Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco 910 Industrial Routers (*hereafter* referred to as the router).

This chapter consists of these sections:

Understanding System Message Logging

By default, a router sends the output from system messages and **debug** privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, console port, or a UNIX syslog server, depending on your configuration.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations.

You can access logged system messages by using the router command-line interface (CLI) or by saving them to a properly configured syslog server. The router software saves syslog messages in an internal buffer.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the router through Telnet or through the console port.

Configuring System Message Logging

These sections contain this configuration information:

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Messages appear in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description

Table 7 describes the elements of syslog messages.

Table 7 System Log Message Elements

Element	Description
seq no:	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured. For more information, see the "Defining the Message Severity Level" section on page -82.
timestamp formats: mm/dd h*h:mm:ss*	Date and time of the message or event.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 10 on page -84.
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 9 on page -83.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

Default System Message Logging Configuration

Table 8 shows the default system message logging configuration.

Table 8 Default System Message Logging Configuration

Feature	Default Setting
System message logging	Enabled.
System message logging to the console	Disabled.
Console severity	Debugging (and numerically lower levels; see Table 9 on page -83).
Logging file configuration	No filename specified.
Logging buffer size	256 KB.
Logging history size	1 message.
Time stamps	Disabled.
Logging server	Disabled.
Syslog server IP address	None configured.
Server facility	Local7 (see Table 10 on page -84).
Server severity	Informational (and numerically lower levels; see Table 9 on page -83).

Enabling and Disabling Message Logging

Message logging is enabled by default, while message logging to the console is disabled by default.

Beginning in privileged EXEC mode, follow these steps to enable or disable message logging.

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**logging on**	Enable message logging.
3.	**exit**	Return to privileged EXEC mode.
4.	**show running-config** or **show logging**	Verify your entries.
5.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Disabling the logging process can slow down the router because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear on the console as soon as they are produced, often appearing in the middle of command output.

To disable logging, use the **no logging on** global configuration command.

Beginning in privileged EXEC mode, follow these steps to enable or disable message logging to the console.

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**logging console** *level*	Log messages that are not higher than required level to the console. See Table 9 on page -83 for the values and definitions of *level*.
3.	**exit**	Return to privileged EXEC mode.
4.	**show running-config** or **show logging**	Verify your entries.
5.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable logging to the console, use the **no logging console** global configuration command.

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages. This procedure is optional.

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**logging buffered size** [*size*]	Log messages to an internal buffer on the router. The range is 4096 bytes (4 KB) to 10485760 bytes (10 MB). The default buffer size is 256 KB. **Note:** Do not make the buffer size too large because the router could run out of memory for other tasks. Use the **show memory** privileged EXEC command to view the free processor memory on the router. However, this value is the maximum available, and the buffer size should *not* be set to this amount.
3.	**logging host** *host* [**port** *port*] [**transport** *transport*]	Log messages to a UNIX syslog server host. ■ *host*–Specify the name or IP address of the host to be used as the syslog server. ■ *port*–Specify the port of the syslog server. If this value is omitted, the default is 514. ■ *transport*–Specify tcp or udp to transmit the message. If this value is omitted, the default is udp. To build a list of syslog servers that receive logging messages, enter this command more than once. By default, message logging to a remote syslog server is disabled.
4.	**exit**	Return to privileged EXEC mode.
5.	**show running-config**	Verify your entries.
6.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The **logging buffered** global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** privileged EXEC command. The first message displayed is the oldest message in the buffer.

To disable logging to the console, use the **no logging console** global configuration command.

Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, which are described in Table 9.

Beginning in privileged EXEC mode, follow these steps to define the message severity level. This procedure is optional.

	Command	Purpose
1.	**configure terminal**	Enter global configuration mode.
2.	**logging console** *level*	Limit messages logged to the console. By default, logging to the console is disabled.
3.	**logging trap** *level*	Limit messages logged to the remote syslog servers. By default, remote syslog servers is disabled.
4.	**exit**	Return to privileged EXEC mode.
5.	**show running-config** or **show logging**	Verify your entries.
6.	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Specifying a *level* causes messages at that level and numerically lower levels to appear at the destination.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to syslog servers, use the **no logging trap** global configuration command.

Table 9 describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 9 Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	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

The software generates the following categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**. These types of messages mean that the functionality of the router is affected.
- Output from the **debug** commands, displayed at the **debugging** level. Debug commands are typically used only by the Technical Assistance Center.
- Interface up or down transitions and system restart messages, displayed at the **notifications** level. This message is only for information; router functionality is not affected.

Table 10 lists the system facilities supported by the software.

Table 10 Logging Facility Types

Facility Type	Description
LOG_KERN	kernel messages
LOG_USER	user-level messages
LOG_MAIL	mail system
LOG_DAEMON	system daemons
LOG_AUTH	security/authorization messages
LOG_SYSLOG	messages generated internally by syslogd
LOG_LPR	line printer subsystem
LOG_NEWS	network news subsystem
LOG_UUCP	UUCP subsystem
LOG_CRON	clock daemon
LOG_AUTHPRIV	security/authorization messages
LOG_FTP	FTP daemon
LOG_LOCAL0	local use 0
LOG_LOCAL1	local use 1
LOG_LOCAL2	local use 2
LOG_LOCAL3	local use 3
LOG_LOCAL4	local use 4
LOG_LOCAL5	local use 5
LOG_LOCAL6	local use 6
LOG_LOCAL7	local use 7

Displaying the Logging Configuration

To display the logging configuration and the contents of the log buffer, use one or more of the privileged EXEC commands in Table 11:

Table 11 Commands for Displaying Logging Configuration

Command	Purpose
show logging	Displays the contents of the log buffer.
show debugging	Displays the state of each debugging option.
show crashinfo	Displays crash information.

To filter the contents of the log buffer, use the output modifiers in Table 12:

Table 12 Output Modifiers of Show Logging Command

Command	Output Modifier	Purpose
show logging	**| include** *string*	Include lines that match.
	| exclude *string*	Exclude lines that match.
	| begin *string*	Begin with the line that matches.
	| redirect *string*	Copy the buffered logging to TFTP, FTP or A local file.

The following example shows the SNMP log:

```
Router# show logging | include snmpd
Jan  1 08:00:04 %snmpd-6-: NET-SNMP version 5.7.1
Jan  1 08:25:13 %snmpd-6-: Received TERM or STOP signal...  shutting down...
..
```

The following example shows the state of each debugging option:

```
Router# show debugging
LLDP:
    LLDP packet info debugging is on.
    LLDP errors debugging is on.
```

The following example shows the crash information:

```
Router# show crashinfo

[  138.520000] Unable to handle kernel NULL pointer dereference at virtual address 00000000
[  138.520000] pgd = c0004000
[  138.520000] [00000000] *pgd=00000000
[  138.520000] Internal error: Oops: 817 [#1]
[  138.520000] last sysfs file: /sys/devices/virtual/ubi/ubi0/mtd_num
[  138.520000] Modules linked in: vfat fat
[  138.520000] CPU: 0    Not tainted  (2.6.35.14 #1)
[  138.520000] PC is at mv_btns_handler+0x13c/0x26c
[  138.520000] LR is at handle_IRQ_event+0x48/0x120
[  138.520000] pc : [<c0175d3c>]    lr : [<c01a5004>]    psr: 60000093
[  138.520000] sp : c04a7e98  ip : 00000000  fp : c04a7ef4
[  138.520000] r10: 00021744  r9 : 56251311  r8 : c04aed04
[  138.520000] r7 : 00000088  r6 : 00000004  r5 : c04d233c  r4 : 00000022
[  138.520000] r3 : c04d24d4  r2 : 00000000  r1 : 00000004  r0 : 00000000
[  138.520000] Flags: nZCv  IRQs off  FIQs on  Mode SVC_32  ISA ARM  Segment kernel
[  138.520000] Control: 0005397f  Table: 1f11c000  DAC: 00000017
[  138.520000] Process swapper (pid: 0, stack limit = 0xc04a6270)
[  138.520000] Stack: (0xc04a7e98 to 0xc04a8000)
[  138.520000] 7e80:                                                     c019be08 c04ab1c0
[  138.520000] 7ea0: c04a7ea0 c04a7ea0 c019be20 00000001 00000004 c04d714c 60000093 00000000
[  138.520000] 7ec0: 00000008 c04d7150 c04a7f1c dfc29680 00000000 00000000 00000062 00021778
[  138.520000] 7ee0: 56251311 00021744 c04a7f14 c04a7ef8 c01a5004 c0175c10 c04b2d04 00000062
[  138.520000] 7f00: 00000000 c04a9e58 c04a7f2c c04a7f18 c01a6994 c01a4fcc c04c0234 00000062
[  138.520000] 7f20: c04a7f4c c04a7f30 c0026040 c01a6924 60000013 ffffffff 0000001f 00000004
[  138.520000] 7f40: c04a7fb4 c04a7f50 c0028f70 c0026010 00000000 0005397f 0005297f 60000013
[  138.520000] 7f60: c04a6000 c04d1b24 c04a6000 c04a9e58 00021778 56251311 00021744 c04a7fb4
[  138.520000] 7f80: c04a7f98 c04a7f98 c012c214 c012c3bc 60000013 ffffffff c04d99f0 c0022ba4
[  138.520000] 7fa0: c08f1140 c04a9e50 c04a7fc4 c04a7fb8 c002d338 c012c34c c04a7ff4 c04a7fc8
[  138.520000] 7fc0: c0008904 c002d2e8 c0008374 00000000 00000000 c0022ba4 00000000 00053975
[  138.520000] 7fe0: c04d1bd4 c0022ba0 00000000 c04a7ff8 00008034 c00086ec 00000000 00000000
[  138.520000] Backtrace:
[  138.520000] [<c0175c00>] (mv_btns_handler+0x0/0x26c) from [<c01a5004>] (handle_IRQ_event+0x48/0x120)
[  138.520000] [<c01a4fbc>] (handle_IRQ_event+0x0/0x120) from [<c01a6994>]
(handle_level_irq+0x80/0x110)
```

```
[  138.520000]  r7:c04a9e58 r6:00000000 r5:00000062 r4:c04b2d04
[  138.520000] [<c01a6914>] (handle_level_irq+0x0/0x110) from [<c0026040>] (asm_do_IRQ+0x40/0x90)
[  138.520000]  r5:00000062 r4:c04c0234
[  138.520000] [<c0026000>] (asm_do_IRQ+0x0/0x90) from [<c0028f70>] (__irq_svc+0x30/0x180)
[  138.520000] Exception stack(0xc04a7f50 to 0xc04a7f98)
[  138.520000] 7f40:                                     00000000 0005397f 0005297f 60000013
[  138.520000] 7f60: c04a6000 c04d1b24 c04a6000 c04a9e58 00021778 56251311 00021744 c04a7fb4
[  138.520000] 7f80: c04a7f98 c04a7f98 c012c214 c012c3bc 60000013 ffffffff
[  138.520000]  r6:00000004 r5:0000001f r4:ffffffff r3:60000013
[  138.520000] [<c012c33c>] (cpu_idle+0x0/0xbc) from [<c002d338>] (rest_init+0x60/0x78)
[  138.520000]  r7:c04a9e50 r6:c08f1140 r5:c0022ba4 r4:c04d99f0
[  138.520000] [<c002d2d8>] (rest_init+0x0/0x78) from [<c0008904>] (start_kernel+0x228/0x270)
[  138.520000] [<c00086dc>] (start_kernel+0x0/0x270) from [<00008034>] (0x8034)
[  138.520000] Code: ea000011 e3a02000 e0843084 e0853103 (e5822000)
[  138.530000] ---[ end trace 39f8e093c1b90767 ]---
```

Debugging the System

To debug the system, use one or more of the privileged EXEC commands in Table 13:

Table 13 Commands for Debugging the System

Command	Purpose
debug charon	Enable debug charon information.
debug dhclinet	Enable debug dhclient information.
debug dhcp	Enable debug dhcp information.
debug l2tp	Enable debug l2tp information.
debug lldp errors	Enable debug LLDP errors.
debug lldp packets	Enable debug LLDP packet-related information.
debug ntp	Enable debug ntp information.
debug ppp	Enable debug ppp information.
debug pptp	Enable debug pptp information.
ebug snmp	Enable debug SNMP information.

To disable the debugging fuction, use the **no debug** global configuration command.

The following examples show the LLDP debugging logs:

```
Router# debug lldp packets

Jan  1 01:48:53: %lldpd-7-: LLDP advertisement packet RX'd on intf GigabitEthernet0/1
Jan  1 01:49:03: %lldpd-7-: LLDP advertisement packet TX'd on intf GigabitEthernet0/1
Jan  1 01:49:05: %lldpd-7-: LLDP advertisement packet RX'd on intf GigabitEthernet0/1
Jan  1 01:49:06: %lldpd-7-: LLDP advertisement packet RX'd on intf GigabitEthernet0/1
Jan  1 01:49:23: %lldpd-7-: LLDP advertisement packet RX'd on intf GigabitEthernet0/1
Jan  1 01:49:33: %lldpd-7-: LLDP advertisement packet TX'd on intf GigabitEthernet0/1
….

Router# debug lldp errors

Jan  1 01:48:35: %lldpd-7-: LLDP unknown tlv type 9 recd - ignoring it
Jan  1 01:48:35: %lldpd-7-: LLDP unknown tlv type 127 recd - ignoring it
….
```