Implementing Logging Services

This module describes the new and revised tasks you need to implement logging services on the router.

The Cisco IOS XR Software provides basic logging services. Logging services provide a means to gather logging information for monitoring and troubleshooting, to select the type of logging information captured, and to specify the destinations of captured system logging (syslog) messages.

Note For more information about logging services on the Cisco IOS XR Software and complete descriptions of the logging commands listed in this module, see the Related Documents, on page 25 section of this module.

Feature History for Implementing Logging Services

Release	Modification
Release 3.2	This feature was introduced.
Release 3.7.0	The **logging on** command was removed. The logging process is enabled by default.

Prerequisites for Implementing Logging Services

These prerequisites are required to implement logging services in your network operating center (NOC):

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- You must have connectivity with syslog servers to configure syslog server hosts as the recipients for syslog messages.

Information About Implementing Logging Services

System Logging Process

By default, routers are configured to send syslog messages to a syslog process. The syslog process controls the distribution of messages to the destination of syslog messages such as the logging buffer, terminal lines, or a syslog server. The syslog process also sends messages to the console terminal by default.

Note For more information about how the syslog process functions within the Alarms and Debugging Event Management System (ALDEMS) infrastructure on Cisco IOS XR software, see *Implementing and Monitoring Alarms and Alarm Log Correlation on Cisco IOS XR Software*.

Format of System Logging Messages

By default, the general format of syslog messages generated by the syslog process on the Cisco IOS XR software is as follows:

node-id : *timestamp* : *process-name* [*pid*] : % *message category -group -severity -message -code* : *message-text*

This is a sample syslog message:

```
RP/0/0/CPU0:router:Nov 28 23:56:53.826 : config[65710]: %SYS-5-CONFIG_I : Configured from
console by console
```

This table describes the general format of syslog messages on Cisco IOS XR software.

Table 1: General Syslog Message Format

Field	Description
node-id	Node from which the syslog message originated.
timestamp	Time stamp in the form *month day HH:MM:SS*, indicating when the message was generated. **Note** The time-stamp format can be modified using the **service timestamps** command. See the Modifying the Format of Time Stamps, on page 16 section.
process-name	Process that generated the syslog message.

Field	Description
[*pid*]	Process ID (pid) of the process that generated the syslog message.
% *category -group- severity -code*	Message category, group name, severity, and message code associated with the syslog message.
message-text	Text string describing the syslog message.

Duplicate Message Suppression

Suppressing duplicate messages, especially in a large network, can reduce message clutter and simplify the task of interpreting the log. The duplicate message suppression feature substantially reduces the number of duplicate event messages in both the logging history and the syslog file. The suppression and logging process is the same for logging history and for external syslog servers.

When duplicate message suppression is enabled, two types of events are handled differently:

- New messages

  New messages are always logged immediately.

- Repeated messages

  Repeated messages are subject to suppression. The suppression of repeated messages is interrupted when a new message occurs.

For information about configuring this feature, see the Suppressing Duplicate Syslog Messages, on page 19.

Message Suppression

The first occurrence of an event is always logged immediately, but subsequent identical messages are suppressed during three different time intervals. Initially, duplicate messages are suppressed for 30 seconds after the first event, then for 120 seconds, and finally every 600 seconds (10 minutes). At the end of each interval, the next identical event triggers the “last message repeated *nn* times” message, and resets the count of duplicate messages. The end of the interval does not automatically trigger a message, so the summary message can be delayed well beyond the suppression interval.

For example, this syslog excerpt shows the log entries for repeated Telnet failures when the suppress duplicate feature s is enabled. In this case, Telnet failures occur at the rate of four per minute:

```
Jul 24 09:39:10 [10.1.1.1.2.2] 326: ROUTER-TEST  TELNETD_[65778]: %IP-TELNETD-3-ERR_CONNECT
 : Failed to obtain a VTY for a session: ''tty-server' detected the 'resource not available'
 condition 'There are no TTYs available
Jul 24 09:39:45 [10.1.1.1.2.2] 333: ROUTER-TEST last message repeated 2 times
Jul 24 09:41:50 [10.1.1.1.2.2] 358: ROUTER-TEST last message repeated 8 times
Jul 24 09:52:04 [10.1.1.1.2.2] 391: ROUTER-TEST last message repeated 40 times
Jul 24 10:02:35 [10.1.1.1.2.2] 412: ROUTER-TEST last message repeated 40 times
```

The first Telnet failure was logged at 9:39 as a normal error message. Thirty seconds later, a summary message reports two repetitions. Then after another 120 seconds, another message reports eight more repetitions. Finally, two more messages report the 40 repetitions that occurred in two consecutive 600-second intervals.

Because the errors are occurring at regular 15-second intervals, a new error triggers a summary message just after the end of a suppression interval. The end of a suppression interval itself does not trigger a message.

Interruption of Message Suppression

The sequence of suppression intervals is interrupted if a different event occurs. The first occurrence of all new events is always logged immediately, so a new event aborts the current suppression interval. This clears the message queue, so another message from the previous sequence is then treated as a new event, and the suppression sequence starts over.

The repeated message summary is generated only at an interval of 0 , 30, 120 and 600 secs, and not on the occurrence of a new event. At every interval it is checked if currently any number of messages are suppressed. If any messages are suppressed at this interval, it's summary is displayed, the message queue is cleared, and the suppression sequence starts all over. So if a new event occurs before the suppression interval, the message queues and counters will be cleared, and at the time of interval, there will be no suppression to be summarized.

Here is an example:

```
RP/0/0/CPU0:router#show running-config logging
Mon Dec  3 12:30:26.346 UTC
logging archive
 device harddisk
 severity debugging
 file-size 4
 archive-size 100
!
logging console disable
logging 223.255.254.248
logging 223.255.254.249
logging suppress duplicates

RP/0/0/CPU0:router#
RP/0/0/CPU0:router#
RP/0/0/CPU0:router#
RP/0/0/CPU0:router#
RP/0/0/CPU0:router#run
Mon Dec  3 12:30:39.798 UTC
#
# while true
> do
> logger -s alert -c 1 "LOGGING SUPRESS DUPLICATE TESTING "
> done

RP/0/0/CPU0:router#
RP/0/0/CPU0:router#

//********************************************** MSGS ON REMOTE
SERVER************************************************************
Message from syslogd@[12.24.50.70.2.2] at Mon Dec  3 05:01:59 2012 ...
[12.24.50.70.2.2] 663231: last message repeated 2 times
Dec  3 05:01:58 [12.24.50.70.2.2] 663230: RP/0/RP1/CPU0:Dec  3 12:52:09.773 : logger[65786]:
 %OS-SYSLOG-1-LOG_ALERT_OWNER_PLANE :  LOGGING SUPRESS DUPLICATE TESTING
Dec  3 05:01:59 [12.24.50.70.2.2] 663231: last message repeated 2 times

Message from syslogd@[12.24.50.70.2.2] at Mon Dec  3 05:02:30 2012 ...
[12.24.50.70.2.2] 663232: last message repeated 110 times
Dec  3 05:02:30 [12.24.50.70.2.2] 663232: last message repeated 110 times

Message from syslogd@[12.24.50.70.2.2] at Mon Dec  3 05:04:31 2012 ...
[12.24.50.70.2.2] 663233: last message repeated 348 times
Dec  3 05:04:31 [12.24.50.70.2.2] 663233: last message repeated 348 times

Message from syslogd@[12.24.50.70.2.2] at Mon Dec  3 05:14:32 2012 ...
[12.24.50.70.2.2] 663234: last message repeated 1797 times
Dec  3 05:14:32 [12.24.50.70.2.2] 663234: last message repeated 1797 times
```

Logging History and Syslog Comparison

The logging process with suppression is the same for logging history and for external syslog servers. Both suppress duplicate messages using a sequence of suppression intervals. This example shows an excerpt from the **show logging history** command.

```
TELNETD_[65778]: %IP-TELNETD-3-ERR_CONNECT : ...
last message repeated 2 times
last message repeated 8 times
last message repeated 7 times
config[65677]: %MGBL-CONFIG-6-DB_COMMIT : ...
TELNETD_[65778]: %IP-TELNETD-3-ERR_CONNECT :  ...
```

The logging history and syslog entries are the same in this case, but they can be different under other conditions. They can differ because of the severity level configured for each type of log and because of the timing of the log messages. Also, if there are just a few repeated messages that occur in less than 30 seconds, the reporting of duplicates can seem to be suppressed altogether. These duplicates ultimately are reported however, just before the next new event is logged.

Syslog Message Destinations

Syslog message logging to the console terminal is enabled by default. To disable logging to the console terminal, use the **logging console disable** command in global configuration mode. To reenable logging to the console terminal, use the **logging console** command in global configuration mode.

Syslog messages can be sent to destinations other than the console, such as the logging buffer, syslog servers, and terminal lines other than the console (such as vtys).

This table lists the commands used to specify syslog destinations.

Table 2: Commands Used to Set Syslog Destinations

Command	Description
logging buffered	Specifies the logging buffer as a destination for syslog messages.
logging {*hostname* | *ip-address*}	Specifies a syslog server host as a destination for syslog messages. IPv4 and IPv6 are supported.
logging monitor	Specifies terminal lines other than the console as destinations for syslog messages.

The **logging buffered** command copies logging messages to the logging buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the syslog messages that are logged in the logging buffer, use the **show logging** command. The first message displayed is the oldest message in the buffer. To clear the current contents of the logging buffer, use the **clear logging** command. To disable logging to the logging buffer, use the **no logging buffered** command in global configuration mode.

The **logging** command identifies a syslog server host to receive logging messages. By issuing this command more than once, you build a list of syslog servers that receive logging messages. To delete the syslog server with the specified IP address (IPv4 and IPv6 are supported) or hostname from the list of available syslog servers, use the **no logging** command in global configuration mode.

The **logging monitor** command globally enables the logging of syslog messages to terminal lines other than the console, such as vtys. To disable logging to terminal lines other than the console, use the **no logging monitor** command in global configuration mode.

Guidelines for Sending Syslog Messages to Destinations Other Than the Console

The logging process sends syslog messages to destinations other than the console terminal and the process is enabled by default. Logging is enabled to the logging buffer, terminal lines and syslog servers.

Logging for the Current Terminal Session

The **logging monitor** command globally enables the logging of syslog messages to terminal lines other than console terminal. Once the **logging monitor** command is enabled, use the **terminal monitor** command to display syslog messages during a terminal session.

To disable the logging of syslog messages to a terminal during a terminal session, use the **terminal monitor disable** command in EXEC mode. The **terminal monitor disable** command disables logging for only the current terminal session.

To reenable the logging of syslog messages for the current terminal session, use the **terminal monitor** command in EXEC mode.

Note The **terminal monitor** and **terminal monitor disable** commands are set locally and will not remain in effect after the terminal session is ended.

Syslog Messages Sent to Syslog Servers

The Cisco IOS XR Software provides these features to help manage syslog messages sent to syslog servers:

- UNIX system facilities
- Hostname prefix logging
- Source interface logging

UNIX System Logging Facilities

You can configure the syslog facility in which syslog messages are sent by using the **logging facility** command. Consult the operator manual for your UNIX operating system for more information about these UNIX system facilities. The syslog format is compatible with Berkeley Standard Distribution (BSD) UNIX version 4.3.

This table describes the facility type keywords that can be supplied for the *type* argument.

Table 3: Logging Facility Type Keywords

Facility Type Keyword	Description
auth	Indicates the authorization system.

Facility Type Keyword	Description
cron	Indicates the cron facility.
daemon	Indicates the system daemon.
kern	Indicates the Kernel.
local0–7	Reserved for locally defined messages.
lpr	Indicates line printer system.
mail	Indicates mail system.
news	Indicates USENET news.
sys9	Indicates system use.
sys10	Indicates system use.
sys11	Indicates system use.
sys12	Indicates system use.
sys13	Indicates system use.
sys14	Indicates system use.
syslog	Indicates the system log.
user	Indicates user process.
uucp	Indicates UNIX-to-UNIX copy system.

Hostname Prefix Logging

To help manage system logging messages sent to syslog servers, Cisco IOS XR Software supports hostname prefix logging. When enabled, hostname prefix logging appends a hostname prefix to syslog messages being sent from the router to syslog servers. You can use hostname prefixes to sort the messages being sent to a given syslog server from different networking devices.

To append a hostname prefix to syslog messages sent to syslog servers, use the **logging hostname** command in global configuration mode.

Syslog Source Address Logging

By default, a syslog message contains the IP address (IPv4 and IPv6 are supported) of the interface it uses to leave the router when sent to syslog servers. To set all syslog messages to contain the same IP address,

regardless of which interface the syslog message uses to exit the router, use the **logging source-interface** command in global configuration mode.

UNIX Syslog Daemon Configuration

To configure the syslog daemon on a 4.3 BSD UNIX system, include a line such as the following in the /etc/syslog.conf file:

```
local7.debug /usr/adm/logs/cisco.log
```

The **debugging** keyword specifies the syslog level; see Table 7: Syslog Message Severity Levels, on page 11 for a general description of other keywords. The **local7** keyword specifies the logging facility to be used; see Table 7: Syslog Message Severity Levels, on page 11 for a general description of other keywords.

The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

Archiving Logging Messages on a Local Storage Device

Syslog messages can also be saved to an archive on a local storage device, such as the hard disk or a flash disk. Messages can be saved based on severity level, and you can specify attributes such as the size of the archive, how often messages are added (daily or weekly), and how many total weeks of messages the archive will hold.

Setting Archive Attributes

To create a logging archive and specify how the logging messages will be collected and stored, use the **logging archive** command in global configuration mode. The **logging archive** command enters the logging archive submode where you can configure the attributes for archiving syslogs.

This table lists the commands used to specify the archive attributes once you are in the logging archive submode.

Table 4: Commands Used to Set Syslog Archive Attributes

Command	Description
archive-length *weeks*	Specifies the maximum number of weeks that the archive logs are maintained in the archive. Any logs older than this number are automatically removed from the archive.
archive-size *size*	Specifies the maximum total size of the syslog archives on a storage device. If the size is exceeded then the oldest file in the archive is deleted to make space for new logs.

Command	Description
device {**disk0** | **disk1** | **harddisk**}	Specifies the local storage device where syslogs are archived. By default, the logs are created under the directory <device>/var/log. If the device is not configured, then all other logging archive configurations are rejected. We recommend that syslogs be archived to the harddisk because it has more capacity than flash disks.
file-size *size*	Specifies the maximum file size (in megabytes) that a single log file in the archive can grow to. Once this limit is reached, a new file is automatically created with an increasing serial number.
frequency{**dailyweekly**}	Specifies if logs are collected on a daily or weekly basis.
severity *severity*	Specifies the minimum severity of log messages to archive. All syslog messages greater than or equal to this configured level are archived while those lesser than this are filtered out. See the Severity Levels, on page 9 for more information.

Archive Storage Directories

By default, syslog archives are stored in the directory <device>/var/log. Individual archive files are saved to sub directories based on the year, month, and day the archive was created. For example, archive files created on February 26, 2006 are stored in this directory:

```
harddisk:/var/log/2006/02/26
```

Severity Levels

You can limit the number of messages sent to a logging destination by specifying the severity level of syslog messages sent to a destination (see Table 7: Syslog Message Severity Levels, on page 11 for severity level definitions).

This table lists the commands used to control the severity level of syslog messages.

Table 5: Commands Used to Control the Severity Level of Syslog Messages

Command	Description
logging buffered [*severity*]	Limits the syslog messages sent to the logging buffer based on severity.
logging console [*severity*]	Limits the syslog messages sent to the console terminal based on severity.

Command	Description
logging monitor [*severity*]	Limits the syslog messages sent to terminal lines based on severity.
logging trap [*severity*]	Limits the syslog messages sent to syslog servers based on severity.
severity *severity*	Limits the syslog messages sent to a syslog archive based on severity.

The **logging buffered**, **logging console**, **logging monitor**, and **logging traps** commands limit syslog messages sent to their respective destinations to messages with a level number at or below the specified severity level, which is specified with the *severity* argument.

Note Syslog messages of lower severity level indicate events of higher importance. See Table 7: Syslog Message Severity Levels, on page 11 for severity level definitions.

Logging History Table

If you have enabled syslog messages traps to be sent to a Simple Network Management Protocol (SNMP) network management station (NMS) with the **snmp-server enable traps syslog** command, you can change the level of messages sent and stored in a history table on the router. You can also change the number of messages that get stored in the history table.

Messages are stored in the history table, because SNMP traps are not guaranteed to reach their destination. By default, one message of the level warning and above (see Table 7: Syslog Message Severity Levels, on page 11) is stored in the history table even if syslog traps are not enabled.

This table lists the commands used to change the severity level and table size defaults of the logging history table

Table 6: Logging History Table Commands

Command	Description
logging history *severity*	Changes the default severity level of syslog messages stored in the history file and sent to the SNMP server.
logging history size *number*	Changes the number of syslog messages that can be stored in the history table.

Note Table 7: Syslog Message Severity Levels, on page 11 lists the level keywords and severity level. For SNMP usage, the severity level values use +1. For example, **emergency** equals 1 not 0 and **critical** equals 3 not 2.

Syslog Message Severity Level Definitions

This table lists the severity level keywords that can be supplied for the *severity* argument and corresponding UNIX syslog definitions in order from the most severe level to the least severe level.

Table 7: Syslog Message Severity Levels

Severity Keyword	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Syslog Severity Level Command Defaults

This table lists the default severity level settings for the commands that support the *severity* argument.

Table 8: Severity Level Command Defaults

Command	Default Severity Keyword	Level
logging buffered	debugging	7
logging console	informational	6
logging history	warnings	4
logging monitor	debugging	7

Command	Default Severity Keyword	Level
logging trap	informational	6

How to Implement Logging Services

Setting Up Destinations for System Logging Messages

This task explains how to configure logging to destinations other than the console terminal.

For conceptual information, see the Syslog Message Destinations, on page 5 section.

SUMMARY STEPS

1. **configure**
2. **logging buffered** [*size* | *severity*]
3. **logging monitor** [*severity*]
4. **commit**
5. **terminal monitor**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**logging buffered** [*size* | *severity*] **Example:** `RP/0/0/CPU0:router(config)# logging buffered severity warnings`	Specifies the logging buffer as a destination for syslog messages, sets the size of the logging buffer, and limits syslog messages sent to the logging buffer based on severity. • The default value for the *size* argument is 4096 bytes. • The default value for the *severity* argument is **debugging**. • Keyword options for the *severity* argument are **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**. • By default, entering this command without specifying a severity level for the *severity* argument or specifying the size of the buffer for the *size* argument sets the severity level to **debugging** and the buffer size to 4096 bytes.
Step 3	**logging monitor** [*severity*] **Example:** `RP/0/0/CPU0:router(config)# logging monitor critical`	Specifies terminal lines other than console terminal as destinations for syslog messages and limits the number of messages sent to terminal lines based on severity. • Keyword options for the *severity* argument are **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**. • By default, entering this command without specifying a severity level for the *severity* argument sets the severity level to **debugging**.

	Command or Action	Purpose
Step 4	**commit**	
Step 5	**terminal monitor** **Example:** `RP/0/0/CPU0:router# terminal monitor`	Enables the display of syslog messages for the current terminal session. **Note** The logging of syslog message for the current terminal can be disabled with the **terminal monitor disable** command. • Use this command to reenable the display of syslog messages for the current session if the logging of messages for the current session was disabled with **terminal monitor disable** command. **Note** Because this command is an EXEC mode command, it is set locally and will not remain in effect after the current session is ended.

Configuring Logging to a Remote Server

This task explains how to configure logging to remote syslog servers.

Before You Begin

You must have connectivity with syslog servers to configure syslog server hosts as the recipients for syslog messages.

SUMMARY STEPS

1. **configure**
2. **logging** {*ip-address* | *hostname*}
3. **logging trap** [*severity*]
4. **logging facility** [*type*]
5. **logging hostnameprefix** *hostname*
6. **logging source-interface** *type interface-path-id*
7. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**logging** {*ip-address*	*hostname*} **Example:** `RP/0/0/CPU0:router(config)# logging 10.3.32.154`	Specifies a syslog server host as a destination for syslog messages. IPv4 and IPv6 are supported. • By issuing this command more than once, you build a list of syslog servers that receive logging messages.

	Command or Action	Purpose
Step 3	**logging trap** [*severity*] **Example:** `RP/0/0/CPU0:router(config)# logging trap`	Limits the syslog messages sent to syslog servers based on severity. • By default, entering this command without specifying a severity level for the *severity* argument sets the severity level to **informational**.
Step 4	**logging facility** [*type*] **Example:** `RP/0/0/CPU0:router(config)# logging facility kern`	(Optional) Configures syslog facilities. • By default, entering this command without specifying a facility type for the *type* argument sets the facility to **local-7**.
Step 5	**logging hostnameprefix** *hostname* **Example:** `RP/0/0/CPU0:router(config)# logging hostnameprefix 123.12.35.7`	(Optional) Appends a hostname prefix to syslog messages being sent from the router to syslog servers. **Tip** Hostname prefix logging can be useful for sorting syslog messages received by syslog servers.
Step 6	**logging source-interface** *type interface-path-id* **Example:** `RP/0/0/CPU0:router(config)# logging source-interface HundredGigE 0/1/0/0`	(Optional) Sets the syslog source address. • By default, a syslog message sent to a syslog server contains the IP address (IPv4 and IPv6 are supported) of the interface it uses to leave the router. • Use this command to set all syslog messages being sent from the router to contain the same IP address, regardless of which interface the syslog message uses to exit the router.
Step 7	**commit**	

Configuring the Settings for the Logging History Table

This task explains how to configure the settings for the logging history table.

For conceptual information, see the Severity Levels, on page 9 section.

Before You Begin

Logging of messages to an SNMP NMS is enabled by the **snmp-server enable traps syslog** command. For more information about SNMP, see the Related Documents, on page 25 section.

SUMMARY STEPS

1. **configure**
2. **logging history** *severity*
3. **logging history size** *number*
4. **commit**
5. **show logging history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**logging history** *severity* **Example:** `RP/0/0/CPU0:router(config)# logging history errors`	Changes the default severity level of syslog messages stored in the history file and sent to the SNMP server. • By default, syslog messages at or below the **warnings** severity level are stored in the history file and sent to the SNMP server.
Step 3	**logging history size** *number* **Example:** `RP/0/0/CPU0:router(config)# logging history size 200`	Changes the number of syslog messages that can be stored in the history table. • By default, one syslog message is stored in the history table. **Note** When the history table is full (that is, when it contains the maximum number of messages specified with this command), the oldest message is deleted from the table to allow the new message to be stored.
Step 4	**commit**	
Step 5	**show logging history** **Example:** `RP/0/0/CPU0:router# show logging history`	(Optional) Displays information about the state of the syslog history table.

Modifying Logging to the Console Terminal and the Logging Buffer

This task explains how to modify logging configuration for the console terminal and the logging buffer.

Note Logging is enabled by default.

SUMMARY STEPS

1. **configure**
2. **logging buffered** [*size* | *severity*]
3. **logging console** [*severity*]
4. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**logging buffered** [*size* | *severity*] **Example:** `RP/0/0/CPU0:router(config)# logging buffered size 60000`	Specifies the logging buffer as a destination for syslog messages, sets the size of the logging buffer, and limits the syslog messages sent to the logging buffer based on severity. • The default for the *size* argument is 4096 bytes. • The default for the *severity* argument is **debugging**. • Keyword options for the *severity* argument are **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**. • By default, entering this command without specifying a severity level for the *severity* argument or specifying the size of the buffer for the *size* argument sets the severity level to **debugging** and the buffer size to 4096 bytes.
Step 3	**logging console** [*severity*] **Example:** `RP/0/0/CPU0:router(config)# logging console alerts`	Limits messages sent to the console terminal based on severity. • Syslog messages are logged to the console terminal at the **informational** severity level by default. • Keyword options for the *severity* argument are **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**. • Entering this command without specifying a severity level for the *severity* argument sets the severity level to **informational**. **Note** Use this command to reenable logging to the console terminal if it was disabled with the **logging console disable** command.
Step 4	**commit**	

Modifying the Format of Time Stamps

This task explains how to modify the time-stamp format for syslog and debugging messages.

SUMMARY STEPS

1. **configure**
2. Do one of the following:
   - **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]
   - **service timestamps log uptime**
3. Do one of the following:
   - **service timestamps debug datetime** [**localtime**] [**msec**] [**show-timezone**]
   - **service timestamps debug uptime**
4. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	

Step 2	Do one of the following:
	• **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]
	• **service timestamps log uptime**
	Example:
	`RP/0/0/CPU0:router(config)# service timestamps log datetime localtime msec`
	or
	`RP/0/0/CPU0:router(config)# service timestamps log uptime`
		Modifies the time-stamp format for syslog messages.
		• By default, time stamps are enabled. The default time-stamp format is month day HH:MM:SS.
		• Issuing the **service timestamps log datetime** command configures syslog messages to be time-stamped with the date and time.
		◦ The optional **localtime** keyword includes the local time zone in time stamps.
		◦ The optional **msec** keyword includes milliseconds in time stamps.
		◦ The optional **show-timezone** keyword includes time zone information in time stamps.
		• Issuing the **service timestamps log uptime** command configures syslog messages to be time-stamped with the time that has elapsed since the router last rebooted.
		◦ The **service timestamps log uptime** command configures time-stamps to be configured in HHHH:MM:SS, indicating the time since the router last rebooted.

Step 3	Do one of the following: • **service timestamps debug datetime** [**localtime**] [**msec**] [**show-timezone**]	Modifies the time-stamp format for debugging messages. • By default, time-stamps are enabled. The default time stamp format is month day HH:MM:SS.

	Command or Action	Purpose

	• **service timestamps debug uptime**
	
	Example:
	
	`RP/0/0/CPU0:router(config)# service timestamps debug datetime msec show-timezone`
	or
	
	`RP/0/0/CPU0:router(config)# service timestamps debug uptime`
		• Issuing the **service timestamps log datetime** command configures debugging messages to be time-stamped with the date and time.
		◦ The optional **localtime** keyword includes the local time zone in time stamps.
		◦ The optional **msec** keyword includes milliseconds in time stamps.
		◦ The optional **show-timezone** keyword includes time zone information in time stamps.
		• Issuing the **service timestamps log uptime** command configures debugging messages to be time-stamped with the time that has elapsed since the networking device last rebooted.
		Tip Entering the **service timestamps** command without any keywords or arguments is equivalent to entering the **service timestamps debug uptime** command.

Step 4	**commit**	

Disabling Time Stamps

This tasks explains how to disable the inclusion of time stamps in syslog messages.

SUMMARY STEPS

1. **configure**
2. Do one of the following:
   - **service timestamps disable**
   - **no service timestamps** [**debug** | **log**] [**datetime** [**localtime**] [**msec**] [**show-timezone**]] | **uptime**]
3. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	Do one of the following:	Disables the inclusion of time stamps in syslog messages.

	Command or Action	Purpose
	• **service timestamps disable** • **no service timestamps** [**debug** | **log**] [**datetime** [**localtime**] [**msec**] [**show-timezone**]] | **uptime**]	**Note** Both commands disable the inclusion of time stamps in syslog messages; however, specifying the **service timestamps disable** command saves the command to the configuration, whereas specifying the **no** form of the **service timestamps** command removes the command from the configuration.
Step 3	**commit**	

Suppressing Duplicate Syslog Messages

This task explains how to suppress the consecutive logging of duplicate syslog messages.

SUMMARY STEPS

1. **configure**
2. **logging suppress duplicates**
3. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**logging suppress duplicates** **Example:** `RP/0/0/CPU0:router(config)# logging suppress duplicates`	Prevents the consecutive logging of duplicate syslog messages. **Caution** If this command is enabled during debugging sessions, you could miss important information related to problems that you are attempting to isolate and resolve. In such a case, you might consider disabling this command.
Step 3	**commit**	

Disabling the Logging of Link-Status Syslog Messages

This task explains how to disable the logging of link-status syslog messages for logical and physical links.

When the logging of link-status messages is enabled, the router can generate a high volume of link-status updown syslog messages. Disabling the logging of link-status syslog messages reduces the number of messages logged.

SUMMARY STEPS

1. **configure**
2. **logging events link-status disable**
3. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**logging events link-status disable** **Example:** `RP/0/0/CPU0:router(config)# logging events link-status disable`	Disables the logging of link-status syslog messages for software (logical) and physical links. • The logging of link-status syslog messages is enabled by default for physical links. • To enable link-status syslog messages for both physical and logical links, use the **logging events link-status software-interfaces** command. • Use the **no logging events link-status** command to enable link-status syslog messages on physical links only.
Step 3	**commit**	

Displaying System Logging Messages

This task explains how to display the syslog messages stored in the logging buffer.

Note The commands can be entered in any order.

SUMMARY STEPS

1. **show logging**
2. **show logging location** *node-id*
3. **show logging process** *name*
4. **show logging string** *string*
5. **show logging start** *month day hh*:*mm*:*ss*
6. **show logging end** *month day hh*:*mm*:*ss*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show logging** **Example:** `RP/0/0/CPU0:router# show logging`	Displays all syslog messages stored in the buffer.
Step 2	**show logging location** *node-id* **Example:** `RP/0/0/CPU0:router# show logging location 0/1/CPU0`	Displays syslog messages that have originated from the designated node.
Step 3	**show logging process** *name* **Example:** `RP/0/0/CPU0:router# show logging process init`	Displays syslog messages that are related to the specified process.
Step 4	**show logging string** *string* **Example:** `RP/0/0/CPU0:router# show logging string install`	Displays syslog messages that contain the specified string.
Step 5	**show logging start** *month day hh*:*mm*:*ss* **Example:** `RP/0/0/CPU0:router# show logging start december 1 10:30:00`	Displays syslog messages in the logging buffer that were generated on or after the specified date and time.
Step 6	**show logging end** *month day hh*:*mm*:*ss* **Example:** `RP/0/0/CPU0:router# show logging end december 2 22:16:00`	Displays syslog messages in the logging buffer that were generated on or before the specified date and time.

Archiving System Logging Messages to a Local Storage Device

This task explains how to display save syslog messages to an archive on a local storage device.

Before You Begin

Note The local storage device must have enough space available to store the archive files. We recommend that syslogs be archived to the harddisk because it has more capacity than flash disks.

SUMMARY STEPS

1. **configure**
2. **logging archive**
3. **device** {**disk0** | **disk1** | **harddisk**}
4. **frequency** {**daily** | **weekly**}
5. **severity** *severity*
6. **archive-length** *weeks*
7. **archive-size** *size*
8. **file-size** *size*
9. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**logging archive** **Example:** `RP/0/0/CPU0:router(config)# logging archive`	Enters logging archive configuration mode.
Step 3	**device** {**disk0**	**disk1**	**harddisk**} **Example:** `RP/0/0/CPU0:router(config-logging-arch)# device disk1`	Specify the device to be used for logging syslogs. • This step is required. If the device is not configured, then all other logging archive configurations are rejected. • We recommend that syslogs be archived to the harddisk because it has more capacity than flash disks. • By default, the logs are created under the directory <device>/var/log
Step 4	**frequency** {**daily**	**weekly**} **Example:** `RP/0/0/CPU0:router(config-logging-arch)# frequency weekly`	(Optional) Specifies if logs are collected on a daily or weekly basis. Logs are collected daily by default.
Step 5	**severity** *severity* **Example:** `RP/0/0/CPU0:router(config-logging-arch)# severity warnings`	(Optional) Specifies the minimum severity of log messages to archive. All syslog messages greater than or equal to this configured level are archived while those lesser than this are filtered out. The severity levels are: • emergencies • alerts • critical

	Command or Action	Purpose
		• errors • warnings • notifications • informational • debugging See the Syslog Message Severity Level Definitions, on page 11 section for information.
Step 6	**archive-length** *weeks* **Example:** `RP/0/0/CPU0:router(config-logging-arch)# archive-length 6`	(Optional) Specifies the maximum number of weeks that the archive logs are maintained in the archive. Any logs older than this number are automatically removed from the archive. By default, archive logs are stored for 4 weeks.
Step 7	**archive-size** *size* **Example:** `RP/0/0/CPU0:router(config-logging-arch)# archive-size 50`	(Optional) Specifies the maximum total size of the syslog archives on a storage device. If the size is exceeded then the oldest file in the archive is deleted to make space for new logs. The default archive size is 20 MB.
Step 8	**file-size** *size* **Example:** `RP/0/0/CPU0:router(config-logging-arch)# file-size 10`	(Optional) Specifies the maximum file size (in megabytes) that a single log file in the archive can grow to. Once this limit is reached, a new file is automatically created with an increasing serial number. By default, the maximum file size is 1 megabyte.
Step 9	**commit**	

Configuration Examples for Implementing Logging Services

This section provides these configuration examples:

Configuring Logging to the Console Terminal and the Logging Buffer: Example

This example shows a logging configuration where logging to the logging buffer is enabled, the severity level of syslog messages sent to the console terminal is limited to syslog messages at or below the **critical** severity level, and the size of the logging buffer is set to 60,000 bytes.

```
!
logging console critical
logging buffered 60000
!
```

Setting Up Destinations for Syslog Messages: Example

This example shows a logging configuration where logging is configured to destinations other than the console terminal. In this configuration, the following is configured:

- Logging is enabled to destinations other than the console terminal.
- Syslog messages at or below the **warnings** severity level are sent to syslog server hosts.
- Syslog messages at or below the **critical** severity level are sent to terminal lines.
- The size of the logging buffer is set to 60,000 bytes.
- The syslog server host at IP addresses 172.19.72.224 (IPv4) and 2001:DB8:A00:1::1/64 (IPv6) are configured as recipients for syslog messages.

```
!
logging trap warnings
logging monitor critical
logging buffered 60000
logging 172.19.72.224
logging 2001:DB8:A00:1::1/64
!
```

Configuring the Settings for the Logging History Table: Example

This example shows a logging configuration in which the size of the logging history table is to 200 entries and the severity of level of syslog messages sent to the logging history table is limited to messages at or below the **errors** severity level:

```
logging history size 200
logging history errors
```

Modifying Time Stamps: Example

This example shows a time-stamp configuration in which time stamps are configured to follow the format month date HH:MM:SS time zone:

```
service timestamps log datetime show-timezone
```

This example shows a time-stamp configuration in which time stamps are configured to follow the format month date HH:MM:SS.milliseconds time zone:

```
service timestamps log datetime msec show-timezone
```

Configuring a Logging Archive: Example

This example shows how to configure a logging archive, and define the archive attributes:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# logging archive
RP/0/0/CPU0:router(config-logging-arch)# device disk1
```

```
RP/0/0/CPU0:router(config-logging-arch)# frequency weekly
RP/0/0/CPU0:router(config-logging-arch)# severity warnings
RP/0/0/CPU0:router(config-logging-arch)# archive-length 6
RP/0/0/CPU0:router(config-logging-arch)# archive-size 50
RP/0/0/CPU0:router(config-logging-arch)# file-size 10
```

Where to Go Next

To configure alarm log correlation, see the *Implementing and Monitoring Alarms and Logging Correlation* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

Additional References

The following sections provide references related to implementing logging services on Cisco IOS XR software .

Related Documents

Related Topic	Document Title
Logging services command reference	*Logging Services Commands* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco XR 12000 Series Router*
Onboard Failure Logging (OBFL) configuration	*Onboard Failure Logging Commands* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.
Onboard Failure Logging (OBFL) commands	*Onboard Failure Logging Commands* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco XR 12000 Series Router*.
Alarm and logging correlation commands	*Alarm Management and Logging Correlation Commands* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco XR 12000 Series Router*.
Alarm and logging correlation configuration and monitoring tasks	*Implementing and Monitoring Alarms and Alarm Log Correlation* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.
SNMP commands	*SNMP Commands* module in the *Cisco IOS XR System Monitoring Command Reference for the Cisco XR 12000 Series Router*.
SNMP configuration tasks	*Implementing SNMP* module in the *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*

Related Topic	Document Title
Cisco IOS XR getting started material	*Cisco IOS XR Getting Started Guide for the Cisco XR 12000 Series Router*
Information about user groups and task IDs	*Configuring AAA Services* module in the *Cisco IOS XR System Security Command Reference for the Cisco XR 12000 Series Router*.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	*http://www.cisco.com/cisco/web/support/index.html*