table 0-22** L2VPN Configuration Limits

	Port/Bundle	Network Processor	Line Card	Bridge Domain	System
Subinterfaces	NA	16K	32K	NA	64K
Bridge Domains	NA	16K	32K	NA	NA
Pseudowires	NA	NA	NA	NA	64K
LAG Bundles	NA	NA	40K	NA	128K
Interflex Pairs	NA	NA	NA	NA	128K
LAG Subinterfaces	4K	NA	8K	NA	16K
Learned MACs	256K	512K	512K	256K	512K



**Note**

The limitations are specified for each VFI (Virtual Forwarding Instance).

