CHAPTER 1

Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco 4700 Series Application Control Engine (ACE) appliance. Each ACE contains a number of log files that retain records of specified ACE-related activities and the performance of various ACE functions. You can access these log files using the ACE CLI to troubleshoot problems or to better understand the operation of the ACE.

This chapter includes the following major sections:

- Information About System Message Logging
- Guidelines and Limitations
- Default Settings
- Configuring System Message Logging
- Clearing Log Messages
- Viewing Log Message Information

Information About System Message Logging

This section includes the following topics:

- Overview
- Log Message Format
- Logging Severity Levels
- Variables

Overview

The system message logging function of the ACE saves these messages in a log file and allows you to send the logging messages to one or more output locations. System log messages provide you with logging information for monitoring and troubleshooting the operation of the ACE. By default, messages are not saved in a log file. You must enable the transmission of syslog messages to a specified output location.

The logging configuration is flexible and allows you to customize many aspects of how the ACE handles system messages. Using the system message logging feature, you can do the following:

- Specify one or more output locations where messages should be sent, including the console, an internal buffer, one or more syslog servers, an SNMP network management station, to Telnet or SSH sessions, or to Flash memory on the ACE.
- Specify which messages should be logged.
- Specify the severity level of a message.
- Enable time stamps.
- Specify the unique device ID of the ACE that is sent to a syslog server.
- Change the size of the logging message queue.
- Limit the rate at which the ACE generates messages in the syslog.
- Enable the logging of connection setup and teardown messages.

Note Not all system messages indicate an error condition. Some messages report normal events or log a configuration change.

Log Message Format

The ACE supports the EMBLEM syslog format for logging with each syslog server. The EMBLEM syslog format is consistent with the Cisco IOS software format and is compatible with CiscoWorks management applications. EMBLEM-format logging is available for UDP syslog messages only.

System log messages begin with a percent sign (%) and are structured as follows:

```
%<ACE>-Level-[Subfacility]-Message_number: Message_text
```

ACE	Identifies the message facility code for messages generated by the ACE. This value is always ACE.
Level	Level reflects the severity of the condition described by the message. The levels are 0 to 7. The lower the number, the more severe the condition. See Table 1-1 for a summary of logging severity levels. See Chapter 3, Messages Listed by Severity Level for a listing of ACE system log messages by severity code.
Subfacility	(Optional) Name of the component or subcomponent that initiated the system log message (for example, IFMGR).
Message_number	Unique 6-digit number that identifies the message. See Chapter 2, System Messages, for a detailed list of the ACE system log messages. The messages are listed numerically by message code.
Message_text	A text string describing the condition. This portion of the message sometimes includes virtual context, virtual user, IP addresses, port numbers, usernames, and so on.

Note Syslog messages received at the ACE serial console contain only the code portion of the message.

For example, this syslog message shows the information that is displayed when you assign a VLAN number to the ACE:

```
%ACE-6-615004 : VLAN <VLAN-number> available for configuring an interface
```

Where *VLAN-number* identifies the VLAN number assigned to the ACE. The ACE can use that VLAN to configure an interface and receive traffic.

Logging Severity Levels

You instruct the ACE which system messages to log by specifying a logging level. The logging level designates that the ACE logs emergency, alert, critical, error, or warning messages for the various software functions. The ACE also logs notification, informational, and debugging messages. The ACE supports eight logging levels to identify a wide range of critical and noncritical logged events that may occur on an ACE. Severity level values are 0 to 7; the lower the level number, the more severe the error.

The level you specify causes the ACE to apply the command to messages of that level or lower. For example, if you enter a command that specifies severity level 3, the ACE applies the command results to messages with a severity level of 0, 1, 2, and 3.

Table 1-1 lists the log message severity levels.

Table 1-1 Log Message Severity Levels

Level Number	Level Keyword	Description
0	**emergency**	System unusable (for example, the ACE has shut down and cannot be restarted, or it has experienced a hardware failure).
1	**alert**	Immediate action needed (for example, one of the ACE subsystems is not running).

Table 1-1 Log Message Severity Levels (continued)

Level Number	Level Keyword	Description
2	**critical**	Critical condition (for example, the ACE has encountered a critical condition that requires immediate attention).
3	**error**	Error condition (for example, error messages about software or hardware malfunctions).
4	**warning**	Warning condition (for example, the ACE encountered an error condition that requires attention but is not interfering with the operation of the device).
5	**notification**	Normal but significant condition (for example, interface up/down transitions and system restart messages).
6	**informational**	Informational message only (for example, reload requests and low-process stack messages).
7	**debugging**	Appears during debugging only.

Variables

Log messages often contain variables. Table 1-2 lists most variables that are used in this guide to describe ACE log messages. Some variables that appear in only one log message are not listed.

Table 1-2 Variable Fields in Syslog Messages

Type	Variable	Type of Information
Misc.	*command*	Command name.
	device	Memory storage device. For example, Flash memory, TFTP, the failover standby unit, or the console terminal.
	filename	Filename of the type ACE image or configuration.
	privilege_level	User privilege level.
	reason	Text string describing the reason for the message.
	string	Text string (for example, a username).
	url	URL.
	user	Username.
Numbers	*number*	Number. The exact form depends on the log message.
	bytes	Number of bytes.
	code	Decimal number returned by the message to indicate the cause or source of the error, depending on the message.
	connections	Number of connections.
	time	Duration, in the format *hh*:*mm*:*ss*.
	dec	Decimal number.
	hex	Hexadecimal number.
	octal	Octal number.

Table 1-2 Variable Fields in Syslog Messages (continued)

Type	Variable	Type of Information
Addresses	*IP_address*	IP address in the form *n.n.n.n*, where *n* is an integer from 1 to 255.
	MAC_address	MAC address.
	global_address	Global IP address, an address on a lower security level interface.
	source_address	Source address of a packet.
	dest_address	Destination address of a packet.
	real_address	Real IP address, before Network Address Translation (NAT).
	mapped_address	Translated IP address.
	gateway_address	Network gateway IP address.
	netmask	Subnet mask.
Interfaces	*interface_number*	Interface number, **1** to *n*, where the number is determined by the order the interfaces load in the ACE. Use the **show interface internal** command to view detailed information about the interfaces.
	interface_name	Name assigned to the interface. Use the **show interface** command to view the interfaces and their names.
Ports, Services, and Protocols	*port*	TCP or UDP port number.
	source_port	Source port number.
	dest_port	Destination port number.
	real_port	Real port number, before NAT.
	mapped_port	Translated port number.
	global_port	Global port number.
	protocol	Protocol of the packet, for example, ICMP, TCP, or UDP.
	service	Service specified by the packet, for example, SNMP or Telnet.

Guidelines and Limitations

This section describes the guidelines and limitations for the system message logging function and includes the following topics:

- ACE Buffer Limitations
- View Logs that the ACE Saves
- Multiple-Context Mode Logging

ACE Buffer Limitations

The ACE saves syslog messages in an internal buffer that can store up to 8192 messages. By default, the ACE can hold 80 syslog messages in the message queue while awaiting processing.

View Logs that the ACE Saves

To view logs generated by the ACE, you must configure an output location. You can choose to send all messages, or subsets of messages, to one or more output locations. You can limit which messages are sent to an output location by specifying the severity level of the message.

Multiple-Context Mode Logging

If the ACE is operating in multiple-context mode, you can configure the ACE to include an identifier for the virtual context and the virtual user responsible for executing the function in the log message.

Default Settings

Table 1-3 lists the default settings for the ACE system message logging function.

Table 1-3 Default System Message Logging Parameters

Parameters	Default
Message logging	Disabled
Message queue	80 messages
Local buffer logging	Disabled
Remote connection logging using the Secure Shell (SSH) or Telnet	Disabled
Console session syslog message display	Disabled
Syslog server logging on a host	Disabled
Traps and inform requests to an SNMP network management station (NMS)	Disabled
ACE Flash memory logging	Disabled
Message time stamp	Disabled
Logging facility	20 (LOCAL4)
Message rate limiting	Disabled
Connection setup and teardown syslog message logging through the control plane	Enabled

Configuring System Message Logging

This section includes the following topics:

- Task Flow for Configuring System Message Logging
- Enabling or Disabling System Message Logging
- Specifying Syslog Output Locations
- Enabling Time Stamps on System Messages
- Identifying Messages Sent to a Syslog Server
- Specifying an ACE Device ID for Messages to a Syslog Server
- Changing the Syslog Logging Facility
- Changing the Logging Message Queue
- Disabling a Syslog Message or Changing its Severity Level
- Limiting the Syslog Rate
- Enabling Logging on the Standby ACE
- Enabling the Logging of Connection Setup and Teardown Syslog Messages Through the Fastpath

Task Flow for Configuring System Message Logging

Follow these steps to configure system message logging:

Step 1 If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.

```
host1/Admin# changeto C1
host1/C1#
```

The rest of the examples in this procedure use the Admin context, unless otherwise specified. For details on creating contexts, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Step 2 Enter configuration mode by entering **config**.

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

Step 3 Enable logging to send system log messages to one or more output locations.

```
host1/Admin(config)# logging enable
```

Step 4 Configure the ACE system software to send system logging messages to the output locations of your choice.

For example, to set the logging buffer level to 3 for logging error messages, enter:

```
host1/Admin(config)# logging buffered 3
```

For example, to send log messages to a syslog server, enter:

```
host1/Admin(config)# logging host 192.168.10.1
```

Step 5 (Optional) Enable the display of a time stamp on system logging messages.

```
host1/Admin(config)# logging timestamp
```

Step 6 (Optional) Limit the number of messages sent to a syslog server based on severity.

```
host1/Admin(config)# logging trap 6
```

Step 7 (Optional) Display a unique device ID in non-EMBLEM format syslog messages sent to the syslog server.

```
host1/Admin(config)# logging device-id hostname
```

Step 8 (Optional) Set the syslog logging facility to a value other than the default of 20 (LOCAL4).

```
host1/Admin(config)# logging facility 16
```

Step 9 (Optional) Change the number of syslog messages that can appear in the message queue while awaiting processing.

```
host1/Admin(config)# logging queue 100
```

Step 10 (Optional) Disable the display of a specific syslog message or change the severity level of a specific system log message.

For example, to disable the %<ACE>-6-615004 syslog message, enter:

```
host1/Admin(config)# no logging message 615004
```

For example, to change the level of the 615004 syslog message, enter:

```
(config)# logging message 615004 level 5
```

Step 11 (Optional) Limit the rate at which the ACE generates messages in the syslog.

```
host1/Admin(config)# logging rate-limit 42 60 level 6
```

Step 12 (Optional) Enable logging on the failover standby ACE.

```
host1/Admin(config)# logging standby
```

Step 13 (Optional) Enable the logging of connection setup and teardown messages at a faster rate (that is, at the connection rate).

```
host1/Admin(config)# logging fastpath
```

Step 14 (Optional) Save your configuration changes to Flash memory.

```
host1/Admin(config)# exit
host1/Admin# copy running-config startup-config
```

Enabling or Disabling System Message Logging

Message logging is disabled by default. You must enable logging if you want to send messages to one or more output locations. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Prerequisites

You must set a logging output location to view any logs (see the "Specifying Syslog Output Locations" section).

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging enable** **Example:** host1/Admin(config)# logging enable	Enables message logging.
Step 3	**no logging enable** **Example:** host1/Admin(config)# no logging enable	(Optional) Disables message logging.
Step 4	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Specifying Syslog Output Locations

You configure the ACE to send syslog messages to the output location of your choice. The ACE provides several output locations for sending syslog messages:

- An internal buffer on the ACE
- One or more syslog servers running on hosts
- A Telnet or SSH connection
- The console

Note We recommend sending syslog messages directly to the console only during testing.

- An SNMP network management station
- Flash memory

This section includes the following topics:

- Sending Syslog Messages to a Buffer
- Sending Syslog Messages to a Telnet or SSH Session
- Sending Syslog Messages to the Console
- Sending Syslog Messages to a Syslog Server
- Sending Syslog Messages as Traps to an SNMP Network Management Station

- Sending Syslog Messages to Flash Memory on the ACE

Sending Syslog Messages to a Buffer

By default, logging to the local buffer on the ACE is disabled. To enable system logging to a local buffer and to limit the messages sent to the buffer based on severity, use the **logging buffered** configuration mode command. New messages append to the end of the buffer. The first message displayed is the oldest message in the buffer. When the log buffer fills, the ACE deletes the oldest message to make space for new messages.

Prerequisite

You must enable logging on the ACE using the **logging enable** command before messages are sent to the specified output device. See the "Enabling or Disabling System Message Logging" section.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging buffered** *severity_level* **Example:** host1/Admin(config)# logging buffered 3	Enables system message logging to a local buffer and limits the messages sent to the buffer based on severity level. The *severity_level* argument specifies the maximum level for system log messages sent to the buffer. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. Allowable entries include: • **0—emergencies** (System unusable messages) • **1—alerts** (Take immediate action) • **2—critical** (Critical condition) • **3—errors** (Error message) • **4—warnings** (Warning message) • **5—notifications** (Normal but significant condition) • **6—informational** (Information message) • **7—debugging** (Debug messages)
Step 3	**no logging buffered** **Example:** host1/Admin(config)# no logging buffered 3	(Optional) Disables system message logging to the local buffer.
Step 4	**clear logging** **Example:** host1/Admin(config)# clear logging	(Optional) Clears the messages that the logging buffer currently contains to make it easier to view new messages. See the "Clearing Log Messages" section.

	Command	Purpose
Step 5	**show logging** **Example:** host1/Admin(config)# show logging	(Optional) Displays the messages that the logging buffer currently contains. See the "Viewing Log Message Information" section.
Step 6	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Sending Syslog Messages to a Telnet or SSH Session

By default, logging to a remote connection using the Secure Shell (SSH) or Telnet is disabled on the ACE. You can display log messages on a remote SSH or Telnet connection by setting the logging preferences for Telnet and SSH sessions. To display syslog messages as they occur when accessing the ACE through an SSH or Telnet sessions, use the following commands:

- **terminal monitor**—Exec mode command that enables syslog messages for all sessions in the current context and sets the logging preferences for each individual Telnet session (see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*).
- **logging monitor**—Configuration mode command that sets the logging preferences for all SSH and Telnet sessions. You can limit the display of messages based on severity.

Prerequisites

This configuration topic includes the following prerequisites:

- If you have not done so already, enable remote access on the ACE and establish a remote connection using the Secure Shell (SSH) or Telnet protocols from a PC. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for details.
- You must enable logging on the ACE using the **logging enable** command before messages are sent to the specified output device. See the "Enabling or Disabling System Message Logging" section.

Detailed Steps

	Command	Purpose
Step 1	**terminal monitor** **Example:** host1/Admin# terminal monitor	Enables the terminal monitor function.
Step 2	**config** **Example:** host1/Admin# config Enter configuration commands, one per line. End with CNTL/Z (config)#	Enters global configuration mode.

	Command	Purpose
Step 3	**logging monitor** *severity_level* **Example:** host1/Admin(config)# logging monitor 6	Enables syslog messages to display as they occur when accessing the ACE through an SSH or Telnet sessions. The *severity_level* argument specifies the maximum level for system log messages to display during the current Telnet or SSH session. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. Allowable entries include: • **0—emergencies** (System unusable messages) • **1—alerts** (Take immediate action) • **2—critical** (Critical condition) • **3—errors** (Error message) • **4—warnings** (Warning message) • **5—notifications** (Normal but significant condition) • **6—informational** (Information message) • **7—debugging** (Debug messages)
Step 4	**no logging monitor** **Example:** host1/Admin(config)# no logging monitor	(Optional) Disables system message logging to the current SSH or Telnet session.
Step 5	**terminal no monitor** **Example:** host1/Admin(config)# exit host1/Admin# terminal no monitor host1/Admin# config host1/Admin(config)#	(Optional) Disables the terminal monitor function.
Step 6	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Sending Syslog Messages to the Console

By default, the ACE does not display syslog messages during console sessions. To enable the logging of syslog messages during console sessions and to limit the display of messages based on severity, use the **logging console** configuration command.

Restriction

Logging to the console can degrade system performance. Use the **logging console** command only when you are testing and debugging problems, or when there is minimal load on the network. Do not use this command when the network is busy, as it can reduce ACE performance. When the ACE is active, use the following commands:

- The **logging buffered** command to store message
- The **show logging** command to view messages
- The **clear logging** command to clear the messages displayed by the **logging buffered** command

Prerequisite

You must enable logging on the ACE using the **logging enable** command before messages are sent to the specified output device. See the "Enabling or Disabling System Message Logging" section.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging console** *severity_level* **Example:** host1/Admin(config)# logging buffered 3	Enables system message logging to the console and limits the messages sent to the buffer based on severity level. The *severity_level* argument specifies the maximum level for system log messages sent to the console. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. Allowable entries include: • **0—emergencies** (System unusable messages) • **1—alerts** (Take immediate action) • **2—critical** (Critical condition) • **3—errors** (Error message) • **4—warnings** (Warning message) • **5—notifications** (Normal but significant condition) • **6—informational** (Information message) • **7—debugging** (Debug messages)

	Command	Purpose
Step 3	**no logging console** **Example:** host1/Admin(config)# no logging buffered 3	(Optional) Disables system message logging to the console.
Step 4	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Sending Syslog Messages to a Syslog Server

By default, logging to a syslog server on a host is disabled on the ACE. If you choose to send log messages to a host, the ACE sends those messages using either UDP or TCP.

Restriction

You can use either UDP or TCP to send messages to the syslog server. UDP-based logging does not prevent the ACE from passing traffic if the syslog server fails. If you use TCP as the logging transport protocol, the ACE denies new network access sessions as a security measure if the ACE is unable to reach the syslog server, if the syslog server is misconfigured, if the TCP queue is full, or if the disk is full.

Prerequisites

This configuration topic includes the following prerequisites:

- You must enable logging on the ACE using the **logging enable** command before messages are sent to the specified output device. See the "Enabling or Disabling System Message Logging" section.
- The host must run a program (known as a server) called syslogd, which is a daemon that accepts messages from other applications and the network, and writes them out to system wide log files. UNIX provides the syslog server as part of its operating system. For Microsoft Windows, you must obtain a syslog server for the Windows operating system.
- To identify which messages are sent to a syslog server, you must also configure the **logging trap** command. The **logging trap** command limits the logging messages sent to a syslog server based on severity. See the "Identifying Messages Sent to a Syslog Server" section.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging host** *ip_address* [**tcp** | **udp** [*/port#*]} | [**default-udp**] | [**format emblem**]]] **Example:** host1/Admin(config)# logging host 192.168.10.1 tcp1025 format emblem default-udp	Enables logging to a syslog server. The keywords and arguments are as follows: • *ip_address*—Specifies the IP address of the host to be used as the syslog server. • **tcp**—(Optional) Specifies to use TCP to send messages to the syslog server. A server can only be specified to receive either UDP or TCP, not both. • **udp**—(Optional) Specifies to use UDP to send messages to the syslog server. A server can only be specified to receive either UDP or TCP, not both. • */port#*—(Optional) Port that the syslog server listens to for syslog messages. Valid values are as from 1025 to 65535. The default protocol and port are UDP/514. The default TCP port, if specified, is 1470. • **default-udp**—(Optional) Instructs the ACE to default to UDP if the TCP transport fails to communicate with the syslog server. • **format emblem**—(Optional) Enables EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for either TCP or UDP syslog messages. If you enable EMBLEM-format logging for a particular syslog host, then the messages are sent to that host. The Cisco Resource Management Environment (RME) is a network management application that collects syslogs. RME can process syslog messages only if they are in EMBLEM format. For example, the EMBLEM format for a message with time stamp appears as follows: `ipadress or dns name [Dummy Value/Counter]: [mmm dd hh:mm:ss TimeZone]: %FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: [vtl-ctx: context id] Message-text`
Step 3	**no logging host** *ip_address* **Example:** host1/Admin(config)# no logging host 192.168.10.1	(Optional) Disables logging to a syslog server.
Step 4	**logging timestamp** **Example:** host1/Admin(config)# logging timestamp	(Optional) Sends messages to the syslog server with a time stamp. See the "Enabling Time Stamps on System Messages" section.

	Command	Purpose
Step 5	**logging device-id** **Example:** host1/Admin(config)# logging device-id	(Optional) Specifies that the device ID of the ACE is included in the syslog message, use the **logging device-id** command. Once enabled, the ACE includes a unique device ID in non-EMBLEM format syslog messages sent to the syslog server. The device ID specification does not affect the syslog message text that is in EMBLEM format.
Step 6	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Sending Syslog Messages as Traps to an SNMP Network Management Station

By default, the ACE does not send traps and inform requests to an SNMP network management station (NMS). To enable the ACE to send system messages as traps to the NMS, use the **logging history** configuration mode command.

Prerequisites

This configuration topic includes the following prerequisites:

- You must enable syslog traps by using the **snmp-server enable traps** configuration command. For details on configuring SNMP, see the *Cisco 4700 Series Application Control Engine Appliance Administration Guide*
- You must enable logging on the ACE using the **logging enable** command before messages are sent to the specified output device. See the "Enabling or Disabling System Message Logging" section.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging history** *severity_level* **Example:** host1/Admin(config)# logging history 6	(Optional) Enables the ACE to send system messages as traps to the NMS. The *severity_level* argument specifies the maximum level for system log messages sent as traps to the NMS. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. Allowable entries include: • **0—emergencies** (System unusable messages) • **1—alerts** (Take immediate action) • **2—critical** (Critical condition) • **3—errors** (Error message) • **4—warnings** (Warning message) • **5—notifications** (Normal but significant condition) • **6—informational** (Information message) • **7—debugging** (Debug messages) **Note** We recommend that you use the debugging (7) level during initial setup and during testing. After setup, set the level from debugging (7) to a lower value for use in your network.
Step 3	**no logging history** **Example:** host1/Admin(config)# no logging history	(Optional) Disables sending system message logs as traps to an SNMP NMS.
Step 4	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Sending Syslog Messages to Flash Memory on the ACE

By default, logging to Flash memory is disabled on the ACE. The ACE allows you to specify that system message logs that you want to keep after a system reboot by saving them to Flash memory. To send specific log messages to Flash memory on the ACE, use the **logging persistent** configuration mode command.

After you enable the logging persistence function the ACE starts logging messages to a file in disk0: with name messages. For example, enter:

```
host1/Admin(config)# logging persistent 7
host1/Admin(config)# end
host1/Admin# dir disk0:

12 Jul 26 2008 02:57:04 messages

           Usage for disk0: filesystem
                    5903360 bytes total used
                    5261312 bytes free
                   11164672 bytes total
host1/Admin#
```

Prerequisite

You must enable logging on the ACE using the **logging enable** command before messages are sent to the specified output device. See the "Enabling or Disabling System Message Logging" section.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging persistent** *severity_level* **Example:** host1/Admin(config)# logging persistent 6	Enables system message logging to Flash memory. The *severity_level* argument sets the maximum level for system log messages sent to Flash memory. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. We recommend that you use a lower severity level, such as 3, since logging at a high rate to Flash memory on the ACE may impact performance. Allowable entries include: • **0—emergencies** (System unusable messages) • **1—alerts** (Take immediate action) • **2—critical** (Critical condition) • **3—errors** (Error message) • **4—warnings** (Warning message) • **5—notifications** (Normal but significant condition) • **6—informational** (Information message) • **7—debugging** (Debug messages)

	Command	Purpose
Step 3	**no logging persistent** **Example:** host1/Admin(config)# no logging persistent	(Optional) Disables system message logging to Flash memory.
Step 4	**show file disk 0:** **Example:** host1/Admin(config)# show file disk0:	(Optional) Displays the context of the log file.
Step 5	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Enabling Time Stamps on System Messages

By default, the ACE does not include the date and time in syslog messages. To specify that syslog messages should include the date and time that the message was generated, use the **logging timestamp** configuration mode command.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging timestamp** **Example:** host1/Admin(config)# logging timestamp	Enables the time stamp display on system logging messages.
Step 3	**no logging timestamp** **Example:** host1/Admin(config)# no logging timestamp	(Optional) Disables the time stamp display on system logging messages.
Step 4	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Identifying Messages Sent to a Syslog Server

To identify which messages are sent to a syslog server, use the **logging trap** configuration command. The **logging trap** command limits the logging messages sent to a syslog server based on severity.

Prerequisite

To send logging messages to a syslog server, use the **logging host** command to specify the name or IP address of the host to be used as the syslog server (see the "Sending Syslog Messages to a Syslog Server" section).

Detailed Steps

	Command	Purpose

Step 1	**config**
	
	Example:
	`host1/Admin# config`
	`(config)#`
		Enters global configuration mode.

Step 2	**logging trap** *severity_level* **Example:** `host1/Admin(config)# logging trap 6`	Enables system message logging to Flash memory. The *severity_level* argument specifies the maximum level for system log messages sent to a syslog server. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. Allowable entries include: • **0—emergencies** (System unusable messages) • **1—alerts** (Take immediate action) • **2—critical** (Critical condition) • **3—errors** (Error message) • **4—warnings** (Warning message) • **5—notifications** (Normal but significant condition) • **6—informational** (Information message) • **7—debugging** (Debug messages)
Step 3	**no logging trap** **Example:** `host1/Admin(config)# no logging trap`	(Optional) Disables system message logging to Flash memory.

Step 4	**do copy running-config startup-config**
	
	Example:
	`host1/Admin(config)# do copy`
	`running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Specifying an ACE Device ID for Messages to a Syslog Server

The ACE allows you to include a unique device ID in non-EMBLEM format syslog messages sent to the syslog server. The message includes the specified device ID (either the hostname and IP address of the specified interface [even if the message comes from another interface] or a string) in messages sent to a syslog server. The device ID does not appear in EMBLEM-formatted messages.

Use the **logging device-id** configuration mode command to specify that the device ID of the ACE is included in all non-EMBLEM-formatted syslog messages.

Restriction

The device ID part of the syslog message is viewed through the syslog server only and not directly on the ACE.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging device-id** {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*} **Example:** host1/Admin(config)# logging device-id hostname	Specifies that the device ID of the ACE is included in the syslog message. The keywords and arguments are as follows: • **context-name**—Specifies the name of the current context as the device ID to uniquely identify the syslog messages sent from the ACE. • **hostname**—Specifies the hostname of the ACE as the device ID to uniquely identify the syslog messages sent from the ACE. • **ipaddress** *interface_name*—Specifies the IP address of the interface as the device ID to uniquely identify the syslog messages sent from the ACE. You can specify the IP address of a VLAN interface or BVI as the device ID. If you use the **ipaddress** keyword, syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface the ACE uses to send the log data to the external server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. • **string** *text*—Specifies a text string to uniquely identify the syslog messages sent from the ACE. The maximum **string** length is 64 characters without spaces. You cannot use the following characters: & (ampersand), ‘ (single quote), “ (double quote), < (less than), > (greater than), or ? (question mark).
Step 3	**no logging device-id** {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*} **Example:** host1/Admin(config)# no logging device-id hostname	(Optional) Disables the device ID logging function.
Step 4	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Changing the Syslog Logging Facility

If necessary, you can change the syslog logging facility to a value other than the default of 20 (LOCAL4) by using the **logging facility** configuration mode command. Most UNIX systems expect the messages to use facility 20. The ACE allows you to change the syslog facility type to identify the behavior of the syslog daemon (syslogd) on the host. The syslog daemon uses the specified syslog facility to determine how to process messages. Each logging facility configures how the syslog daemon on the host handles a message. Syslog servers file messages based on the facility number in the message. There are eight possible facilities, 16 (LOCAL0) through 23 (LOCAL7).

Note For more information on the syslog daemon and facility levels, see your syslog daemon documentation.

Detailed Steps

	Command	Purpose

Step 1	**config**
	
	Example:
	`host1/Admin# config`
	`(config)#`
		Enters global configuration mode.

Step 2	**logging facility** *number* **Example:** `host1/Admin(config)# logging facility 16`	Specifies the syslog facility. The *number* argument specifies the syslog facility number. Valid values are 16 (LOCAL0) through 23 (LOCAL7). The default is 20 (LOCAL4).
Step 3	**no logging facility** *number* **Example:** `host1/Admin(config)# no logging facility 16`	(Optional) Changes the syslog facility back to the default of 20 (LOCAL4).
Step 4	**do copy running-config startup-config** **Example:** `host1/Admin(config)# do copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Changing the Logging Message Queue

By default, the ACE can hold 80 syslog messages in the message queue while awaiting processing. To change the number of syslog messages that can appear in the message queue, use the **logging queue** configuration mode command.

Prerequisite

Set the queue size before the ACE processes syslog messages. When traffic is heavy, messages may be discarded.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging queue** *queue_size* **Example:** host1/Admin(config)# logging queue 1000	Sets the logging queue size. The *queue_size* argument specifies the size of the queue for storing syslog messages. Valid values are from 1 to 8192 messages. The default is 80 messages.
Step 3	**no logging queue 0** **Example:** host1/Admin(config)# no logging queue 0	(Optional) Resets the logging queue size to the default of 80 messages.
Step 4	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Disabling a Syslog Message or Changing its Severity Level

When you enable system message logging (see the "Enabling or Disabling System Message Logging" section), all syslog messages are enabled. Use the **logging message** configuration mode command to control:

- The display of a specific system logging message (enabled or disabled).
- The severity level associated with a specific system logging message.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**do show logging** **Example:** host1/Admin(config)# do show logging	(Optional) Displays the severity level currently assigned to a message and whether the system logging message is enabled.
Step 3	**no logging message** *syslog_id* **Example:** host1/Admin(config)# no logging message 615004	Disables a specific logging message. The *syslog_id* argument identifies the specific message you want to disable. For example, if a message is listed in the syslog as %<ACE>-4-411001, enter **411001** as the *syslog_id*. See Chapter 2, System Messages, for a detailed list of the ACE system log messages. The messages are listed numerically by message code.

	Command	Purpose
Step 4	**logging message** *syslog_id* **Example:** host1/Admin(config)# logging message 615004	(Optional) Enables a specific logging message.
Step 5	**logging message** *syslog_id* **level** *severity_level* **Example:** host1/Admin(config)# logging message 615004 level 6	Assigns a logging level to a specific logging message. The keywords and arguments are as follows: • *syslog_id*—Identifies the specific message you want to disable or to enable. For example, if a message is listed in the syslog as **%**<ACE>-4-411001, enter **411001** as the *syslog_id*. See Chapter 2, System Messages, for a detailed list of the ACE system log messages. The messages are listed numerically by message code. • **level** *severity_level*—Changes the default severity level associated with a specific system log message. For example, the **%**<ACE>-4-411001 message listed in the syslog has the default severity level of 4 (warning message). You can change the assigned default severity level to a different level. See Chapter 2, System Messages, for a detailed list of the ACE system log messages and associated default severity codes. Allowable entries include: – **0**—**emergencies** (System unusable messages) – **1**—**alerts** (Take immediate action) – **2**—**critical** (Critical condition) – **3**—**errors** (Error message) – **4**—**warnings** (Warning message) – **5**—**notifications** (Normal but significant condition) – **6**—**informational** (Information message) – **7**—**debugging** (Debug messages) **Note** Use this command to set the message severity level back to its default value, where the *severity_level* argument is the default value.
Step 6	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Limiting the Syslog Rate

By default, the ACE disables rate limiting for messages in the syslog. To limit the rate at which the ACE generates messages in the syslog, use the **logging rate-limit** configuration mode command. You can limit the number of syslog messages generated by the ACE for specific messages.

Detailed Steps

	Command	Purpose

Step 1	**config**
	
	Example:
	`host1/Admin# config`
	`(config)#`
		Enters global configuration mode.

Command	Purpose
Step 2 **logging rate-limit** {*num* {*interval* | **level** *severity_level* | **message** *syslog_id*} | **unlimited** {**level** *severity_level* | **message** *syslog_id*}} **Example:** `host1/Admin(config)# logging rate-limit 42 60 level 6`	Enables rate limiting and specifies the rate at which the ACE generates messages in the syslog,system logging. The keywords and arguments are as follows: • *num*—Number at which the syslog is to be rate limited. • *interval*—Time interval (in seconds) over which the system message logs should be limited. The default time interval is one second. • **level** *severity_level*—Specifies the syslog level that you want to rate limit. The severity level you enter indicates that you want all syslog messages at the specified level to be rate-limited. For example, if you specify a severity level of 7, the ACE applies a rate limit only to level 7 (debugging messages). If you want to apply a logging rate limit on a different severity level, you must configure the **logging rate-limit level** command for that level as well. Allowable entries include: – **0—emergencies** (System unusable messages) – **1—alerts** (Take immediate action) – **2—critical** (Critical condition) – **3—errors** (Error message) – **4—warnings** (Warning message) – **5—notifications** (Normal but significant condition) – **6—informational** (Information message) – **7—debugging** (Debug messages) • **message** *syslog_id*—Identifies the ID of the specific message you want to suppress reporting. For example, if a message is listed in the syslog as %ACE-4-411001, enter **411001** as the *syslog_id*. See Chapter 2, System Messages, for a detailed list of the ACE system log messages. The messages are listed numerically by message code. • **unlimited—**Disables rate limiting for messages in the syslog (default). **Note** Disabled rate limiting is the default setting. In this case, the **logging rate-limit unlimited** command will not be displayed in the ACE running-configuration file.

	Command	Purpose
Step 3	**no logging rate-limit** {*num* {*interval* | **level** *severity_level* | **message** *syslog_id*} | **unlimited** {**level** *severity_level* | **message** *syslog_id*}} **Example:** host1/Admin(config)# no logging rate-limit 42 60 level 6	(Optional) Disables rate limiting.
Step 4	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Example

For example, to suppress reporting of system message 302022, enter:

```
host1/Admin(config)# logging rate-limit 42 60 level 6 message 302022
```

Enabling Logging on the Standby ACE

To enable logging on the failover standby ACE, use the **logging standby** configuration mode command. When enabled, the standby ACE syslog messages remain synchronized should failover occur. This command is disabled by default.

Note When logging on the failover standby ACE is enabled, this command causes twice the message traffic on the syslog server.

Detailed Steps

	Command	Purpose
Step 1	**config** **Example:** host1/Admin# config (config)#	Enters global configuration mode.
Step 2	**logging standby** **Example:** host1/Admin(config)# logging standby	Enables logging on the failover standby ACE.
Step 3	**no logging standby** **Example:** host1/Admin(config)# no logging standby	(Optional) Disables logging on the failover standby ACE.
Step 4	**do copy running-config startup-config** **Example:** host1/Admin(config)# do copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Enabling the Logging of Connection Setup and Teardown Syslog Messages Through the Fastpath

By default, the ACE logs the following connection setup and teardown syslog messages through the control plane:

- 106023
- 302022
- 302023
- 302024
- 302025

Because of the large number of these syslog messages that are generated by connection setup and teardown, you can instruct the ACE to send these syslogs through the fast path instead of the control plane. The fast path supports a much higher rate of syslogs than the control plane does. When you instruct the ACE to send these syslogs through the fast path, the message formatting changes (different message spacing) and the syslog IDs change to 106028, 302028, 302029, 302030, and 302031, respectively.

To enable the logging of connection setup and teardown messages through the fast path, use the **logging fastpath** configuration mode command.

Restriction

When you enable this command, the syslog messages do not arrive at the output destination in the correct order. In addition, the syslog messages are sent only to the external syslog servers and are not seen on the other enabled syslog output destinations, such as the local buffer or the console.

Detailed Steps

	Command	Purpose

Step 1	**config**
	
	Example:
	`host1/Admin# config`
	`(config)#`
		Enters global configuration mode.

Step 2	**logging fastpath** **Example:** `host1/Admin(config)# logging fastpath`	Configures the ACE to log connection setup and teardown syslog messages through the fast path.
Step 3	**no logging fastpath** **Example:** `host1/Admin(config)# no logging fastpath`	(Optional) Stops the ACE from logging connection setup and teardown syslog messages through the fast path.
Step 4	**do copy running-config startup-config** **Example:** `host1/Admin(config)# do copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Clearing Log Messages

To clear the syslog messages contained in the message buffer created with the **logging buffered** configuration mode command, use the **clear logging** command in the privileged Exec mode.

Detailed Step

Command	Purpose
clear logging [**disabled** | **rate-limit** | **statistics**] **Example:** host1/Admin# clear logging	Clears the syslog messages contained in the message buffer. • **disabled**—(Optional) Clears all disabled syslog messages. • **rate-limit**—(Optional) Clears the rate-limit configuration at which the ACE generates the syslog, as specified by the **logging rate-limit** command. • **statistics**—(Optional) Clears (sets to zero) all statistics that are displayed by the **show logging statistics** command.

Viewing Log Message Information

Use the **show logging** command in privileged Exec mode to view the current severity level and state of all syslog messages stored in the buffer or to display information related to specific syslog messages. This command lists the current syslog messages and identifies which **logging** command options are enabled. Use the **do** form of the command to use the command in configuration mode.

Prerequisite

To view the contents of the syslog buffer, configure the buffer output location (see the "Sending Syslog Messages to a Buffer" section).

Detailed Step

Command	Purpose
show logging [**history** | **internal** {**event-history dbg** | **facility**} | **message** [*syslog_id* | **all** | **disabled**] | **persistent** | **queue** | **rate-limit** | **statistics**]] **Example:** host1/Admin# show logging message 615004 Message logging: message 615004: default-level 6 (enabled)	Displays the current severity level and state of all syslog messages stored in the buffer. The keywords and arguments are as follows: • **history**—Displays the syslog message history file. • **internal**—Displays syslog internal messages. • **event-history db**—Displays the debug history for the syslog server. **Note** The ACE debug commands are intended for use by trained Cisco personnel only. • **facility**—Lists the various internal facilities contained within the ACE. • **message**—Displays a list of syslog messages that have been modified from the default settings. These are syslog messages that have been assigned a different severity level or messages that have been disabled. • *syslog_id*—Displays a specific system log message (by message ID), the assigned default severity level, and identifies whether the message is enabled or disabled. See Chapter 2, System Messages, for a detailed list of the ACE system log messages. The messages are listed numerically by message code. • **all**—Displays all system log message IDs, the assigned default severity level, and identifies whether each message is enabled or disabled. • **disabled**—Displays a complete list of disabled syslog messages. • **persistent**—Displays statistics for the log messages sent to Flash memory on the ACE. • **queue**—Displays statistics for the internal syslog queue. • **rate-limit**—Displays the current syslog rate-limit configuration. • **statistics**—Displays syslog statistics.

Table 1-4 describes the fields in the **show logging** command output.

Table 1-4 Field Descriptions for the show logging Command

Field	Description
Syslog Logging	Status of system message logging for the ACE: Enabled or Disabled.
Facility	System message logging facility setting.

Table 1-4 Field Descriptions for the show logging Command (continued)

Field	Description
History Logging	Status of the system message logging history setting: Enabled or Disabled.
Trap Logging	Status of the syslog server trap level setting: Enabled or Disabled.
Timestamp Logging	Status of including the date and time on syslog messages: Enabled or Disabled.
Fastpath Logging	Status of syslog fastpath logging: Enabled or Disabled.
Persist Logging	Status of logging to Flash memory on the ACE: Enabled or Disabled.
Standby Logging	Status of logging to the failover standby ACE: Enabled or Disabled.
Rate-limit logging	Status of limiting the rate at which the ACE generates syslog messages: Enabled or Disabled.
Console Logging	Status of logging to the console: Enabled or Disabled.
Monitor Logging	Status of logging to a remote connection using the Secure Shell (SSH) or Telnet: Enabled or Disabled.
Device ID	Status of including a unique device ID in non-EMBLEM format syslog messages sent to the syslog server: Enabled or Disabled.
Message Logging	Status of disabled syslog messages or syslog messages with a modified severity level. The state is either Enabled or Disabled.
Buffered Logging	Status of logging to the local buffer on the ACE is disabled: Enabled or Disabled.
Buffer Info	Presents information about the syslog message buffer.
Current Size	Current size of the syslog buffer memory on the ACE.
Global Pool	Total size of available syslog buffer memory.
Used Pool	Total size of used syslog buffer memory.
Min.	Minimum available syslog buffer memory.
Max.	Maximum available syslog buffer memory.
Cur Ptr	Current pointer location in syslog buffer memory. Cur Ptr is automatically advanced after each buffer memory read or write.
Wrapped	Indicates if wraparound has occurred to the data in the syslog buffer memory.

Table 1-5 describes the fields in the **show logging disabled** command output.

Table 1-5 Field Descriptions for the show logging disabled Command

Field	Description
Message Logging	Status of disabled syslog messages in the ACE: Enabled or Disabled.

Table 1-6 describes the fields in the **show logging history** command output.

Table 1-6 Field Descriptions for the show logging history Command

Field	Description
syslog_trinity_show_ history for context *x*	Status of the syslog message history setting for the active user context: Enabled or Disabled.

Table 1-7 describes the fields in the **show logging internal facility** command output.

Table 1-7 Field Descriptions for the show logging internal facility Command

Field	Description
Syslog registered *x* facilities	Displays a list of all syslog registered facilities.

Table 1-8 describes the fields in the **show logging persistent** command output.

Table 1-8 Field Descriptions for the show logging persistent Command

Field	Description
Current Size	Current size of the syslog buffer memory on the ACE.
Global Pool	Total size of available syslog buffer memory.
Used Pool	Total size of used syslog buffer memory.
Min.	Minimum available syslog buffer memory.
Max.	Maximum available syslog buffer memory.
Cur Ptr	Current pointer location in syslog buffer memory. Cur Ptr is automatically advanced after each buffer memory read or write.
Wrapped	Indicates if wraparound has occurred to the data in the syslog buffer memory.

Table 1-9 describes the fields in the **show logging queue** command output.

Table 1-9 Field Descriptions for the show logging queue Command

Field	Description
Logging Queue length limit	Number of syslog messages that can appear in the message queue along with the number of discarded messages.
Current *x* msg on queue, *xxx* msgs most on queue	Number of messages currently in the logging queue along with the default number of syslog messages that can appear in the message queue.
CP messages received	Number of messages received from the control plane along with the number of discarded messages.
IXP messages received	Number of messages received from the IXP2800 Network Processor along with the number of discarded messages.
Xscale messages received	Number of messages received from the Xscale CPU.
System Max Queue size	Maximum size of the logging queue.
System Free Queue size for allocation	Available space in the logging queue.

Table 1-10 describes the fields in the **show logging rate-limit** command output.

Table 1-10 Field Descriptions for the show logging rate-limit Command

Field	Description
Rate-limit Logging	Current syslog rate-limit configuration.

Table 1-11 describes the fields in the **show logging statistics** command output.

Table 1-11 Field Descriptions for the show logging statistics Command

Field	Description
Syslog Statistics	System message log-specific statistics.
Messages sent	
Console	Total number of messages sent to the console.
Buffer	Total number of messages sent to the local buffer on the ACE.
Persistent	Total number of messages sent to Flash memory on the ACE.
History	Total number of SNMP messages sent to an NMS.
Host	Total number of messages sent to a syslog server on a host.
Misc	Total number of miscellaneous system logging messages.

Table 1-11 Field Descriptions for the show logging statistics Command (continued)

Field	Description
Messages Discarded	
Cfg rate-limit	Total number of messages discarded due to the syslog message rate specified through the **logging rate-limit** command.
Hard rate-limit	Total number of messages discarded due to the internally set syslog message rate.
Server down	Total number of messages discarded due to a syslog server failure on a host.
Queue full	Total number of messages discarded because the message queue is full.
Errors	Total number of messages discarded due to an error condition.
SNMP-related Counters	
Notifications sent	Total number of times the ACE sent SNMP traps (event notifications) to an NMS.
History table flushed	Total number of times the syslog message trap history table has been flushed.
Messages ignored	Total number of SNMP messages ignored by the ACE.
NP-related Counters	Network processor-related message counters.
To-CP dropped	Total number of messages sent by the network processor that were dropped by the control plane.
Fastpath sent	Total number of connection setup and teardown messages sent by the ACE.
Fastpath dropped	Total number of connection setup and teardown messages dropped by the ACE.