

Memory Logs on the 200/300 Series Managed Switches

Objectives

The 200/300 Series Managed Switches have the ability to record a set of messages, called logs, which gives information about system events. The switch stores two sets of local logs: one list of logged events written to RAM, which is erased after reboot, and a cyclical log-file written to Flash memory, which is saved upon reboot. In addition, these logs can be sent to a remote SYSLOG server where they can easily be viewed and monitored in the form of traps and SYSLOG messages.

This article explain how to view system logs and how to configure logs on the 200/300 Series Managed Switches.

Applicable Devices

- SF/SG 200 and SF/SG 300 Series.

Software Version

- 1.3.0.62

RAM Memory Logs

This section explains how to access the RAM Memory Log Table, and its different options.

Step 1. Log in to the web configuration utility and choose **Status and Statistics > View Log > RAM Memory**. The *RAM Memory* page opens:

Log Index	Log Time	Severity	Description
2147483616	2012-Jul-19 18:46:27	Informational	%AAA-I-CONNECT: New http connection for user cisco, source 192.168.1.1 destination 192.168.1.254 ACCEPTED
2147483617	2012-Jul-19 18:21:26	Informational	%BOOTP_DHCP_CL-I-BOOTPCONFIGURED: The device has been configured via BOOTP
2147483618	2012-Jul-19 18:21:24	Warning	%STP-W-PORTSTATUS: gi2: STP status Forwarding
2147483619	2012-Jul-19 18:21:20	Informational	%LINK-I-Up: Vlan 1
2147483620	2012-Jul-19 18:21:20	Informational	%LINK-I-Up: gi2
2147483621	2012-Jul-19 17:58:57	Informational	%INIT-I-Startup: Cold Startup
2147483622	2012-Jul-19 17:56:48	Warning	%LINK-W-Down: gi20
2147483623	2012-Jul-19 17:56:48	Warning	%LINK-W-Down: gi19
2147483624	2012-Jul-19 17:56:48	Warning	%LINK-W-Down: gi18
2147483625	2012-Jul-19 17:56:48	Warning	%LINK-W-Down: gi17

The RAM Log Table has these fields:

- Log Index — Log entry number.
- Log Time — Date and time the log was created.

- Severity — Event Severity.
- Description — Informational message describing the event logged.

Step 2. (Optional) To disable the alert blink function, click **Disable Alert Icon Blinking**.

Step 3. (Optional) To see a specific number of entries in the RAM Memory Log Table, in the Showing drop-down list, choose the number of entries you want to see per page.

Step 4. (Optional) To see the next page of entries in the RAM Memory Log Table, click the **Next** button.

Step 5. (Optional) To Clear the logs in RAM, click **Clear Logs**.

Flash Memory Logs

This section explains how to access the Flash Memory Log Table, and its different options.

Step 1. Log in to the web configuration utility and choose **Status and Statistics > View Log > Flash Memory**. The Flash Memory page opens:

Flash Memory			
Flash Memory Log Table			
Log Index	Log Time	Severity	Description
2147470822	2012-Jul-19 17:57:31	Error	%INIT-E-ApplErr: Errors occurred during initialization
2147470966	2012-Jul-19 17:55:21	Error	%MNG_DIAG-E-DIAGATINIT: Init: Port gl1:Action is illegal in current Port Mode
2147471159	2012-Jul-19 18:21:42	Error	%HTTP_HTTPS-E-DIAGNOSTICS: in <RL_vtQueryEntryGet> tag, the key rIDnsCIDomainNameName is missing in the query., aggregated (1)
2147471352	2012-Jul-19 18:16:56	Error	%HTTP_HTTPS-E-DIAGNOSTICS: in <RL_vtQueryEntryGet> tag, the key rIDnsCIDomainNameName is missing in the query., aggregated (1)
2147471545	2012-Jul-19 18:14:11	Error	%HTTP_HTTPS-E-DIAGNOSTICS: in <RL_vtQueryEntryGet> tag, the key rIDnsCIDomainNameName is missing in the query., aggregated (1)
2147471722	2012-Jul-19 18:11:40	Error	%HTTP_HTTPS-E-DIAGNOSTICS: in <RL_vtQueryEntryGet> tag, the key rIDnsCIDomainNameName is missing in the query.
2147471915	2012-Jul-19 18:09:54	Error	%HTTP_HTTPS-E-DIAGNOSTICS: in <RL_vtQueryEntryGet> tag, the key rIDnsCIDomainNameName is missing in the query., aggregated (2)
2147472108	2012-Jul-19 18:05:11	Error	%HTTP_HTTPS-E-DIAGNOSTICS: in <RL_vtQueryEntryGet> tag, the key rIDnsCIDomainNameName is missing in the query., aggregated (1)
2147472285	2012-Jul-19 18:02:45	Error	%HTTP_HTTPS-E-DIAGNOSTICS: in <RL_vtQueryEntryGet> tag, the key rIDnsCIDomainNameName is missing in the query.
2147472466	2012-Jul-19 18:00:33	Error	%HTTP_HTTPS-E-DIAGNOSTICS: ERROR - in <RL_vtLeadTableGet> tag, can not find the table pethMainPseTable in the MIB.

The Flash Memory Log Table has these fields:

- Log Index — Log entry number.
- Log Time — Date and time the log was created.
- Severity — Event Severity.
- Description — Informational message describing the event logged.

Step 2. (Optional) To see a specific number of entries in the Flash Memory Log Table, in the Showing drop-down list, choose the number of entries you want to see per page.

Step 3. (Optional) To see the next page of entries in the Flash Memory Log Table, click the **Next** button.

Step 4. (Optional) To Clear the logs in RAM, click **Clear Logs**.

Logs Setup

This section explains how to configure the different Logs options the 200/300 Series Managed Switches offers.

Step 1. Log in to the web configuration utility and choose **Administration > System Log > Log Settings**. The *Log Settings* page opens:

The screenshot shows the 'Log Settings' web configuration page. At the top, there are two sections: 'Logging:' with an 'Enable' checkbox checked, and 'Syslog Aggregator:' with an 'Enable' checkbox checked. Below these is a field for 'Max. Aggregation Time:' set to '500' seconds, with a range of 15 to 3600 and a default of 300. The page is divided into two columns: 'RAM Memory Logging' and 'Flash Memory Logging'. Each column has a list of log levels with corresponding checkboxes. In the RAM Memory Logging column, all levels from Emergency to Debug are checked. In the Flash Memory Logging column, only Emergency, Alert, and Critical are checked, while Warning, Notice, Informational, and Debug are unchecked. At the bottom, there are 'Apply' and 'Cancel' buttons.

RAM Memory Logging		Flash Memory Logging	
Emergency:	<input checked="" type="checkbox"/>	Emergency:	<input checked="" type="checkbox"/>
Alert:	<input checked="" type="checkbox"/>	Alert:	<input checked="" type="checkbox"/>
Critical:	<input checked="" type="checkbox"/>	Critical:	<input checked="" type="checkbox"/>
Error:	<input checked="" type="checkbox"/>	Error:	<input checked="" type="checkbox"/>
Warning:	<input checked="" type="checkbox"/>	Warning:	<input type="checkbox"/>
Notice:	<input checked="" type="checkbox"/>	Notice:	<input type="checkbox"/>
Informational:	<input checked="" type="checkbox"/>	Informational:	<input type="checkbox"/>
Debug:	<input type="checkbox"/>	Debug:	<input type="checkbox"/>

Step 2. In the Logging field, check the **Enable** check box to enable logs.

Step 3. (Optional) To Enable Syslog Aggregator, in the Syslog Aggregator field, check the **Enable** check box. This feature enables identical and sequential logs to display as a single message. The number of times a message has been aggregated is included in the message information.

Step 4. If Syslog Aggregator is enabled, in the Max Aggregator Time field, enter the time interval in seconds that syslogs messages are aggregated.

Step 5. Under RAM Memory Logging and Flash Memory Logging, check the events check boxes you want the switch to keep a log. The following are the events you can check:

- Emergency — System is not usable.
- Alert — An Action is needed. This event tells the user to perform a specific action on the device immediately
- Critical — The System is in a critical condition. This event has more relevance than an error event and needs to be checked, otherwise, the switch could not function at all.
- Error — The System is in error condition. The switch works under an error, and tells the user where the error was originated.
- Warning — A System warning has occurred. a system change, whether hardware or software, occurred and some of the switch components might not be working properly.
- Notice — The System is functioning properly, but a system notice has occurred.

- Informational — This event only show information about the activities in the device.
- Debug — Shows Detailed information about an event. This event will constantly keep information about everything the switch performance.

6. Click **Apply** to save your configuration.

Remote Log Servers

This section explains how to add a remote log server to the 200/300 Series Managed Switches.

Step 1. Log in to the web configuration utility and choose **Administration > System Log > Remote Log Servers**. The *Remote Log Servers* page opens:



Remote Log Servers					
Remote Log Server Table					
<input type="checkbox"/>	Log Server	UDP Port	Facility	Description	Minimum Severity
0 results found.					
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>					

The Remote Log Server Table shows all Syslog servers currently configured and includes these fields:

- Log Server — The IP Address or domain name of the Syslog server.
- UDP Port — The Syslog server UDP port to where the logs are sent.
- Facility — The value that identifies the device from which the logs are originated.
- Description — A description of the Syslog server.
- Minimum Severity — The minimum severity level required for logs to be sent to the server.

Step 2. Click **Add** to add a log server. The **Add Remote Log Server** window appears.

Server Definition: ☒ By IP address ☐ By name

IP Version: ☐ Version 6 ☒ Version 4

IPv6 Address Type: ☐ Link Local ☐ Global

Link Local Interface: None

Log Server IP Address/Name: 192.168.1.1

UDP Port: 514 (Range: 1 - 65535, Default: 514)

Facility: Local 7

Description: Test Log Server

Minimum Severity: Informational

Apply Close

Step 3. In the Server Definition field, click **By IP Address** to enter the IP address of the server, or click **By Name** to enter the name of the server.

Step 4. In the IP Version field, click **Version 6** or **Version 4** to enter the server IP address.

Step 5. If version 6 is chosen, in the IPv6 Address Type field, click **Link Local** Or **Global**. A link local IPv6 address uniquely identifies host on a single network link, while a global IPv6 address is visible and reachable from other networks.

Step 6. If the IPv6 Address Type chosen is Link Local, choose the appropriate link local interface in the Link Local Interface drop-down list.

Step 7. In the Log Server IP Address/Name field, enter the IP address of the remote log server.

Step 8. In the UDP Port field, enter the UDP port to which the logs will be sent to the remote server.

Step 9. In the Facility drop-down list, choose the facility value from which system logs are sent to the remote server.

Step 10. (Optional) To enter a description about the remote log server, in the Description field, enter the desired description.

Step 11. In the Minimum Severity drop-down list, choose the minimum level of system log messages that are going to be sent to the remote server..

Step 12. Click **Apply** to save your configuration.

Note: To edit or delete a remote log server, refer to the section *Edit a Remote Log Server*.

Edit a Remote Log Server


This section explains how to edit a remote log server.

Step 1. Log in to the web configuration utility and choose **Administration > System Log > Remote Log Servers**. The *Remote Log Servers* page opens:

Remote Log Servers					
Remote Log Server Table					
<input checked="" type="checkbox"/>	Log Server	UDP Port	Facility	Description	Minimum Severity
<input checked="" type="checkbox"/>	192.168.1.1	514	Local 7	Test Log Server	Informational
<div>Add... Edit... Delete</div>					

Step 2. To edit a remote log server configuration, check the check box of the remote server you wish to edit.

Step 3. Click **Edit**. The Edit Remote Log Server window appears.

Log Server IP Address:	<input type="text" value="192.168.1.1"/>
 UDP Port:	<input type="text" value="514"/> (Range: 1 - 65535, Default: 514)
Facility:	<input type="text" value="Local 7"/>
Description:	<input type="text" value="Test Log Server"/>
Minimum Severity:	<input type="text" value="Informational"/>
<div>Apply Close</div>	

Step 4. In the Log Server IP Address drop-down list, choose an available IP address.

Step 5. In the UDP Port field, change the UDP port number to the desired value.

Step 6. In the Facility drop-down list, change the facility value to the desired value.

Step 7. In the Description field, change your current description to the desired description.

Step 8. In the Minimum Severity drop-down list, change the severity level to the desired level.

Step 9. Click **Apply** to save your configuration.

Step 10. (Optional) To delete remote server, check the check box of the remote server you wish to delete and click **Delete**.