7 Switch Logging

Logging Overview

Whether you are troubleshooting, configuring, or simply monitoring the switch, you may find it useful to view a history of various switch activities. The Logging submenu contains a list of commands for viewing and configuring logging on the system. To enter the logging submenu, enter

```
logging
```

at the system prompt Enter a question mark (**?**) and then press **<Enter>** to display the following list of commands:

Command	Logging Menu
syslog	Change the syslog parameters (not part of Switch Logging feature)
swlogc	Configure Switch Logging source/destination mapping and priority levels
cmdlog	Show UI Command entries in the mpm.log file
conlog	Show Connection entries (logins/logouts) entries in the mpm.log file
caplog	Show Screen Capture entries in the mpm.log file
debuglog	Show Debug message entries in the mpm.log file
seclog	Show Secure Access entries in the mpm.log file

Commands in the submenu are described here.

System Log Messages

The **syslog** command is used to configure how system log messages, like diagnostic and error messages, are handled on the switch. See *Configuring the Syslog Parameters* on page 7-2.

Switch Logging Parameters

The **swlogc** and remaining commands in the submenu are part of the Switch Logging feature, which is a separate logging mechanism. The **swlogc** command is used for configuring the logging parameters of various switch activities such as FTP and Telnet, and is described in *Configuring Switch Logging* on page 7-6.

The other commands listed in the submenu above are support commands for Switch Logging.

- **cmdlog** command—displays the UI command entries in the flash file system (FFS) log (mpm.log) which is one of the possible destinations for Switch Logging data. See *Displaying the Command History Entries in the FFS Log* on page 7-10.
- **conlog** command—displays the connection entires in the FFS log. See *Displaying the Connection Entries in the FFS Log* on page 7-11.
- **caplog** command—displays the screen capture entries in the FFS log. See *Displaying Screen (Console) Capture Entries in the FFS Log* on page 7-12.
- **debuglog** command—shows the debug entries in the FFS log. See *Displaying Debug Entries in the FFS Log* on page 7-14.
- **seclog** command—shows the Secure Access violation event entries in the FFS log. See *Displaying Secure Access Entries in the FFS Log* on page 7-14.

Configuring the Syslog Parameters

Syslog messages are messages generated by individual processes in the switch. These messages contain information for conditions that range from debugging to emergency error conditions.

The **syslog** command allows you to control how these messages will be handled. You can designate what kinds of messages you will see and where the messages will be sent. This syslog implementation is compatible with the standard BSD UNIX implementation for syslog services.

To see the current syslog configuration, enter

```
syslog
```

at the system prompt. A screen similar to the following will be displayed.

```
SYSLOG current configuration:

 1) Log host                - UNDEFINED
 2) Log host IP             -
 3) Syslog port (514)       - 514
 4) Default facility code   - local0
   41) Override internals   - no
 5) Default priority mask   - emerg
   51) Override internals   - no
   52) Display internals    - no
 6) Console logging         - yes
 7) Log Task ID             - yes
   71) Use Task Name        - no
 8) Message tag             - switch

(save/quit/cancel)
      :
```

Select the number of the item you want to change. To change any of the values on the previous page, enter the line number, followed by an equal sign (**=**), and then the new value. For example, to turn off console logging, enter:

```
6=no
```

The question mark (**?**) option refreshes the screen. To update the values you have changed, enter **save**. If you do not want to save the changes enter **quit** or **cancel**, or press **Ctrl-D**.

The fields displayed by the **syslog** command are described below.

1. **Log host**. The name of the host where you want the syslog messages sent. The Domain Name Server (DNS) must be configured for this to work. Use the **res** command to configure the DNS. (The **res** command is described in Chapter 11, "RMON and DNS Resolver.")

2. **Log host IP.** The IP address of the host where you want the syslog messages sent. If the IP address and the Log host name disagree, the IP address takes precedence.

3. **Syslog port (514)**. The port to which the syslog messages will be sent on the specified host. Port 514 is the normal port number used and is the default.

4. **Default facility code.** The facility code is used to identify which sub-system generated the syslog message. Note that this code is used only as a default for tasks that do not have a facility code. See the table below for a list of the facility codes. The default is **local0**.

Syslog Facility Codes

Facility	Source
LOG_KERN	Messages generated by the kernel
LOG_USER	Message generated by random user processes
LOG_MAIL	The mail system
LOG_DAEMON	System daemons
LOG_AUTH	The authorization system
LOG_LPR	The line printer spooling system
LOG_NEWS	Reserved for the USENET system
LOG_UUCP	Reserved for the UUCP system
LOG_CRON	The cron/at facility
LOG_LOCAL0-7	Reserved for local use

41. Override internals. This setting will force all syslog messages to use the default facility code specified in item No. 4 above instead of their own predefined facility codes.

5. **Default priority mask.** The mask for the priority code. Indicates the type of syslog message. Note that this mask is used only as a default for tasks that do not have a priority code. Priority codes for syslog messages are usually hardcoded. The table below is a list of priority codes.

Syslog Priority Codes

Level	Value	Meaning
LOG_EMERG	0	FATAL system event
LOG_ALERT	1	FATAL subsystem event
LOG_CRIT	2	Problem, subsystem unstable
LOG_ERR	3	Problem, bad event, recoverable
LOG_WARNING	4	Unexpected, non-fatal event
LOG_NOTICE	5	normal but significant condition
LOG_INFO	6	info
LOG_DEBUG	7	Internal debug messages

51. **Override internals.** This field will force all syslog messages to use the default priority mask specified in item No. 5 above instead of their own predefined priority masks.

52. **Display internals**. This field allows the user to display the task log level. Enter **52=yes** to display the sub-menu below. If, for example, you wanted to change the priority mask **CM via kern** from "warn" to "alert," you would enter **4=alert**. Note that this change will take place immediately and you do not need to enter **save** for it to take effect. Type **save**, **quit**, or **cancel** and then press **<Enter>** to return to the main **syslog** menu.

```
Internal task syslog configuration:
 (NOTE: changes take effect immediately and
      are NOT saved across reboots!)

 0 )     PPM via kern          - alert
 1 )     LPM via kern          - alert
 2 )     VPM via kern          - alert
 3 )     SNMP via kern         - alert
 4 )     CM via kern           - warn
 5 )     ATMmgr via kern       - alert
 6 )     atmLANE via kern      - alert
 7 )     Q93bif via kern       - alert
 8 )     ILMIif via kern       - alert
 9 )     SSI0 via kern         - alert
 10)     atmSNMP via kern      - alert
```

6. **Console logging.** Determines whether or not you want to see syslog messages on your console (terminal). If set to yes, the messages will be displayed on either an **ASCII** terminal connected to the console port or via a Telnet session.

7. **Log Task ID**. Determines whether or not you want to see the task ID that can be included in the syslog message.

   71. **Use Task Name.** This allows the user to display descriptive task names for syslog messages (see the **Display internals** sub-menu above) instead of numeric codes.

8. **Message tag.** Text of up to 10 characters that is added to every message leaving the switch. It is useful when multiple switches send messages to the same host.

.

Configuring Switch Logging

Switch logging is a feature that allows you to activate and configure the logging of various types of switch information. Once you activate logging for a specific facility through the switch logging command, you also assign a priority level to the facility's output, if applicable. To enter the switch logging submenu, enter

swlogc

at the system prompt. A screen similar to the following displays:

```
                    CONFIGURATION MENU FOR SWITCH LOGGING

1) Security Logging                              : Disabled
   11) Output to File                                : Yes
   12) Output to Console                             : No
2) FTP Logging                                   : Disabled
   21) Output to File                                : Yes
   22) Output to Console                             : No
3) Flash File Logging                            : Disabled
   31) Output to Console                             : Yes
4) Screen Capture                                : Disabled
   41)Output to File                                 : Yes
5) Console Event Logging                         : Disabled
   51) Output to File                                : Yes
   52) Output to Console                             : No
6) User Interface Logging                        : Disabled
   61) Output to File                                : Yes
   62) Output to Console                             : No
7) Telnet Logging                                : Disabled
   71) Output to File                                : Yes
   72) Output to Console                             : No
8) Log File (mpm.log) Size                       : 20000 bytes
9) Return Logging to Default Configuration       : No

Command {Item/ Item=Value/ ?/ Help/ Quit/ Cancel/ Save} (Redraw) :
```

The options are described here:

1) Security Logging:

Enabling security logging allows you to view all security violations that occur within the switch. Set to **enable** to activate logging for any security violations that occur within the switch. Set to **disable** to de-activate logging for security violations.

♦ Note ♦

Security Violations must be enabled in order to display the Secure Switch Access violations log (**seclog**).

11) File:

Set to **yes** (**y**) to store the log in the flash file system. Set to **no** (**n**) to disable the flash file system as the output device for Security Logging.

12) Console:

Set to **yes** to store the log to the screen. Set to **no** to disable the screen as an output device for Security Logging.

2) FTP Logging

FTP Session Events is a record of all FTP (File Transfer Protocol) activities since session logging was activated. Once you enable FTP Logging by entering 2**=enable**, you may view it through the **conlog** command (described in *Displaying the Connection Entries in the FFS Log* on page 7-11). To disable FTP Session Events logging, enter **2=disable**. To store the data in the flash file system or screen, enter **21=yes**. To disable FTP Logging to the flash file system, enter **21=no**.

21) File

Set to **yes** (**y**) to store the log in the flash file system. Set to **no** (**n**) to disable the flash file system as the output device for Security Logging.

22) Console

Set to **yes** to store the log to the screen. Set to **no** to disable the screen as an output device for Security Logging.

3) Flash File Logging

FFS Log logging records debug information from the FFS Log facility itself. To enable the FFS Log, enter **3=enable**. To disable the FFS Log, enter **3=disable**. Logging to the flash file system is not permitted for this facility, but logging to the screen may be enabled by entering **31=yes**. To disable logging to the screen, enter **31=no**.

31) File

Set to **yes** (**y**) to store the log in the flash file system. Set to **no** (**n**) to disable the flash file system as the output device for Flash File Logging.

32) Console

Set to **yes** to store the log to the screen. Set to **no** to disable the screen as an output device for Flash File Logging.

4) Screen Capture

Screen logging captures screen text for logging. To enable screen logging, enter **4=enable**. To disable screen logging, enter **4=disable**. To store the screen capture in the flash file system, enter **41=yes**. Note that since screen text already goes to the screen, screen logging is not permitted. If you want to display the screen capture entries for all logged users, use the **caplog** command (for more information, see *Displaying Screen (Console) Capture Entries in the FFS Log* on page 7-12). To disable screen logging to the flash file system, enter **41=no**.

41) File

Set to **yes** (**y**) to store the log in the flash file system. Set to **no** (**n**) to disable the flash file system as the output device for Screen Capture.

42) Console

Set to **yes** to store the log to the screen. Set to **no** to disable the screen as an output device for Screen Capture.

5) Console Event Logging

Console Session Events is a record of all console login activities in the switch, including user names, privileges, and connection times. Once you enable Console Session Events logging by entering **5=enable**, you may view it through the **conlog** command (described in *Displaying the Connection Entries in the FFS Log* on page 7-11). To disable logging for Console Session Events, enter **5=disable**. To store the data in the flash file system, enter **51=yes**. To disable Console Session Events logging to the flash file system or screen, enter **no** at the corresponding line.

51) File

Set to **yes** (**y**) to store the log in the flash file system. Set to **no** (**n**) to disable the flash file system as the output device for Console Event Logging.

52) Console

Set to **yes** to store the log to the screen. Set to **no** to disable the screen as an output device for Console Event Logging.

6) User Interface Logging

User Interface Logging is executed on the switch since the session log was activated. Once you enable the UI Commands logging by entering **6=enable**, you may view it through the **cmdlog** command (described in *Displaying the Command History Entries in the FFS Log* on page 7-10). To disable logging for UI Commands, enter **6=disable**. Enter **61=yes** to store the data in the flash file system and **62=yes** to store the data on the screen. To disable UI Commands logging to the flash file system or screen, enter **no** at the corresponding line.

61) File

Set to **yes** (**y**) to store the log in the flash file system. Set to **no** (**n**) to disable the flash file system as the output device for User Interface Logging.

62) Console

Set to **yes** to store the log to the screen. Set to **no** to disable the screen as an output device for User Interface Logging.

6) Telnet Logging

Telnet Logging is a record of all Telnet activities since session logging was activated. Once you enable Telnet Session Events logging by entering **6=enable**, you may view it through the **conlog** command (described in *Displaying the Connection Entries in the FFS Log* on page 7-11). To disable logging for Telnet Session Events, enter **4=disable**. To store the data in the flash file system or screen, enter **61=yes** (ffs) or **62=yes** (screen). To disable Telnet Session Events logging to the flash file system or screen, enter **no** at the corresponding line.

61) File

Set to **yes** (**y**) to store the log in the flash file system. Set to **no** (**n**) to disable the flash file system as the output device for Telnet Logging.

62) Console

Set to **yes** to store the log to the screen. Set to **no** to disable the screen as an output device for Telnet Logging.

7) Log File Size

Set this parameter to the log file size you desire. The default is 20000 bytes. The maximum number of bytes is dependent upon the available flash in your system. If you set a file that is too large, the command will tell you the maximum allowed size.

8) Return Logging to Default Configuration

Use this parameter to return all of the switch logging options to their default values. Enter **8=yes** to reset the configuration at reboot. To keep the same logging configuration at the next reboot, make sure this parameter is set to **no**.

Displaying the Command History Entries in the FFS Log

The **cmdlog** command displays a list commands executed since this facility logging was activated by the **swlogc** command (described in *Configuring Switch Logging* on page 7-6). To display this data, enter

```
cmdlog
```

at the system prompt. The following is a sample display.

```
User       Line                  Time                       User Input
---------- --------------------- -------------------------- --------------------------
admin      198.206.187.113       TUE NOV 18 16:42           cmdlog
admin      198.206.187.113       TUE NOV 18 16:42           xlat
admin      198.206.187.113       TUE NOV 18 16:43           conlog
admin      console               WED NOV 19 10:28           logging
admin      console               WED NOV 19 10:28           ?
admin      198.206.187.113       WED NOV 19 14:03           taskstat
admin      198.206.187.113       WED NOV 19 14:05           taskstat
```

The fields displayed by the **cmdlog** command are described below.

User. The login name of the user who executed the command.

Line. The login type of the user who executed the command. If, for example, the user was connected through the console port, "console" will be displayed. If the user was connected through Telnet, on the other hand, then the IP address of that user will be displayed.

Time. The time that the command was executed.

User Input. The actual text (up to 32 characters) that the user entered at the system prompt.

♦ Note ♦

If you just want to display the commands executed during the current session you can use the **history** command, which is described in Chapter 2, "The User Interface."

Displaying the Connection Entries in the FFS Log

The **conlog** command displays a list of connections made since a connection logging was activated by the **swlogc** command (described in *Configuring Switch Logging* on page 7-6). To display this data, enter

```
conlog
```

at the system prompt. A screen similar to the following will be displayed.

```
User        Line          Peer              Start                 Finish
--------    ----------    ---------------   ----------------      ------------------
CREATED     system                          FRI NOV 14 10:05
admin       Telnet        198.206.187.113   WED NOV 19 09:47 -    09:47  (00:00)
admin       Telnet        198.206.187.113   WED NOV 19 09:47 -    09:53  (00:05)
admin       Telnet        198.206.187.113   WED NOV 19 09:55 -    10:00  (00:05)
admin       console                         WED NOV 19 10:35      logged in  (00:27)
admin       Telnet        198.206.187.113   WED NOV 19 11:02      logged in(00:00)
```

The fields displayed by the **conlog** command are described below.

User. Normally, this field lists the name of the user who made the connection to the switch. At the beginning of the log it will display **CREATED** instead.

Line. The login type of connection to the switch (e.g., a Telnet or console port connection).

Peer. If the user was connected through Telnet, then the IP address of the user will be displayed. If the user was connected through the console port, then this field will be blank.

Start. The time that the connection started.

Displaying Screen (Console) Capture Entries in the FFS Log

The **caplog** command displays the screen capture entries in the FFS log. In order to view screen capture entries through this command, you must first enable the Screen Capture log facility through the **swlogc** command (see *Configuring Switch Logging* on page 7-6). To display screen capture entries in the FFS log, enter

```
caplog
```

at the system prompt. A screen similar to the following will be displayed.

```
1) Console
2) Modem
3) Telnet (0)
4) Telnet (1)
5) Telnet (2)
6) Telnet (3)
        select ?
```

Select which user's screen entries you would like to view by entering the user's line number at the prompt. The following is a sample display of screen capture entries after you have made your selection:

```
1) Console
2) Modem
3) Telnet (0)
4) Telnet (1)
5) Telnet (2)
6) Telnet (3)
        select ? 1
=======================Start Screen Capture Display for Console==================

        / % systat

        System Uptime                   : 0 days, 01:01:47.01
        MPM Transmit Overruns           : 0
        MPM Receive Overruns            : 0
        MPM total memory                : 18548968 bytes
        MPM CPU Utilization (5 sec)     : 3 % ( 0% kernel 1% task 97% idle)
        MPM CPU Utilization (60 sec)    : 4% ( 0% intr 0% kernel 2% task 96% idle)\
        Power Supply 1 State            : OK
        Power Supply 2 State            : Not Present
        Temperature                     : 32.00c 89.60f
        Temperature Sensor              : OF - Under Threshold
        Temperature Alarm Masking       : Disabled
=======================End Screen Capture Display for Console==================
```

The options displayed by the **caplog** command are described below.

1) Console. Displays screen capture entries for the user logged in from the console.

2) Modem. Displays screen capture entries for the user logged in from the modem.

3) Telnet (0). Displays screen capture entries for the user logged in from the first telnet session.

4) Telnet (1). Displays screen capture entries for the user logged in from the second telnet session.

5) Telnet (2). Displays screen capture entries for the user logged in from the third telnet session.

6) Telnet (3).Displays screen capture entries for the user logged in from the fourth telnet session.

Displaying Debug Entries in the FFS Log

The **debuglog** command displays the debug entries in the FFS log. Debug entries are only available to users logged in as **debug** or **diag**. Please note that currently, there are no facilities using debugging. Below is a sample display of the **debuglog** command.

```
Task Name                        Time                Debug Message
-------------------------------- ------------------- ------------------------------------------------------------
tUdpRelay                        14:33:36            Undersized DHCP req rcvd; discarding
```

The fields displayed by the **debuglog** command are described below.

Task Name. The task that generated the debug message.

Time. The time the message was generated by the task.

Debug Message. Information relevant to debugging.

Displaying Secure Access Entries in the FFS Log

The **seclog** command displays the secure access violation event entries in the FFS log. To display this data, enter

```
seclog
```

at the system prompt. A screen similar to the following will be displayed.

```
Secure Access Violations Log

Time                    Protocol    Source IP       Attempts   Slot/ Intf   Elapsed Time (secs)
----------------------- ----------- --------------- ---------- ------------ --------------------
12:49:02                FTP         172.23.8.801    1          5/1          23
03:15:34                Telnet      198.20.2.101    10         2/3          240
```

Descriptions of the fields are as follows:

Time. The first time the access violation occurred.

Protocol. The IP protocol for which the violation occurred.

Source IP. The source IP address of the unauthorized user.

Attempts. The number of access attempts made by this user within the sample period (5 minutes).

Slot/Intf. The physical port that received the unauthorized user information.

Elapsed Time (secs). The duration (in seconds) from the first unauthorized access to the end of the sampling period.