Chapter 33

Logging Facility

Introduction

The Logging facility generates, processes, and displays log messages from the router. User-defined output definitions provide a powerful and flexible mechanism to filter and prioritise log messages, and to output selected messages to RAM, an asynchronous port on the router, or a UNIX syslog server. A secure router-to-router log message protocol (SRLP) forwards log messages from regional and remote office routers to a central router for monitoring and processing.

The Logging facility is backwardly compatible with the Net Manage log system. Net Manage log messages generated locally or forwarded via UDP port 5024 are intercepted by the new Logging facility and converted into the new log message format.

A major task of network management is to monitor the operation of both permanent and on-demand network links (such as PPP links, ISDN calls, Frame Relay, X.25 circuits), to maintain a high level of availability of network services, to record network usage and loading information for planning future developments, and for billing purposes.

The Logging facility provides network managers with a powerful, flexible, and easily configurable tool to monitor network activity and to display results. The Logging facility provides the following functions:

- Processing log messages generated by any router module.
- Forwarding log messages to other routers, and reception of log messages from other routers, via the Secure Router Log Protocol (SRLP, UDP port 5023).
- Receiving Net Manage (UDP port 5024) log messages from other routers, or UNIX syslog messages, and conversion to the new log message format.
- Forwarding log messages to a UNIX syslog server (UDP port 514).
- Filtering log messages based on user-defined filters.
- Storing selected log messages in RAM.
- Outputting log messages via email in either full or summary format.
- Outputting log messages to an asynchronous port in either full or summary format.
- Displaying log messages stored in RAM, or messages queued for processing.

The Logging facility is particularly helpful in tracking the following:

- critical router problems (`SEVERITY=>5`)
- interface status changes (`TYPE=VINT`)
- user login/authentication (`TYPE=AUTH`, `TYPE=USER`)
- trigger activity and script output (`TYPE=BATCH`)
- asynchronous call control (ACC) activity (`TYPE=ACC`)
- router commands (`TYPE=CMD`)
- router messages (`TYPE=MSG`)
- matches to IP filters, including IP header information and the contents of the data portion of IP packets (`TYPE=IPFILT`)

Format of Log Messages

A log message is a single entry in a router log, and is the fundamental unit of information processed by the Logging facility. Each log message contains a number of data fields (Table 33-1 on page 33-3). A log message may contain accounting, user, debugging or other information as determined by the values of the log message fields. Depending on the type of log message generated, not all fields contain a value.

Table 33-1: Log message fields .

Field	Size (bytes)	Description
Msg ID	4	Unique ID number for this message.
Flags	2	Contains control flags and the severity of the message. Severity is expressed as a number from 0 to 7 (Table 33-2).
Date	2	Local date when the message was generated (for the router that generated the message).
Time	3	Local time when the message was generated (for the router that generated the message). Messages are stored and processed using UTC (Universal Coordinated Time) so that routers in different time zones can share messages.
Origin IP	4	IP address of the originator of the message.
Module	2	ID of the module generating the message. See "Module Identifiers and Names" on page C-2 of Appendix C, Reference Tables for a complete list.
Type	2	Identifies the general category of event that triggered the log message.Types can be specified or displayed by name or numeric identifier. See "Log Message Types and Subtypes" on page C-11 of Appendix C, Reference Tables for a complete list.
SubType	2	Identifies a specific event within that category. Subtypes can be specified or displayed by name or numeric identifier. See "Log Message Types and Subtypes" on page C-11 of Appendix C, Reference Tables for a complete list.
Source File	12	File name of the source file where the message originated.
Source Line	2	Line number in the source file where the message originated.
Reference	15	Reference ID (for example, user name, ISDN call name). Type and SubType fields determine the contents of this field.
Message	80	Message text. Type and SubType fields determine the contents of this field.

Table 33-2: Log message severity levels .

Severity	Value	Description
CRITICAL	7	Router operation severely impaired.
URGENT	6	Router operation has been or could be affected.
IMPORTANT	5	Issue that requires manager attention, possible problem.
NOTICE	4	Issue that may require manager attention.
INFO	3	Normal notification of an event, but not serious or particularly important.

Table 33-2: Log message severity levels (continued).

Severity	Value	Description
DETAIL	2	Useful information that can be ignored during normal operation.
TRIVIAL	1	Generally unimportant everyday events.
DEBUG	0	Extremely detailed (possibly high-volume) debugging information.

Secure Router Log Protocol (SRLP)

The Logging facility provides an extensible log message protocol, the Secure Router Logging Protocol (SRLP), to permit the secure exchange of log messages between routers.

A log message is encoded into a UDP datagram with a checksum and an MD5 authentication digest, and transmitted to UDP port 5023. Since UDP is an unreliable transport medium, each log message must be acknowledged by the receiver. The acknowledgements (ACKs) are also UDP datagrams transmitted to UDP port 5023. Unacknowledged messages are retransmitted after 1, 4, 16, 64, and 256 minutes.

UDP packets are protected by encryption, preventing them from being read by unauthorised parties, and can be authenticated using passwords and MD5 digests.

Net Manage Message Protocol

The Logging facility accepts log messages from routers using the Net Manage UDP logging protocol on port 5024. The Logging facility does **not** return log messages to routers that use this protocol, but instead generates ACKs to acknowledge reception of the Net Manage messages. No other Net Manage facilities are supported.

Net Manage messages received via the Net Manage logging protocol or generated locally are converted to the new log message format. Log message fields with no equivalent in the old Net Manage message format are set to defaults. In particular, the Type and Subtype fields are set to NULL (displayed as a blank in output) and the Severity field is set to 0.

Processing Log Messages

The processing of log messages is controlled by user-defined filters and output definitions.

Output Definitions and Message Filters

A *log message filter* is a set of conditions on the fields of a log message. Log messages that meet these conditions are said to “match” the filter. Log message filters specify log entries that should be displayed (using the **show log** command on page 33-34), accepted for further processing by an output definition, or ignored.

An *output definition* describes the processing to be performed on log messages that match one of the log message filters associated with the output definition. Log messages can be stored in RAM, output to an asynchronous port on the router, sent via email to a specified email address, forwarded to another router via the Secure Router Logging Protocol (SRLP), or forwarded to a UNIX syslog server. An output definition may have one or more associated log message filters.

The Logging facility can receive Net Manage messages locally generated or via the Net Manage protocol on UDP port 5024, syslog messages on UDP port 514, and new-format log messages generated locally or transmitted via the new Secure Router Logging Protocol (SRLP) on UDP port 5023. Net Manage and syslog messages are automatically converted to the new log message format. When a log message is received, the Logging facility checks to see whether the log message can be processed by one or more of the output definitions.

Filters associated with each output definition are applied in sequence. When a log message matches a filter with an IGNORE action, processing continues with the next output definition, if any. When the log message does not match a filter, processing continues with the next output definition, if any. When the log message matches a filter with a PROCESS action, the log message is processed according to the output definition. Processing then continues with the next output definition, if any.

A single log message may be processed more than once. For example, all regional and remote office routers could be configured to forward all log messages to a central site router. At the central site router, log messages could be stored in RAM and output to an asynchronous port where a printer is attached. In addition, all low severity log messages relating to user activity (for example, logins) and on-demand links (for example, normal call establishment and clearing) could be forwarded to a syslog server on an accounting host, while high severity log messages are forwarded to a syslog server on a network management station.

Each output definition has its own separate message queue. When a log message matches a filter associated with an output definition, a copy of the log message is placed on the output definition queue as part of the processing performed by the output definition. The function of the queue varies depending on the output definition. For output definitions that store log messages in RAM, the queue represents the actual log messages stored in RAM. The **show log** command on page 33-34 simply displays the contents of the queue. For output definitions that forward log messages to an asynchronous port, to an email address, to another router via SRLP, or to a syslog server, the queue represents the log messages waiting to be processed (or acknowledged).

The flexibility of the output definition mechanism means that it is possible to create two or more output definitions with the same destination (e.g. a syslog server) but with different filters. As a result, the Logging facility maintains two or more separate queues of log messages, all of which are waiting to be forwarded to the same syslog server. This flexibility could potentially cause problems for output definitions that store messages in RAM. The TEMPORARY output definition accepts a destination of MEMORY (RAM). Messages processed by this output definition can be displayed by the **show log** and **show log=temporary** commands.

Destinations

Storage in RAM

Log messages may be stored in the router's RAM memory. Log messages stored in RAM are **not** retained over a power failure or router restart. There is no preset limit on the number of log messages that can be stored in RAM, except that log messages are not stored in RAM when the number of buffers falls below Buffer Level 2. However, the maximum number of messages that may be stored in RAM at any one time can be configured. When the number of messages reaches the maximum, the oldest message is deleted to make room for a new message.

Output to an Asynchronous Port

Log messages may be output to an asynchronous port, which can be connected to a serial printer, terminal, or other serial device. Log messages may be displayed in either summary or full format.

Forwarding Via Email

Log messages may be transferred to an email address in either summary or full format. The source of the email message appears in the message's "From" header field.

Forwarding to Another Router Via SRLP

Log messages may be transferred to a central router for display, processing and output, using the Secure Router Logging Protocol (SRLP). The messages transferred to the remote router appear intact, with no information loss. The remote router knows where the log message came from, and this can be displayed with the **show log** command on page 33-34 by using the **full** parameter.

Forwarding to a UNIX Syslog Server

Log messages may be converted to UNIX syslog format and transmitted to a UNIX-style logging daemon, normally called syslogd, on a host accessible via IP. Syslog is a system Logging facility provided by many versions of UNIX. Some translation is performed to match the database-like structure of the router's log message format to the textual format of syslog records.

The type and subtype codes are translated into syslog facility identifiers (Table 33-3 on page 33-7) and the log message severity is translated into a syslog "level" (Table 33-4 on page 33-7). When converted to syslog textual format, the module ID in the new log message format is converted to a short module abbreviation at the start of the syslog message.

The syslog-format messages are transmitted via UDP to the syslog port of the defined syslog server. The syslog protocol does not support message encryption, authentication or reliable delivery (acknowledgements).

Table 33-3: Mapping between Logging facility module identifier, type and subtype, and syslog facility identifiers .

Type	Facility	Meaning
000/NULL	LOG_USER	Log messages without a type (old message format.)
010/LIC		Licencing information.
011/AUTH	LOG_AUTH	Authentication and security issues.
012/TRIG	LOG_CRON	Time-based activities (triggers and output).
013/LPR	LOG_LPR	Line Printer Daemon activity.
001/REST	LOG_LOCAL7	Router restarts.
008/EXCEP		Exceptions.
009/BUFF		Buffer issues.
002/PINT	LOG_LOCAL6	Physical interface and data-link issues.
003/DLINK		
004/CALL	LOG_LOCAL5	ISDN, ACC, and L2TP call issues.
005/VINT		Virtual Interface issues.
006/CIRC	LOG_LOCAL4	Circuit, DLCI and PPP control protocol issues.
007/ATT		Attachments.

Table 33-4: Mapping between Logging facility severity levels and syslog levels .

Severity	Syslog Level	Meaning
7	LOG_EMER	Emergency error, system unusable.
6	LOG_ALERT	Router error, function impaired.
5	LOG_CRIT	Critical link or interface problem, may not work.
4	LOG_ERR	Less serious problem or authentication warning.
3	LOG_WARNING	Possible problem with interface or configuration.
2	LOG_NOTICE	Fairly important informational message/tracing.
1	LOG_INFO	Less important informational message/tracing.
0	LOG_DEBUG	Trivial debugging or tracing.

If you send messages to a syslog server, they have normal format by default (Figure 33-1).

Figure 33-1: Examples of syslog messages with **syslogformat=normal**

```
<12>SSH:SSH/ACPT, SSH connection accepted - pwduser
<14>CH:CMD/USER, logoff
<12>USER:USER/LOFF, pwduser logoff on TTY17
```

To send extended log messages with date, time, and system name to the syslog server (Figure 33-2), use one of the commands:

```
create log output={temporary|output-id} destination=syslog
   syslogformat=extended [other-log-parameters]
```

```
set log output={temporary|output-id} [destination=syslog]
   syslogformat=extended [other-log-parameters]
```

Figure 33-2: Examples of syslog messages with **syslogformat= extended**

```
23-Oct-2003 16:39:37 <12>SSH:SSH/ACPT, Src: AR450 ,SSH connection accepted - pwduser
23-Oct-2003 16:39:41 <14>CH:CMD/USER, Src: AR450 ,logoff
23-Oct-2003 16:39:41 <12>USER:USER/LOFF, Src: AR450 ,pwduser logoff on TTY17
```

To set the system name to a unique identifier, use the command **set system name** command on page 1-124 of Chapter 1, Operation.

Configuring Output Definitions

By default, logging is enabled. The TEMPORARY output definition contains a log message filter that matches all log messages of severity 3 or greater, and stores up to 300 messages in RAM.

To create an output definition, use the **create log output** command on page 33-17.

A log message filter must be defined for the output definition before the output definition can process any log messages. By default, output definitions are enabled when they are created. Output definitions can be temporarily disabled with the **disable log output** command on page 33-23. To enable them, use the **enable log output** command on page 33-24.

To modify an existing output definition, use the **set log output** command on page 33-26.

To delete an output definition, use the **destroy log output** command on page 33-22.

To display the currently configured output definitions, use the **show log output** command on page 33-42.

Configuring Message Filters

When an output definition is created, it has no associated log message filters and therefore no log messages are selected for processing by the output definition. At least one log message filter must be defined and associated with the output definition before the output definition becomes active (starts processing messages).

To create a log message filter and associate it with an output definition, use the **add log output** command on page 33-12.

To modify an existing log message filter, use the **set log output** command on page 33-26.

Most filter parameters support additional operators (<, >, !, %) between the equals sign ("=") and the value that modifies the comparison between the value in the filter and the value in the log message field (Table 33-5 on page 33-9).

Table 33-5: Log message filter comparison operators .

Operator	Example	Meaning
< Less than	severity=<5	The log message matches when the value in the log message field is less than the value specified in the filter.
> Greater than	device=>1	The log message matches when the value in the log message field is greater than the value specified in the filter.
! Not equal	type=!2	The log message matches when the value in the log message field is not equal to the value specified in the filter.
(none) Equal	mod=PPP	The log message matches when the value in the log message field is equal to the value specified in the filter.
% Contains substring	ref=%call	The log message matches when the value in the log message field contains the value specified in the filter (string fields only).

To delete a log message filter, use the **create log output** command on page 33-17.

To display log message filters definitions that are currently configured, use the **show log output** command on page 33-42.

Configuration Example

The following example shows how to configure the Logging facility in a wide area network environment (Figure 33-3, Table 33-6 on page 33-10). A router at the remote office is connected via a wide area link to a router at the head office. The remote router is configured to forward all log messages to the head office router via the Secure Router Logging Protocol (SRLP) with password authentication. At the head office router, all log messages are to be stored in RAM. In addition, all log messages relating to ISDN or ACC calls are forwarded to a syslog server for accounting purposes, and all critical log messages are forwarded via an asynchronous port to a network management station.

Figure 33-3: Example configuration for a basic Logging facility.

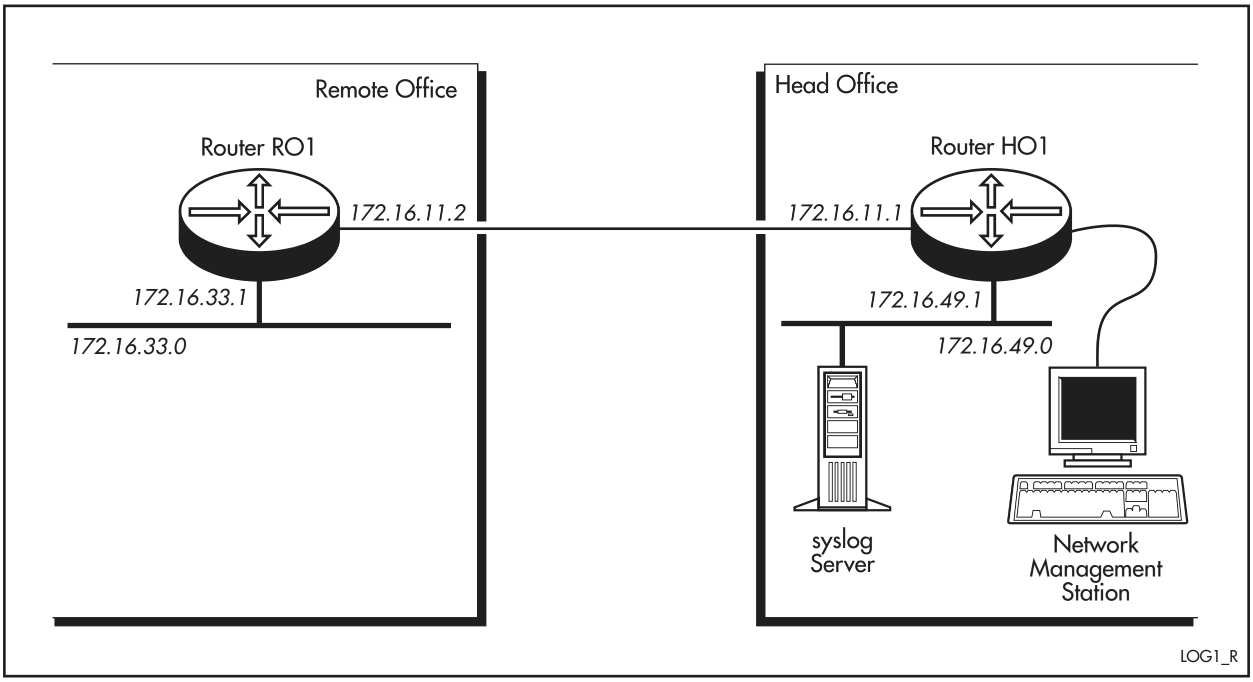

Table 33-6: Example configuration parameters for a basic Logging facility .

Parameter	**Head Office**	**Remote Office**
Router name	HO1	RO1
IP address of LAN	172.16.49.0	172.16.33.0
IP address of Ethernet interface eth0	172.16.49.1	172.16.33.1
IP address of PPP link	172.16.11.0	172.16.11.0
IP address of PPP interface ppp0	172.16.11.1	172.16.11.2
NMS connected to asynchronous port	1	-
IP address of syslog server	172.16.49.8	-

To configure the remote office router:

1. **Enable the Logging facility.**

   Logging is enabled by default but verify this by using the command:

   ```
   show log status
   ```

   If necessary, enable logging and the generation of log messages by using:

   ```
   enable log
   enable log generation
   ```

2. **Create an output definition and a message filter.**

   Create an output definition to forward log messages via the Secure Router Logging Protocol (SRLP) to the head office router, with password authentication. The SECURE option defaults to YES when DESTINATION is set to ROUTER and a password is specified, so security-related messages (for example, password changes) are processed by this output definition:

   ```
   enable ip
   create log output=1 destination=router server=172.16.11.1
      password=GB4La8z
   ```

Add a log message filter that matches any log message to the output definition so that all log messages generated on the router are processed by this output definition. The FILTER parameter is optional; by default the filter is added to the end of the list of filters:

```
add log output=1 filter=1 all
```

3. **Check the configuration.**

   Check that the output definition and message filter configuration is correct by displaying the output definition and its associated filters:

```
show log output=1 full
```

To configure the head office router:

1. **Enable the Logging facility.**

   Logging is enabled by default but verify this by using the command:

```
show low status
```

   If necessary enable logging and the generation of log messages:

```
enable log
enable log generation
```

2. **Enable the reception of log messages from the remote router.**

   Enable the reception of log messages via SRLP, and add the remote router to the log reception table so that log messages are accepted from the remote router with password authentication:

```
enable log reception
add log receive=172.16.11.2 password=GB4La8z protocol=NEW
```

3. **Create output definitions and message filters.**

   The TEMPORARY output definition is automatically defined by the system to match all log messages of severity 3 or greater and to store the log messages in RAM. Since this is exactly what is required in this example, there is no need to specify this output definition any further.

   Log messages cannot be stored permanently on the router. If log messages are not forwarded to an asynchronous port, another router (via SRLP) or a syslog server, they are lost when the router restarts.

   Create an output definition and associated message filter to output all critical log messages to asynchronous port 1:

```
create log output=1 destination=asyn asyn=1 format=full
add log output=1 filter=1 severity=>5
```

   Create an output definition and associated message filter to output all call-related log messages to the syslog server:

```
create log output=2 destination=syslog server=172.16.49.8
   messages=20
add log output=2 filter=1 type=call
```

4. **Check the configuration.**

   Check that the output definition and message filter configuration is correct by displaying the output definitions and their associated filters:

```
show log output full
```

Command Reference

This section describes the commands to configure and manage the Logging facility in the router.

Some features and options of the Logging facility require the IP module to be enabled and configured correctly. See Chapter 14, Internet Protocol (IP) for detailed descriptions of the commands required to enable and configure IP.

The shortest valid command is denoted by capital letters in the Syntax section. See "Conventions" on page xcv of Preface in the front of this manual for details of the conventions used to describe command syntax. See Appendix A, Messages for a complete list of messages and their meanings.

add log output

Syntax

```
ADD LOG OUTput={Temporary|output-id} [ACtion={Process|
    Ignore}] [ALL] [DATE=[op]dd-mmm-yyyy]
    [DEVice=[op]device] [FIle=[op]filename]
    [FILter=filter-id] [MASK=ipadd] [MSGtext=[op]string]
    [MODule=[op]module-id] [ORIGin=ipadd]
    [REFerence=[op]string] [SEVerity=[op]0..7]
    [SOUrceline=[op]line] [SUBType=[op]subtype-id]
    [TIme=[op]hh:mm:ss] [TYpe=[op]type-id]
```

where:

- *output-id* is the index number of an output definition from 1 to 20.
- *filter-id* is a filter entry number from 1 to *n*+1 where *n* is the number of filters currently defined for the output definition.
- *op* is a comparison operator (Table 33-5 on page 33-9).
- *dd-mmm-yyyy* is a date where *dd* is the day of the month, *mmm* is an abbreviation for the month or the 2-digit number of the month, and *yyyy* is the year.
- *device* is a router device number.
- *filename* is a module source file name 1 to 12 characters long.
- *ipadd* is an IP address in dotted decimal notation.
- *module-id* is the name or number of a router module. See "Module Identifiers and Names" on page C-2 of Appendix C, Reference Tables for a complete list.
- *string* is a character string 1 to 15 characters long.
- *severity* is a log message severity from 0 (low) to 7 (high).
- *line* is a line number in a module source file from 1 to 65535.
- *subtype-id* is the name or number of a log message subtype. See "Log Message Types and Subtypes" on page C-11 of Appendix C, Reference Tables for a complete list.

- *hh:mm:ss* is a time, where *hh* is the hour, *mm* is the minutes, and *ss* is the seconds.
- *type-id* is the name or number of a log message type. See "Log Message Types and Subtypes" on page C-11 of Appendix C, Reference Tables for a complete list.

Description This command adds a log filter to the specified output definition. The log filter specifies a set of conditions that must hold for a log entry to *match* the filter, and whether to *process* or *ignore* matching log messages. If there are no conditions specified, the filter matches nothing.

The OUTPUT parameter specifies the number of the output definition where the filter entry is to be added. The output definition must already exist. If TEMPORARY is specified, the filter is added to the special TEMPORARY output definition.

The FILTER parameter specifies the entry number of the filter within the output definition. If FILTER is specified, the filter is inserted into the filter list at the specified position. If FILTER is not specified, the filter is added to the end of the filter list for the output definition.

The ACTION parameter specifies the action to perform for log messages matching this filter. If PROCESS is specified, the log message is processed according to the output definition. If IGNORE is specified, the log message is ignored and not processed by this output definition. The default is PROCESS.

The ALL parameter matches all log entries. If ALL is specified, no other selection criteria may be specified for this filter. The default is to match log entries fitting the specified criteria.

The DATE parameter specifies the date value to match in the log message. The first character of the value may be one of the comparison operators "<", ">" or "!" to modify the comparison from "equals" (the default) to "less than or equal to", "greater than or equal to" or "not equal to" respectively (Table 33-5 on page 33-9). The default is to match any date.

The DEVICE parameter specifies the device number to match in the log message. The first character of the value may be one of the comparison operators "<", ">" or "!" to modify the comparison from "equals" (the default) to "less than or equal to", "greater than or equal to" or "not equal to" respectively (Table 33-5 on page 33-9). The default is to match any device number.

The FILE parameter specifies the name of a source file to match in the log message. The first character of the value may be one of the comparison operators "<", ">" or "!" to modify the comparison from "equals" (the default) to "less than or equal to", "greater than or equal to" or "not equal to" respectively (Table 33-5 on page 33-9). The default is to match any source file.

The MASK parameter specifies a subnet mask to use in association with the ORIGIN IP address parameter. The default is 255.255.255.255.

The MSGTEXT parameter specifies a string to match in the text of the log message. The first character of the value may be one of the comparison operators "<", ">", "!" or "%" to modify the comparison from "equals" (the default) to “less than or equal to”, “greater than or equal to”, “not equal to” or “contains substring” respectively (Table 33-5 on page 33-9). The default is to match any text.

The MODULE parameter specifies the router module to match in the log message, as either a decimal number or a recognised module name. See “Module Identifiers and Names” on page C-2 of Appendix C, Reference Tables for a complete list. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any module.

The ORIGIN parameter specifies the IP address to match against the originating IP address field of the log message.

The MASK parameter can specify a host, subnet, or network. The default is to match any IP address in the origin IP address field.

The REFERENCE parameter specifies the reference to match in the log message. The first character of the value may be one of the comparison operators “<”, “>”, “!” or “%” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to”, “not equal to” or “contains substring” respectively (Table 33-5 on page 33-9). The default is to match any reference.

The SEVERITY parameter specifies the log message severity level to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any severity.

The SOURCELINE parameter specifies the line number in the source file where the log message was generated, to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any source line number.

The SUBTYPE parameter specifies the log message subtype to match, as either a decimal number or a recognised subtype name. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any log message subtype.

The TIME parameter specifies the time value to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any time.

The TYPE parameter specifies the log message type to match, as either a decimal number or a recognised type name. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list). The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any log message type.

Parameter values that contain spaces must be in double quotes. If one of the operators ("<", ">", "!", "%") is also present, the operator must be inside the quote marks. For example, **add log output=4 msgtext="%ppp inter"**.

Examples To add a filter to output definition 17 that causes log messages with severity less than 6 to be ignored, use the command:

```
add log out=17 sev=<6 ac=i
```

Related Commands delete log output
set log output
show log output

add log receive

Syntax

```
ADD LOG RECeive={ipadd|ANY} [ALLOw={False|NO|OFF|ON|True|
    YES}] [MASK=ipadd] [PASSword={password|NONE}]
    [PROTocol={ALL|BOTh|NEW|OLD|SYSlog}]
```

where:

- *ipadd* is an IP address in dotted decimal notation.
- *password* is a character string 1 to 16 characters long. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.

Description This command adds an entry to the log reception table. When not empty, the log reception table specifies the router (and networks/subnets if MASK is specified) where log messages are to be accepted. If the log reception table is empty (the default), log messages are not accepted from any source. When comparing the source addresses of received log messages, the most specific entry is used. The order of entries in the log reception table is not significant.

The RECEIVE parameter specifies the IP address of the host, subnet or network from which log messages are to be received. If ANY is specified, a wildcard entry is added to accept log messages from any IP address. If more than one receive entry matches an IP address, the most specific entry (the one with the most specific network mask) is used.

The ALLOW parameter specifies whether log messages are to be accepted from the specified IP address. If YES is specified, log messages are accepted from the IP address. If NO is specified, log messages are not accepted from the IP address. The default is YES.

The MASK parameter specifies a subnet mask to use in association with the RECEIVE parameter. The default is 255.255.255.255 if an IP address is specified for the RECEIVE parameter, or 0.0.0.0 if ALL is specified for the RECEIVE parameter.

The PASSWORD parameter specifies the password that must accompany log messages from the specified IP address, for authentication purposes when log messages are forwarded to another router via the Secure Router Logging Protocol (SRLP). If the PASSWORD option is present, the specified password must accompany log messages from the specified IP address.

The PROTOCOL parameter specifies the protocol to use for message reception from the specified IP address. If OLD is specified, the Logging facility accepts old Net Manage (UDP port 5024) packets. If NEW is specified, the Logging facility accepts the new Secure Router Logging Protocol (SRLP) packets. If SYSLOG is specified, the Logging facility accepts syslog messages. The BOTH option is equivalent to specifying both OLD and NEW. The ALL option is equivalent to specifying OLD, NEW and SYSLOG. The PASSWORD parameter is not valid when TYPE is set to OLD or SYSLOG, as password authentication is not supported in these protocols.

Examples

To ensure that only log messages from network 192.168.0.0 are processed, use the command:

```
add log receive=192.168.0.0 mask=255.255.0.0 proto=bot
```

To accept messages from subnet 192.168.2.0 only with password SECRET, use the command:

```
add log rec=192.168.2.0 mask=255.255.255.0 pass=secret
    prot=new
```

Related Commands

delete log receive
set log receive
show log receive

create log output

Syntax

```
CREate LOG OUTput={Temporary|output-id}
   DEStination={Email|Memory|ASYN|Router|Syslog}
   [ASYn=port-number] [FACILITY={DEFAULT|LOCAL1…LOCAL7}]
   [FORMat={Full|MSGOnly|Summary}]
   [MAXQueueseverity=severity] [MESSages=message-count]
   [PASSword={password|NONE}] [QUEueonly={False|NO|OFF|ON|
   |True|YES}] [SECure={False|NO|OFF|ON|True|YES}]
   [SERVER=ipadd] [SYslogformat=Extended|Normal]
   [TO=email-address] [ZOne={time-zone-name|
   utc-offset}][LOCAL={NONE|1..15}]
```

where:

- *output-id* is the index number of an output definition from 1 to 20.
- *severity* is a message severity level from 0 (low) to 7 (high).
- *message-count* is the maximum number of log messages that may be queued for processing.
- *password* is a character string 1 to 16 characters long. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.
- *port-number* is the number of an asynchronous port. Ports are numbered sequentially starting with port 0.
- *ipadd* is an IP address in dotted decimal notation.
- *email-address* is a character string 3 to 80 characters long. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.
- *time-zone-name* is the name of a recognised time zone (Table 33-7 on page 33-19).
- *utc-offset* is a time offset from GMT/UTC from +23:59:59 to 23:59:59.

Description

This command creates an output definition, which specifies the processing to be performed on log messages that match one of the log message filters associated with the output definition. The specified output definition must not already exist. Once the output definition has been created, log message filters are added using the **add log output** command on page 33-12.

The OUTPUT parameter specifies the index number of the output definition to be created, or the special output definition TEMPORARY. If TEMPORARY is specified, the parameters MAXQUEUESEVERITY, QUEUEONLY and SECURE may not be specified. An output definition must not already exist with this index number.

The DESTINATION parameter specifies the type of processing to be performed and the destination of log messages processed by this output definition. The EMAIL option forwards log messages to the email address specified by the TO parameter. If DESTINATION is set to EMAIL, the parameter TO must also be specified. The MEMORY option stores log messages in RAM. The MEMORY option is valid when OUTPUT is set to TEMPORARY. The ASYN option outputs log messages to an asynchronous port on the router. If DESTINATION is set to ASYN, the parameters MAXQUEUESEVERITY, MESSAGES and QUEUEONLY may not be specified. The ROUTER option forwards log messages via the Secure Router Logging Protocol (SRLP) to another router. The SYSLOG option forwards log messages in syslog format to a syslog server.

The FACILITY parameter specifies whether to override the mapping between logging facility type and syslog facility identifiers. The DEFAULT option keeps the mapping between type and facility. If LOCAL1…LOCAL7 are specified then the syslog facility identifier will always be sent with the value specified. The FACILITY parameter is valid only if DESTINATION is set to SYSLOG. The default for FACILITY is DEFAULT.

The FORMAT parameter specifies the format of log messages when converted into ASCII text for output to an asynchronous port. The FULL option displays the entire log message in multiple lines, with a blank line between messages. The SUMMARY option produces an abbreviated display. The MSGONLY option displays the text of the message. The FORMAT parameter is valid if DESTINATION is set to ASYN. The default is to display a summary of each log message on a single line, omitting some fields.

The MAXQUEUESEVERITY parameter specifies the maximum message severity level where messages are to be queued, but not output, when QUEUEONLY is set to YES. If QUEUEONLY is set to YES, log messages with a severity level less than that specified by the MAXQUEUESEVERITY parameter are queued until the queue length reaches the limit set by the MESSAGES parameter, at which point all the messages are processed. Log messages with a priority greater than the value of MAXQUEUESEVERITY flushes (processes) queued messages. If the DESTINATION parameter is set to ASYN or the OUTPUT parameter is set to TEMPORARY, MAXQUEUESEVERITY may not be specified. The default for MAXQUEUESEVERITY is 7 (i.e. only messages with the maximum severity level are output immediately).

The MESSAGES parameter specifies the number of log messages that are to be added to the output definition queue before actually being processed. For a DESTINATION of MEMORY, the MESSAGES parameter specifies the maximum number of messages to be stored. When the limit is reached, older messages are purged to make room for new messages. For a DESTINATION of SYSLOG or ROUTER, the MESSAGES parameter specifies the maximum number of messages awaiting processing or acknowledgement. The MESSAGE parameter is not permitted if DESTINATION is set to ASYN. For SYSLOG and ROUTER, the MAXQUEUESEVERITY parameter can cause high-priority messages (and any other queued messages) to be output immediately. The default is 200 for a DESTINATION of MEMORY, and 20 for a DESTINATION of ROUTER or SYSLOG.

The PASSWORD parameter specifies the password to attach to log messages for authentication purposes when log messages are forwarded to another router via the Secure Router Logging Protocol (SRLP). If the remote router requires a password, this password must match. The PASSWORD parameter is valid when DESTINATION is set to ROUTER. The password is not transmitted over the network, but is used to compute an MD5 digest. The default is no password.

The ASYN parameter specifies an asynchronous port on the router where log messages are to be directed. The ASYN parameter is valid and required when DESTINATION is set to ASYN.

The QUEUEONLY parameter controls the output of log messages from the output definition queue. When QUEUEONLY is set to YES log messages are queued by the output definition and are not actually processed (forwarded, printed, displayed, etc.) until the queue is full. If the DESTINATION parameter is set to ASYN or the OUTPUT parameter is set to TEMPORARY, QUEUEONLY may not be specified. The default is NO.

The SECURE parameter specifies whether messages processed through this output definition are "secure" (the meaning of the word "secure" in this context is defined by the router manager). Certain log messages (e.g. information on password changes) are not be processed through insecure (SECURE=NO) output definitions to prevent interception by unauthorised parties. If the OUTPUT parameter is set to TEMPORARY, SECURE may not be specified. The default is YES when DESTINATION is set to ROUTER and PASSWORD is set to a valid password, or when DESTINATION is set to MEMORY. For all other cases, the default is NO.

The SERVER parameter specifies a destination IP address for log messages processed by this output definition. The SERVER parameter is required if the DESTINATION parameter is set to ROUTER or SYSLOG, and is not permitted for other values of DESTINATION. When the DESTINATION parameter is set to ROUTER, the SERVER parameter specifies the IP address of the router to transmit SRLP packets to via UDP port 5023. When the DESTINATION parameter is set to SYSLOG, the SERVER parameter specifies the IP address of the UNIX host running the syslog server. syslog messages are transmitted via UDP port 514.

The SYSLOGFORMAT parameter specifies whether the log messages sent to the syslog server contain the date, time, and system name. If the parameter is set to EXTENDED the date, time, and system name are included. If the parameter is set to NORMAL the date, time, and system name are not included. This parameter is valid if DESTINATION is SYSLOG. The default is NORMAL.

The TO parameter specifies the email address for log messages processed by output definitions with a DESTINATION set to EMAIL. If TO is specified, the DESTINATION parameter must be set to EMAIL.

The ZONE parameter specifies the time zone to use for time information in log messages, as the recognised name of a time zone (Table 33-7 on page 33-19), or the offset from UTC/GMT of the time zone where the times should be shown. The default is LOCAL.

The LOCAL parameter specifies a local interface to be used as the source for all LOG messages sent to a SYSLOG server. The local interface must already be configured and fall in the range 1-15. If either the parameter is not set or the option NONE is specified theswitch will select a source from the current available interfaces instead.

Table 33-7: Recognised time zone names .

Time Zone Name	Offset from GMT	Description
ASIA	+8:00	Asia
ACDT	+10:30	Australian Central Daylight Time
ACST	+9:30	Australian Central Standard Time
AEDT	+11:00	Australian Eastern Daylight Time
AEST	+10:00	Australian Eastern Standard Time
AWST	+8:00	Australian Western Standard Time
BST	+1:00	British Standard Time

Table 33-7: Recognised time zone names (continued).

Time Zone Name	Offset from GMT	Description
CHINA	+8:00	China
GMT	+0:00	Greenwich Mean Time
UK	+0:00	Greenwich Mean Time
HK	+8:00	Hong Kong
JST	+9:00	Japan Standard Time
MET	+1:00	Mid-European time
NZDT	+13:00	New Zealand Daylight Time
NZST	+12:00	New Zealand Standard Time
SING	+8:00	Singapore
TAIWAN	+8:00	Taiwan
UTC	+0:00	Universal Coordinated Time
CDT	-5:00	US Central Daylight Time
CST	-6:00	US Central Standard Time
EDT	-4:00	US Eastern Daylight Time
EST	-5:00	US Eastern Standard Time
MDT	-6:00	US Mountain Daylight Time
MST	-7:00	US Mountain Standard Time
PDT	-7:00	US Pacific Daylight Time
PST	-8:00	US Pacific Standard Time
DEFAULT	-	-
NONE	-	-

Examples

To create an output definition to forward log messages to another router with IP address 192.168.32.7, use the command:

```
cre log out=5 des=r server=192.168.32.7
```

To create an output definition to forward log messages to a local UNIX host with IP address 192.168.32.77, use the command:

```
cre log out=3 des=s server=192.168.32.77
```

To create an output definition to output log messages to asynchronous port 1 in summary (single-line) format, use the command:

```
cre log out=21 des=asyn asy=1
```

To create an output definition to transfer log messages to the email address netman@sellit.com, use the command:

```
cre log out=10 des=e to=“netman@sellit.com“
```

Related Commands

add log output
delete log output
destroy log output
disable log output
enable log output
set log output

delete log output

Syntax

```
DELete LOG OUTput={Temporary|output-id} FILter={ALL|
   filter-id}
```

where:

- *output-id* is the index number of an output definition from 1 to 20.
- *filter-id* is a filter entry number from 1 to *n*+1 where *n* is the number of filters currently defined for the output definition.

Description

This command deletes the specified filter entry or entries from the specified output definition.

The OUTPUT parameter specifies the number of the output definition containing the filter to be deleted. The output definition must already exist. If TEMPORARY is specified, the filter is deleted from the special TEMPORARY output definition.

The FILTER parameter specifies the entry number of the filter to be deleted. The filter entry must already exist. If ALL is specified, all filters are deleted from the specified output definition or definitions.

Examples

To delete the first filter entry from output definition 8, use the command:

```
del log out=8 fil=1
```

To delete all filter entries from output definition 10, use the command:

```
del log out=10 fil=all
```

Related Commands

add log output
show log output

delete log receive

Syntax

```
DELete LOG RECeive={ipadd|ANY}
```

where *ipadd* is an IP address in dotted decimal notation

Description

This command removes the log receive entry associated with the specified IP address. The RECEIVE parameter specifies the IP address of the entry to be deleted. If ANY is specified, the wildcard entry that matches all IP addresses is removed.

Examples

To remove the receive entry for network 192.168.30.0, use the command:

```
del log rec=192.168.30.0
```

Related Commands

add log receive
set log receive
show log receive

destroy log output

Syntax

```
DESTroy LOG OUTput={Temporary|output-id}
```

where *output-id* is the index number of an output definition from 1 to 20

Description

This command destroys the specified output definition.

The OUTPUT parameter specifies the index number of the output definition to be destroyed, or the special output definition TEMPORARY. An output definition must already exist with this index number.

Examples

To erase output definition 14, use the command:

```
dest log out=14
```

Related Commands

create log output
show log output

disable log

Syntax

```
DISable LOG
```

Description

This command disables the Logging facility, preventing the processing and reception of log messages.

Related Commands

disable log generation
disable log output
disable log reception
enable log

disable log generation

Syntax

```
DISable LOG GENeration
```

Description

This command disables the generation of log messages on the router. The reception and processing of log messages from other routers is not affected.

Related Commands

disable log
disable log output
disable log reception
enable log generation

disable log output

Syntax

```
DISable LOG OUTput[={Temporary|output-id}]
```

where *output-id* is the index number of an output definition, from 1 to 20

Description

This command disables the specified output definition. No log messages are processed by an output definition that is disabled.

The OUTPUT parameter specifies the index number of the output definition that is to be disabled. If TEMPORARY is specified, the special TEMPORARY output definition is disabled. The specified output definition must exist. If no value is specified, log message output definitions 1 to 20 are disabled and generates no output. The TEMPORARY output definition is not affected.

Examples

To disable output definition number 5, use the command:

```
dis log output=5
```

Related Commands

disable log
disable log generation
disable log reception
enable log output

disable log reception

Syntax

```
DISable LOG RECeption
```

Description

This command disables the reception of log messages from other routers via the Secure Router Logging Protocol (SRLP), the Net Manage Log Protocol and syslog. The generation and processing of local log messages is not affected by this command.

Related Commands

disable log
disable log generation
disable log output
enable log reception

enable log

Syntax

```
ENAble LOG
```

Description

This command enables the Logging facility. Log messages registered by router modules and received from other routers are now processed.

Related Commands

disable log
enable log generation
enable log output
enable log reception

enable log generation

Syntax

```
ENAble LOG GENeration
```

Description

This command enables the generation of log messages by modules in the router. It does not affect the reception of log messages from other routers over the network. Log message generation cannot occur unless the log module itself is enabled.

Related Commands

disable log generation
enable log
enable log output
enable log reception

enable log output

Syntax

```
ENAble LOG OUTput[={TEMPORARY|output-id}]
```

where *output-id* is the index number of an output definition from 1 to 20

Description

This command enables a specific output definition. An output definition must be enabled before log messages can be processed by the output definition. Output definitions are enabled by default when they are created.

The OUTPUT parameter specifies the index number of the output definition that is to be enabled. The specified output definition must exist. If TEMPORARY is specified, the special TEMPORARY output definition is enabled. If no value is specified, log message output definitions 1 to 20 are enabled and generates output. The TEMPORARY output definition is not affected.

Examples

To enable output definition number 14, use the command:

```
ena log out=14
```

Related Commands

disable log output
enable log
enable log generation
enable log reception

enable log reception

Syntax

```
ENAble LOG RECeption
```

Description

This command enables the reception of log messages from other routers via the Secure Router Logging Protocol (SRLP), the Net Manage Log Protocol and syslog. Received messages are processed in the same manner as messages generated on the router. Log messages cannot be received and processed unless the log module is enabled.

Related Commands

disable log reception
enable log
enable log generation
enable log output

flush log output

Syntax

```
FLUsh LOG OUTput[={Temporary|output-id}]
```

where *output-id* is the index number of an output definition from 1 to 20

Description

This command flushes the queue or queues for the specified output definition or definitions. Flushing an output definition's queue forces the entries in the queue to be processed by the output definition.

The OUTPUT parameter specifies the queue to be flushed. The output definition must already exist. If TEMPORARY is specified, the log messages stored in memory are purged (deleted). If any other output definition is specified, the log messages queued for processing by the specified output definition are processed according to the output definition. If a value is not specified, all queues are flushed.

Examples

To force all log messages queued for output definition 3 (that forwards messages to a syslog server) to be forwarded immediately, use the command:

```
flu log out=3
```

Related Commands

purge log

purge log

Syntax

```
PURge LOG[={Temporary|output-id}]
```

where *output-id* is the index number of an output definition from 1 to 20

Description This command clears the configuration information for the Logging facility and/or deletes log messages queued for processing.

If an output definition is not specified and the Logging facility is enabled when this command is executed, the configuration is restored to the default state. If the Logging facility is disabled, all configuration information is removed from both volatile and non-volatile storage. All log messages stored in memory are deleted by this command, as are any messages queued for transmission to a router via SRLP or to a syslog server.

If an output definition is specified, the log message queue for that definition is purged. All messages in it are discarded. Other output definitions are not affected, and the configuration of the Logging facility is not altered.

Related Commands disable log
enable log

set log output

Syntax

```
SET LOG OUTput={Temporary|output-id} [ASYn=port-number]
    [DEStination={Email|Memory|ASYN|Router|Syslog}]
    [FACILITY={DEFAULT|LOCAL1…LOCAL7}] [FORMat={Full|
   MSGOnly|SUMMARY}] [MAXQueueseverity=severity]
    [MESSages=message-count] [PASSword={password|NONE}]
    [QUEueonly={False|NO|OFF|ON|True|YES}] [SECure={False|
   NO|OFF|ON|True|YES}] [SERVER=ipadd]
    [SYslogformat=Extended|Normal] [TO=email-address]
    [ZOne={time-zone-name|utc-offset}] [LOCAL={NONE|1..15}]
```

```
SET LOG OUTput={Temporary|output-id} FILter=filter-id
    [ACtion={Process|Ignore}] [ALL] [DAte=[op]dd-mmm-yyyy]
    [DEVice=[op]device] [FIle=[op]filename] [MASK=ipadd]
    [MSGtext=[op]string] [MODule=[op]module-id]
    [ORIGin=ipadd] [REFerence=[op]string]
    [SEVerity=[op]severity] [SOUrceline=[op]line]
    [SUBType=[op]subtype-id] [TIme=[op]hh:mm:ss]
    [TYpe=[op]type-id] [LOCAL={NONE|1..15}]
```

where:

- *output-id* is the index number of an output definition from 1 to 20
- *severity* is a log message severity from 0 (low) to 7 (high).
- *message-count* is the maximum number of log messages that may be queued for processing.

- *password* is a character string 1 to 16 characters long. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.
- *port-number* is the number of an asynchronous port. Ports are numbered sequentially starting with port 0.
- *ipadd* is an IP address in dotted decimal notation.
- *email-address* is a character string 3 to 80 characters long. Valid characters are any printable character. If the string contains spaces, it must be in double quotes.
- *time-zone-name* is the name of a recognised time zone (Table 33-7 on page 33-19).
- *utc-offset* is a time offset from GMT/UTC from +23:59:59 to 23:59:59.
- *filter-id* is a filter entry number from 1 to *n*+1 where *n* is the number of filters currently defined for the output definition.
- *op* is a comparison operator (see Table 33-5 on page 33-9).
- *dd-mmm-yyyy* is a date, where *dd* is the day number (1–31), *mmm* is a three-letter abbreviation for the month (“Jan”, “Feb”, “Mar”,...) or the month number in 2 digit format (01-12), and *yyyy* is the year.
- *device* is a router device number.
- *filename* is a module source file name 1 to 12 characters long.
- *ipadd* is an IP address in dotted decimal notation.
- *module-id* is the name or number of a router module (see “Module Identifiers and Names” on page C-2 of Appendix C, Reference Tables for a complete list).
- *string* is a character string 1 to 15 characters long.
- *line* is a line number in a module source file from 1 to 65535.
- *subtype-id* is the name or number of a log message subtype (see “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list).
- *hh:mm:ss* is a time, where *hh* is the hour (0–23), *mm* is the minutes (0–59), and *ss* is the seconds (0–59).
- *type-id* is the name or number of a log message type (see “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list).
- *local* creates up to 15 local interfaces.

Description This command modifies the specified output definition or log message filter. The output definition specifies the processing to be performed on log messages that match one of the log message filters associated with the output definition. The specified output definition or log message filter must already exist.

The OUTPUT parameter specifies the index number of the output definition to be created, or the special output definitions TEMPORARY. If TEMPORARY is specified, the MAXQUEUESEVERITY, QUEUEONLY, and SECURE parameters should not be specified. An output definition must already exist with this index number.

The DESTINATION parameter specifies the type of processing to be performed and the destination of log messages processed by this output definition. The EMAIL option forwards log messages to the email address specified by the TO parameter. If DESTINATION is set to EMAIL, the parameter TO must also be specified. The MEMORY option stores log messages in RAM. The MEMORY option is valid when OUTPUT is set to TEMPORARY The ASYN option outputs log messages to an asynchronous port on the router. If DESTINATION is set to ASYN, the MAXQUEUESEVERITY, MESSAGES, and QUEUEONLY parameters should not be specified. The ROUTER option forwards log messages via the Secure Router Logging Protocol (SRLP) to another router. The SYSLOG option forwards log messages in syslog format to a syslog server.

The FACILITY parameter specifies whether to override the mapping between logging facility type and syslog facility identifiers. The DEFAULT option keeps the mapping between type and facility. If LOCAL1…LOCAL7 are specified then the syslog facility identifier will always be sent with the value specified. The FACILITY parameter is valid only if DESTINATION is set to SYSLOG. The default for FACILITY is DEFAULT

The FORMAT parameter specifies the format of log messages when converted into ASCII text for output to an asynchronous port. The FULL option displays the entire log message in multiple lines, with a blank line between messages. The SUMMARY option produces an abbreviated display. The MSGONLY option displays the text of the message. The FORMAT parameter is valid if DESTINATION is set to ASYN. The default is to display a summary of each log message on a single line, omitting some fields.

The MAXQUEUESEVERITY parameter specifies the maximum message severity level where messages are queued but not output when QUEUEONLY is set to YES. If QUEUEONLY is YES, log messages with a severity level less than that specified by the MAXQUEUESEVERITY parameter are queued until the queue reaches the limit set by the MESSAGES parameter, at which point all the messages are processed. Any log messages with a priority greater than the value of MAXQUEUESEVERITY flushes (processes) queued messages. If the DESTINATION parameter is set to ASYN or the OUTPUT parameter is set to TEMPORARY, MAXQUEUESEVERITY should not be specified. The default for MAXQUEUESEVERITY is 7 (meaning only messages with the maximum severity level are output immediately).

The MESSAGES parameter specifies the number of log messages to be added to the output definition queue before actually being processed. For a DESTINATION of MEMORY, the MESSAGES parameter specifies the maximum number of messages to be stored. When the limit is reached, older messages are purged to make room for new messages. For a DESTINATION of SYSLOG or ROUTER, the MESSAGES parameter specifies the maximum number of messages awaiting processing or acknowledgement. The MESSAGE parameter is not permitted if DESTINATION is set to ASYN. For SYSLOG and ROUTER, the MAXQUEUESEVERITY parameter can cause high-priority messages (and any other queued messages) to be output immediately. The default is 300 for a DESTINATION of MEMORY, and 20 for a DESTINATION of ROUTER or SYSLOG.

The PASSWORD parameter specifies the password to attach to log messages for authentication purposes when log messages are forwarded to another router via the Secure Router Logging Protocol (SRLP). If the remote router requires a password, this password must match. The PASSWORD parameter is valid when DESTINATION is set to ROUTER. The password is not transmitted over the network, but is used to compute an MD5 digest. The default is no password.

The ASYN parameter specifies an asynchronous port on the router where log messages are to be directed. The ASYN parameter is valid and required when DESTINATION is set to ASYN. If the DESTINATION parameter is set to ASYN or the OUTPUT parameter is TEMPORARY, QUEUEONLY may not be specified. The default is NO.

The QUEUEONLY parameter controls the output of log messages from the output definition queue. When QUEUEONLY is set to YES, log messages are queued by the output definition and are not actually processed (forwarded, printed, displayed, etc.) until the queue is full. The default is NO.

The SECURE parameter specifies whether messages processed through this output definition are to be “secure” (secure in this context is defined by the router manager). Certain log messages (e.g. information on password changes) are not processed through insecure (secure=no) output definitions to prevent interception by unauthorised parties. If the OUTPUT parameter is set to TEMPORARY, SECURE should not be specified. The default is YES when DESTINATION is set to ROUTER and PASSWORD is set to a valid password, or when DESTINATION is set to MEMORY. For all other cases, the default is NO.

The SERVER parameter specifies a destination IP address for log messages processed by this output definition. The SERVER parameter is required if the DESTINATION parameter is set to ROUTER or SYSLOG, and is not permitted for other values of DESTINATION. When DESTINATION is set to ROUTER, the SERVER parameter specifies the IP address of the router to transmit SRLP packets to via UDP port 5023. When the DESTINATION parameter is set to SYSLOG, the SERVER parameter specifies the IP address of the UNIX host running the syslog server. syslog messages are transmitted via UDP port 514.

The TO parameter specifies the email address for log messages processed by output definitions with a DESTINATION set to EMAIL. If TO is specified, the DESTINATION parameter must be set to EMAIL.

The ZONE parameter specifies the time zone to use for time information in log messages, as the recognised name of a time zone (Table 33-7 on page 33-19), or the offset from UTC/GMT of the time zone where the times should be shown. The default is LOCAL.

The FILTER parameter specifies the entry number of the filter within the output definition. If FILTER is specified, the filter is inserted into the filter list at the specified position. If FILTER is not specified, the filter is added to the end of the filter list for the output definition.

The ACTION parameter specifies the action to perform for log messages matching this filter. If PROCESS is specified, the log message is processed according to the output definition. If IGNORE is specified, the log message is ignored and not processed by this output definition. The default is PROCESS.

The ALL parameter matches all log entries. If ALL is specified, no other selection criteria may be specified for this filter. The default is to match log entries fitting the specified criteria.

The DATE parameter specifies the date to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any date.

The DEVICE parameter specifies the device number to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any device number.

The FILE parameter specifies the name of a source file to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any source file.

The MASK parameter specifies a subnet mask to use in association with the ORIGIN IP address parameter. The default is 255.255.255.255.

The MSGTEXT parameter specifies a string to match in the text of the log message. The first character of the value may be one of the comparison operators “<”, “>”, “!” or “%” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to”, “not equal to” or “contains substring” respectively (Table 33-5 on page 33-9). The default is to match any text.

The MODULE parameter specifies the router module to match in the log message, as either a decimal number or a recognised module name. See “Module Identifiers and Names” on page C-2 of Appendix C, Reference Tables for a complete list. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any module.

The ORIGIN parameter specifies the IP address to match against the originating IP address field of the log message. The MASK parameter can be used to specify a host, subnet or network. The default is to match any IP address in the origin IP address field.

The REFERENCE parameter specifies the reference to match in the log message. The first character of the value may be one of the comparison operators “<”, “>”, “!” or “%” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to”, “not equal to” or “contains substring” respectively (Table 33-5 on page 33-9). The default is to match any reference.

The SEVERITY parameter specifies the log message severity level to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any severity.

The SOURCELINE parameter specifies the line number in the source file where the log message was generated, to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any source line number.

The SUBTYPE parameter specifies the log message subtype to match, as either a decimal number or a recognised subtype name. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list. The first character of the value may be one of the comparison operators “<”,

">" or "!" to modify the comparison from "equals" (the default) to "less than or equal to", "greater than or equal to" or "not equal to" respectively (Table 33-5 on page 33-9). The default is to match any log message subtype.

The SYSLOGFORMAT parameter specifies whether the log messages sent to the syslog server contain the date, time, and system name. If the parameter is set to EXTENDED the date, time, and system name are included. If the parameter is set to NORMAL the date, time, and system name are not included. This parameter is valid if DESTINATION is SYSLOG. The default is NORMAL.

The TIME parameter specifies the time value to match in the log message. The first character of the value may be one of the comparison operators "<", ">" or "!" to modify the comparison from "equals" (the default) to "less than or equal to", "greater than or equal to" or "not equal to" respectively (Table 33-5 on page 33-9). The default is to match any time.

The TYPE parameter specifies the log message type to match, as either a decimal number or a recognised type name. See "Log Message Types and Subtypes" on page C-11 of Appendix C, Reference Tables for a complete list. The first character of the value may be one of the comparison operators "<", ">" or "!" to modify the comparison from "equals" (the default) to "less than or equal to", "greater than or equal to" or "not equal to" respectively (Table 33-5 on page 33-9). The default is to match any log message type.

The LOCAL parameter specifies a local interface to be used as the source for all LOG messages sent to a SYSLOG server. The local interface must already be configured and fall in the range 1-15. If either the parameter is not set or the option NONE is specified the switch will select a source from the current available interfaces instead.

Parameter values that contain spaces must be in double quotes. If one of the operators ("<", ">", "!", "%") is also present, the operator must be inside the quote marks. For example, `SET LOG OUTPUT=4 MSGTEXT="%PPP Inter"`.

Examples

To redirect log messages from output definition 2 to port 4 instead of port 1, use the command:

```
set log out=2 asy=4
```

To change the first filter entry in output definition 2 to ignore rather than process entries, use the command:

```
set log out=2 fil=1 ac=i
```

Related Commands

create log output
destroy log output
show log output

set log receive

Syntax

```
SET LOG RECeive={ipadd|ANY} [ALLOw={False|NO|OFF|ON|True|
   YES}] [MASK=ipadd] [PASSword={password|NONE}]
   [PROTocol={ALL|BOTh|NEW|OLD|SYSlog}]
```

where:

- *ipadd* is an IP address in dotted decimal notation.
- *password* is a character string 1 to 16 characters long. Valid characters are any printable character. If the string contains spaces it must be in double quotes.

Description

This command modifies the options for an entry in the log reception table. The log reception table specifies the routers (and networks/subnets if MASK is specified) from which log messages are accepted. When the log reception table is empty (the default), log messages are not accepted from any source. When comparing the source addresses of received log messages, the most specific entry is used. The order of entries in the log reception table is not significant.

The RECEIVE parameter specifies the IP address of the host, subnet or network from which log messages to be received. If ALL is specified, log messages are accepted from any IP address.

The ALLOW parameter specifies whether log messages are to be accepted from the specified IP address. If YES is specified, log messages are accepted from the IP address. If NO is specified, log messages are not accepted from the IP address. The default is YES.

The MASK parameter specifies a subnet mask to use in association with the RECEIVE parameter. The default is 255.255.255.255 if an IP address is specified for the RECEIVE parameter, or 0.0.0.0 if ALL is specified for the RECEIVE parameter.

The PASSWORD parameter specifies the password that must accompany log messages from the specified IP address, for authentication purposes when log messages are forwarded to another router via the Secure Router Logging Protocol (SRLP). If the PASSWORD option is present, the specified password must accompany log messages from the specified IP address.

The PROTOCOL parameter specifies the protocol to use for message reception from the specified IP address. If OLD is specified, the Logging facility accepts old Net Manage (UDP port 5024) packets. If NEW is specified, the Logging facility accepts the new Secure Router Logging Protocol (SRLP) packets. If SYSLOG is specified, the Logging facility accept syslog messages. The BOTH option is equivalent to specifying both OLD and NEW. The ALL option is equivalent to specifying OLD, NEW and SYSLOG. The PASSWORD parameter is not valid when TYPE is set to OLD or SYSLOG, as password authentication is not supported in these protocols.

Examples

To change the password for router 192.168.37.6, use the command:

```
set log rec=192.168.37.6 pass=newsecret
```

Related Commands

add log receive
delete log receive
show log receive

set log utcoffset

Syntax

```
SET LOG UTCoffset={time-zone-name|utc-offset}
```

where:

- *time-zone-name* is the name of a recognised time zone (Table 33-7 on page 33-19).
- *utc-offset* is a time offset from GMT/UTC from +23:59:59 to 23:59:59.

Description

This command tells the router the difference between local time (the time the router clock is set to) and UTC/GMT time. The router's clock is assumed to be set to local time, so the offset specified by this command is used to calculate UTC time.

The UTCOFFSET parameter specifies the time difference between the router's clock and UTC/GMT, as the recognised name of a time zone (Table 33-7 on page 33-19), or the time difference between the router's clock and UTC/GMT in hours, minutes and seconds. If the router clock is ahead of UTC, this offset is positive.

NTP and the Logging Facility share a common (system-wide) UTC offset. Changing the UTC offset with the SET LOG UTCOFFSET command also changes the value of the UTC offset used by NTP.

Although there are technical differences between the definitions of UTC and GMT time, the router treats them as if they were equivalent.

Examples

To set the UTC offset to +12 hours (appropriate for New Zealand Standard Time), use the command:

```
set log utc=12:00
```

To set the UTC offset to +1 hour (appropriate for British Summer Time), use the command:

```
set log stc=01:00:00
```

To set the UTC offset to zero (appropriate for Greenwich Mean Time and Universal Coordinated Time) use the command:

```
set log stc=0
```

Related Commands

show log status

show log

Syntax

```
SHow LOG[=output-id] [DAte=[op]dd-mmm-yyyy]
    [DEVice=[op]device] [FIle=[op]filename] [FULL]
    [MASK=ipadd] [MODule=[op]module-id] [MSGOnly]
    [MSGtext=[op]string] [ORIGin=ipadd]
    [REFerence=[op]string] [REVerse[=count]]
    [SEVerity=[op]severity] [SOUrceline=[op]line]
    [SUBType=[op]subtype-id] [TAil[=count]]
    [TIme=[op]hh:mm:ss] [TYpe=[op]type-id]
    [ZOne={time-zone-name|utc-offset}]
```

where:

- *output-id* is the index number of an output definition from 1 to 20.
- *op* is a comparison operator (Table 33-5 on page 33-9).
- *dd-mmm-yyyy* is a date where *dd* is the day of the month, *mmm* is an abbreviation for the month or the 2-digit number of the month, and *yyyy* is the year.
- *device* is a router device number.
- *filename* is a module source file name 1 to 12 characters long.
- *ipadd* is an IP address in dotted decimal notation.
- *module-id* is the name or number of a router module. See "Module Identifiers and Names" on page C-2 of Appendix C, Reference Tables for a complete list.
- *string* is a character string 1 to 15 characters long.
- *count* is a number from 1 to the number of log messages stored.
- *severity* is a log message severity from 0 (low) to 7 (high).
- *line* is a line number in a module source file from 1 to 65535.
- *subtype-id* is the name or number of a log message subtype. See "Log Message Types and Subtypes" on page C-11 of Appendix C, Reference Tables for a complete list.
- *hh:mm:ss* is a time where *hh* is the hour, *mm* is the minutes, and *ss* is the seconds.
- *type-id* is the name or number of a log message type. See "Log Message Types and Subtypes" on page C-11 of Appendix C, Reference Tables for a complete list)
- *time-zone-name* is the name of a recognised time zone (Table 33-7 on page 33-19).
- *utc-offset* is a time offset from GMT/UTC from +23:59:59 to 23:59:59.

Description

This command displays the log messages stored in memory (RAM) or in the log message queue for the specified output definition. If an output definition is not specified, the default is to display the log messages stored by the TEMPORARY output definition in RAM. The output can be filtered to display only entries that match a specific criteria.

The DATE parameter specifies the date value to match in the log message. The first character of the value may be one of the comparison operators "<", ">" or "!" to modify the comparison from "equals" (the default) to "less than or equal to", "greater than or equal to" or "not equal to" respectively (Table 33-5 on page 33-9). The default is to match any date.

The DEVICE parameter specifies the device number to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any device number.

The FILE parameter specifies the name of a source file to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any source file.

The FULL parameter specifies the format of the display. By default each log message is displayed in summary format on a single line, omitting some fields (Figure 33-4 on page 33-37, Table 33-7 on page 33-19). The FULL parameter displays the entire log message in multiple lines, with a blank line between messages (Figure 33-5 on page 33-38, Table 33-9 on page 33-38).

The MASK parameter specifies a subnet mask to use in association with the ORIGIN IP address parameter. The default is 255.255.255.255.

The MODULE parameter specifies the router module to match in the log message, as either a decimal number or a recognised module name. See “Module Identifiers and Names” on page C-2 of Appendix C, Reference Tables for a complete list. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any module.

The MSGONLY parameter specifies the format of the display. By default each log message is displayed in summary format on a single line, omitting some fields (Figure 33-4 on page 33-37, Table 33-7 on page 33-19). The MSGONLY parameter displays just the text of the log message.

The MSGTEXT parameter specifies a string to match in the text of the log message. The first character of the value may be one of the comparison operators “<”, “>”, “!” or “%” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to”, “not equal to” or “contains substring” respectively (Table 33-5 on page 33-9). The default is to match any text.

The ORIGIN parameter specifies the IP address to match against the originating IP address field of the log message. The MASK parameter can be used to specify a host, subnet or network. The default is to match any IP address in the origin IP address field.

The REFERENCE parameter specifies the reference to match in the log message. The first character of the value may be one of the comparison operators “<”, “>”, “!” or “%” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to”, “not equal to” or “contains substring” respectively (Table 33-5 on page 33-9). The default is to match any reference.

The REVERSE parameter specifies that log messages are displayed in reverse date (most recent first) order. If a value is specified, the output is limited to the specified number of log messages. The default, if no value is specified, is to display all log messages.

The SEVERITY parameter specifies the log message severity level to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any severity.

The SOURCELINE parameter specifies the line number in the source file where the log message was generated, to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any source line number.

The SUBTYPE parameter specifies the log message subtype to match, as either a decimal number or a recognised subtype name. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any log message subtype.

The TAIL parameter specifies that the most recent log messages be displayed. If a value is specified, the output is limited to the specified number of log messages. If no value is specified, the default is to display the last 20 log messages.

The TIME parameter specifies the time value to match in the log message. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any time.

The TYPE parameter specifies the log message type to match, as either a decimal number or a recognised type name. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list. The first character of the value may be one of the comparison operators “<”, “>” or “!” to modify the comparison from “equals” (the default) to “less than or equal to”, “greater than or equal to” or “not equal to” respectively (Table 33-5 on page 33-9). The default is to match any log message type.

The ZONE parameter specifies the time zone to use for time information in log messages, as the recognised name of a time zone (Table 33-7 on page 33-19), or the offset from UTC/GMT of the time zone where the times should be shown. The default is LOCAL.

Although there are technical differences between the definitions of UTC and GMT time, the router treats them as if they were equivalent.

Figure 33-4: Example output from the **show log** command

```
Date/Time   S Mod  Type  SType Message
-------------------------------------------------------------------------------
17 10:22:37 2 PPP  ATT   ATTCH ppp0: The IP module has attached
17 10:22:37 2 PPP  ATT   ATTCH ppp1: The IP module has attached
17 10:22:37 7 SYS  REST  NORM  Router startup, version 7.2-00, 21-Jun-1996,
                               4096k RAM
17 10:22:38 2 PPP  DLINK UP    ppp0: Primary link over syn0 has opened
17 10:22:38 3 PPP  VINT  UP    ppp0: Interface has come up and is able to send
                               and receive data
17 10:22:38 2 PPP  CIRC  UP    ppp0: IPCP has opened
17 10:31:28 2 CH   CMD   MGR   show log
17 10:36:43 2 CH   CMD   MGR   show log zone=-24:00
17 10:36:43 4 CH   MSG   ERROR Illegal time: 24:00
17 10:43:57 0 LOG              IP, telnet connection accepted from
                               202.36.163.20
17 10:44:00 3 USER USER  LON   manager login on TTY18
17 10:44:21 2 CH   CMD   MGR   show loge status
17 10:44:21 4 CH   MSG   ERROR Parameter “loge” not recognised
17 10:44:24 2 CH   CMD   MGR   show log status
17 10:44:50 2 CH   CMD   MGR   lo
17 10:44:50 3 USER USER  LOFF  manager logoff on TTY18
17 10:44:52 2 CH   CMD   MGR   show log
17 10:45:41 0 LOG              IP, telnet connection accepted from
                               202.36.163.20
17 10:45:54 3 USER USER  LON   manager login on TTY18
17 10:45:58 2 CH   CMD   MGR   show log
-------------------------------------------------------------------------------
```

Table 33-8: Parameters in the output of the **show log** command

Parameter	Meaning
Date/Time	Date and time the log message was generated. The date is displayed as just the day of the month (1–31).
S	Severity of the log message.
Mod	Name of the module that generated the log message. See “Module Identifiers and Names” on page C-2 of Appendix C, Reference Tables for a complete list.
Type	Message type. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list.
SType	The message subtype. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list.
Message	Contents of the Message field in the log message. For log messages of type IPFILT/PASS, the format of the message text is “*filter-number*/*entry-number* Pass|Fail *src-ipadd*>*dest-ipadd protocol src-port*>*dest-port packet-size*:*data-size*”. For log messages of type IPFILT/DUMP, the message text contains the first 32 octets of the packet.

Figure 33-5: Example output from the **show log full** command

```
Date/Time    Mod  Type  SType Dev   Origin           MSGID Source File/Line
-------------------------------------------------------------------------------
15:38:47  7  SYS  REST  NORM  00000 Local            00001 shostart.c:179
03-JUN-1997  00400040         LOCTIME
             Router startup, version 7.4-00, 12-May-1997, Clock Log  : 15:38:33
             on 03-Jun-1997
15:38:48  3  PPP  VINT  UP    00000 Local            00030 pppinter.c:1655
03-JUN-1997  ppp0             LOCTIME
             ppp0: Interface has come up and is able to send and receive data
15:40:47  5  PPP  DLINK ERROR 00000 Local            00032 ppplqm.c:476
03-JUN-1997  ppp0             LOCTIME
             ppp0: An LQR failure has occured on primary link over syn0
15:40:47  5  PPP  DLINK DOWN  00000 Local            00033 ppplcp.c:1017
03-JUN-1997  ppp0             LOCTIME
             ppp0: Primary link over syn0 has closed
15:40:47  5  PPP  VINT  DOWN  00000 Local            00034 pppinter.c:1792
03-JUN-1997  ppp0             LOCTIME
             ppp0: Interface has gone down and is unable to send or receive
             data
15:40:50  3  PPP  VINT  UP    00000 Local            00037 pppinter.c:1655
03-JUN-1997  ppp0             LOCTIME
             ppp0: Interface has come up and is able to send and receive data
10:04:06  4  CH   MSG   ERROR 00016 Local            00058 utlmsg.c:930
04-JUN-1997  3031012           LOCTIME
             Parameter “tot” not recognised
10:04:36  4  CH   MSG   ERROR 00016 Local            00061 utlmsg.c:930
04-JUN-1997  3031012           LOCTIME
             Parameter “tot” not recognised
10:04:42  4  CH   MSG   ERROR 00016 Local            00063 utlmsg.c:930
04-JUN-1997  3031012           LOCTIME
             Parameter “totta” not recognised
10:04:45  4  CH   MSG   ERROR 00016 Local            00065 utlmsg.c:930
04-JUN-1997  3031259           LOCTIME
             Invalid parameter combination. The correct command should be:
             SHOW FL[ASH] {P[H
10:05:47  4  CH   MSG   ERROR 00016 Local            00070 utlmsg.c:930
04-JUN-1997  3005012           LOCTIME
             Parameter “log” not recognised
-------------------------------------------------------------------------------
```

Table 33-9: Parameters in the output of the **show log full** command

Parameter	Meaning
Date/Time	Date and time the log message was generated, including the UTC offset.
S	Severity of the log message.
Mod	Name of the module that generated the log message. See “Module Identifiers and Names” on page C-2 of Appendix C, Reference Tables for a complete list.
Type	Message type. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list.
SType	Message subtype. See “Log Message Types and Subtypes” on page C-11 of Appendix C, Reference Tables for a complete list.
Dev	Device (such as asynchronous port or TTY session) that triggered the log message.

Table 33-9: Parameters in the output of the **show log full** command (continued)

Parameter	Meaning
Origin	Origin of the log message; either Local or the IP address of the host that generated the log message via either SRLP or syslog.
MSGID	Message ID number.
Source File/Line	File name and line number of the module source file where the log message originated.
Ref	Contents of the Reference field in the log message.
Flags	Contents of the Flags field in the log message; one or more of LOCTIME, SECURE, or CMDOUT.
Message	Contents of the Message field in the log message.

Examples To display all recent log messages, use the command:

```
sh log
```

To display log messages for critical events, use the command:

```
sh log sev=>5
```

To display log messages for recent user activity, use the command:

```
sh log ty=user
```

The PPP link to the head office is not working. To display log messages relating to link activity, use the command:

```
sh log ty=link
```

A terminal connected to port 0 and logged in with Manager privilege was left unattended. To see if someone has interfered with the router, use the command:

```
sh log ty=cmd dev=port0
```

There is a problem with one of the modems. To see who has been affected, use the command:

```
sh log ty=user subt=login dev=port4
```

Related Commands **purge log**
show log status

show log counter

Syntax `SHow LOG COUnter`

Description This command displays diagnostic counters for the Logging facility (Figure 33-6, Table 33-10 on page 33-40).

Figure 33-6: Example output from the **show log counter** command

```
Log Counters

  Idle loop passes .................................283
  Transmit passes .................................. 78

  Messages Generated ...............................136

  Messages Received (Syslog) ....................... 0
  Messages Received (Old protocol) ................. 0
  Messages Received (New protocol, SRLP) ........... 0

  Messages Rejected (Syslog) ....................... 0
  Messages Rejected (Old protocol) ................. 0
  Messages Rejected (New protocol, SRLP) ........... 0
  Messages Rejected (Module disabled) .............. 0
  Messages Rejected (Generation disabled) .......... 0
  Messages Rejected (Reception disabled) ........... 0
  Messages Rejected (Bad parameters) ............... 0

  Messages with invalid time ....................... 0

  Messages Transmitted (Syslog) .................... 0
  Messages Transmitted (New protocol, SRLP) ........72

  Messages Retransmitted (New protocol, SRLP) ...... 0
  ACKs Sent (New protocol) ......................... 0
  ACKs Sent (Old protocol) ......................... 0
  ACKs Received (New protocol, SRLP) ...............72

  Message transmissions failed (New protocol, SRLP) 0


  Messages processed via OD  1 ................78  (Router)
  Messages processed via OD TE ................21  (Memory)
```

Table 33-10: Parameters in the output of the **show log counter** command

Parameter	Meaning
Idle loop passes	Number of times the log message handling process has been activated from the router idle loop.
Transmit passes	Number of times the log message transmission process has been activated.
Messages Generated	Number of log messages generated on this router.
Messages Received (Syslog)	Number of log messages received via syslog by this router.
Messages Received (Old protocol)	Number of log messages received via the Net Manage logging protocol by this router.

Table 33-10: Parameters in the output of the **show log counter** command (continued)

Parameter	**Meaning**
Messages Received (New protocol...	Number of log messages received via the Secure Router Log Protocol (SRLP) by this router.
Messages Rejected (Syslog)	Number of log messages received via syslog by this router that were rejected.
Messages Rejected (Old protocol)	Number of log messages received via the Net Manage logging protocol by this router that were rejected.
Messages Rejected (New protocol...	Number of log messages received via the Secure Router Log Protocol (SRLP) by this router that were rejected.
Messages Rejected (Module...	Number of log messages received by this router that were rejected because the Logging facility is disabled.
Messages Rejected (Generation...	Number of log messages from software modules on this router that were rejected because log message generation is disabled.
Messages Rejected (Reception...	Number of log messages received by this router that were rejected because log message reception is disabled.
Messages Rejected (Bad...	Number of log messages received by this router that were rejected because they contained invalid parameter values.
Messages with invalid time	The number of messages with an invalid timestamp.
Messages Transmitted (Syslog)	The number of log messages transmitted via syslog by this router.
Messages Transmitted (New...	Number of log messages transmitted via the Secure Router Log Protocol (SRLP) by this router.
Messages Retransmitted...	Number of log messages retransmitted via the Secure Router Log Protocol (SRLP) by this router.
ACKs Sent (New protocol)	Number of acknowledgements transmitted for log messages received via the Secure Router Log Protocol (SRLP) by this router.
ACKs Sent (Old protocol)	Number of acknowledgements transmitted for log messages received via the Net Manage logging protocol by this router.
ACKs Received (New protocol...	Number of acknowledgements received for log messages transmitted via the Secure Router Log Protocol (SRLP) by this router.
Message transmissions failed...	Number of retransmissions of log messages via the Secure Router Log Protocol (SRLP) that have failed.
Messages processed via OD *n* (*type*)	Number of messages processed by the specified output definition.

Examples To display diagnostic counters, use the command:

```
sh log cou
```

Related Commands

show log
show log output
show log status
show log queue

show log output

Syntax

```
SHow LOG OUTput[={Temporary|output-id}]
   [{FILter=filter-id|FULL}]
```

where:

- *output-id* is the index number of an output definition from 1 to 20.
- *filter-id* is a filter entry number from 1 to *n*+1 where *n* is the number of filters currently defined for the output definition.

Description

This command displays all output definitions or a specific one. If a value is not specified for the OUTPUT parameter, and neither the FILTER or FULL parameters are specified, summary information of all output definitions is displayed (Figure 33-7 on page 33-42, Table 33-11 on page 33-42).

The OUTPUT parameter specifies the index number of the output definition to be displayed, or a special output definition TEMPORARY. If a value is not specified, the default is to display all output definitions.

If FULL is specified, detailed information about each output definition including details of all message filters is displayed (Figure 33-8 on page 33-43, Table 33-12 on page 33-44). The FILTER and FULL parameters are mutually exclusive – only one may be specified in any one command.

The FILTER parameter produces the same output as the FULL parameter, except that detailed filter information is displayed for the specified filter. The FILTER and FULL parameters are mutually exclusive – only one may be specified in any one command.

Figure 33-7: Example output from the **show log output** command

```
OD# Type      Port Server          Msg  Zone Fmt                          ESQMP
-------------------------------------------------------------------------------
01  Syslog         202.36.163.20        ----                              YNN--
02  Router         202.36.163.40        ----                              YNN--
03  Email                          0020 ----     netman@sellit.com        YNN--
TE  Memory                         0200 ----                              YY---
--------------------------------------------------------------------------------
```

Table 33-11: Parameters in the output of the **show log output** command

Parameter	Meaning
OD#	Index number of the output definition.
Type	Destination for log messages processed by this output definition; either Memory, Port, Router, or Syslog.
Port	Asynchronous port number on the router where log messages are to be directed by this output definition when the Type field is Port.
Server	IP address of the router or host where log messages are to be directed by this output definition when the Type field is Router or Syslog.
Msg	Maximum number of messages that may be queued for processing by this output definition.
Zone	How the date and time are processed and displayed by this output definition; either Local, GMT, UTC, an offset from UTC from -23:59:59 to +23:59:59, or a dash if not set.

Table 33-11: Parameters in the output of the **show log output** command (continued)

Parameter	**Meaning**
Fmt	Whether the format of messages processed by this output definition is full or summary. If the Type is Syslog, then FMT is either normal or extended.
Email Address	Email address where log messages are to be directed by this output definition when the Type field is Email.
ESQMP	For **enabled**, **secure**, and **queueonly**, the value is either yes, no, or not applicable (dash). For **maxqueueseverity**, the value is a severity level from 0 to 7. For **password** the value is a dash (password not set) or an asterisk (password set).

Figure 33-8: Example output from the **show log output full** command

```
Output Definition ........... 1
Enabled ..................... Yes
Type ........................ Syslog
IP Address (Server) ......... 202.36.163.20
Local Interface ............. local3
Time Zone ................... -
Secure ...................... No
Queue Only .................. No


Output Definition ........... 2
Enabled ..................... Yes
Type ........................ Router
IP Address (Server) ......... 202.36.163.40
Time Zone ................... -
Secure ...................... No
Queue Only .................. No
Syslog Format ............... NORMAL
Facility .................... LOCAL2

Filter 1:
    MODULE != IPX
    SEVERITY < 7
    ---> Process
Filter 2:
    ALL

Output Definition ........... Permanent
Enabled ..................... Yes
Max Messages ................ 20
Time Zone ................... -
Secure ...................... Yes

Filter 1:
    ALL

Output Definition ........... Temporary
Enabled ..................... Yes
Type ........................ Memory
Max Messages ................ 200
Time Zone ................... -
Secure ...................... Yes

Filter 1:
    ALL
```

Table 33-12: Parameters in the output of the **show log output full** command

Parameter	Meaning
Output Definition	Index number of the output definition, TE (TEMPORARY).
Enabled	Whether the output definition is enabled and processes log messages matching any of the associated filters.
Type	Destination for log messages processed by this output definition; either Memory, Port, Router, or Syslog.
IP Address (Server)	IP address of the router or host where log messages are to be directed by this output definition when the Type field is Router or Syslog.
Local Interface	The interface used as the source in log messages destined for the UNIX SYSLOG server.
Zone	How the date and time are processed and displayed by this output definition. It is displayed as an offset from UTC from -23:59:59 to +23:59:59 followed by the abbreviation for the time zone (if defined).
Secure	Whether log messages processed by this output definition are secure.
Queue Only	Whether log messages matching one of the filters associated with this output definition are to be queued for processing.
Syslog Format	Whether the format of log messages sent to a syslog server are normal or extended.
Facility	Whether syslog messages will have the facility field overridden or not, when the Type field is "Syslog"
Max Messages	Maximum number of messages that may be queued for processing by this output definition.
Filter #	Index of an associated message filter, the filter attributes to match, and the action to perform. The filter attributes may be ALL (matches all messages) or more conditions. The action is either Process or Ignore.
Port	Asynchronous port number on the router where log messages are to be directed by this output definition when the Type field is Port.
Format	Whether the format of messages processed by this output definition is full or summary.
Email Address	Email address where log messages are to be directed by this output definition when the Type field is Email.
Password	Password attached to log messages for authentication purposes if messages are to forwarded to another router via SRLP by this output definition.
Max Queue Severity	Severity level from 0 (low) to 7 (high) that log messages are queued and not processed immediately by this output definition.

Examples To display all output definitions, use the command:

```
sh log out
```

To display only output definition number 7, use the command:

```
sh log out=7
```

To display the filter entries for output definition 7, use the command:

```
sh log out=7 full
```

To display the second filter entry for output definition 7, use the command:

```
sh log out=7 fil=2
```

Related Commands

- add log output
- create log output
- delete log output
- destroy log output
- set log output
- show log status

show log queue

Syntax `SHow LOG QUEue[=output-id]`

where *output-id* is the index number of an output definition from 1 to 20

Description This command displays information about messages in log message queues and the messages that have been transmitted via SRLP but are awaiting acknowledgement.

If an output definition is specified, entries are displayed for it. If one is not specified, all entries in the log message queues are displayed (Figure 33-9 on page 33-45, Table 33-13 on page 33-45).

Figure 33-9: Example output from the **show log queue** command

```
Queue  RAM Messages    NVS Messages    Type
------------------------------------------------------
TE     0002/0200       0000/0000       Memory
------------------------------------------------------
```

Table 33-13: Parameters in the output of the **show log queue** command

Parameter	Meaning
Queue	Output definition with which this queue is associated; "TE" (TEMPORARY) or an output definition identifier from 1 to 20.
RAM Messages	Number of messages currently stored in RAM and the maximum number of messages that may be stored in RAM.
NVS Messages	Not applicable.
Type	Destination for log messages in this queue; either Memory, Port, Router, or Syslog.
OD#	Index number of an output definition.
Message ID	Message ID number.
Last Attempt	Time expressed as seconds since midnight that the last attempt was made to retransmit the message.

Table 33-13: Parameters in the output of the **show log queue** command (continued)

Parameter	Meaning
Attempts	Number of attempts made to retransmit the message.
Delay	Seconds between each retransmission.

Examples To display the entries in the log message queue for output definition 3, use the command:

```
sh log que=3
```

To display information about all log message queues, use the command:

```
sh log que
```

Related Commands

show log
show log output
show log status

show log receive

Syntax `SHow LOG RECeive[=`*`ipadd`*`] [MASK=`*`ipadd`*`]`

where *ipadd* is an IP address in dotted decimal notation

Description This command displays entries from the log reception table (Figure 33-10 on page 33-46, Table 33-14 on page 33-47).

If an IP address is supplied, the entry for the address is displayed. If a network mask is also supplied, entries within the subnet defined by the IP address and network mask are displayed.

The RECEIVE parameter specifies the IP address to display. If an IP address is not specified, all entries in the log reception table are displayed.

The MASK parameter specifies a subnet mask to use in association with the RECEIVE parameter. The default is 255.255.255.255 if an IP address is specified for the RECEIVE parameter, or 0.0.0.0 if ALL is specified for the RECEIVE parameter. If MASK is specified, all entries falling in the range of IP addresses specified by the combination of RECEIVE and MASK are displayed.

Figure 33-10: Example output from the **show log receive** command

```
Type   IP/Network Addr  Netmask        Protocol  Password
-----------------------------------------------------------
Allow  192.168.0.0      255.255.0.0    BOTH       -
Allow  192.168.2.0      255.255.255.0  NEW       ******
-----------------------------------------------------------
```

Table 33-14: Parameters in the output of the **show log receive** command

Parameter	Meaning	
Allow	Whether messages are to be received from the IP address.	
IP/Network Addr	IP address of a host, subnet, or network where log messages are to be received.	
Netmask	Subnet mask to use in association with the IP address.	
Protocol	Type of message to be received from the IP address:	
	Old	Old Net Manage messages
	New	New format messages
	Both	Equivalent to Old + New
	Syslog	System log
	Any	Equivalent to Old + New + Syslog
Password	Password that must accompany messages from the IP address, if any.	

Examples To display the entry for router 192.168.1.11, use the command:

```
sh log rec=192.168.1.11
```

To display all entries, use the command:

```
sh log rec
```

To display all entries for routers in subnet 192.168.40.0, use the command:

```
sh log rec=192.168.40.0 mask=255.255.255.0
```

Related Commands

add log receive
delete log receive
set log receive
show log status

show log status

Syntax `SHow LOG STAtus`

Description This command displays configuration information for the Logging facility (Figure 33-11 on page 33-47, Table 33-15 on page 33-48).

Figure 33-11: Example output from the **show log status** command

```
Log System Status
--------------------------------------------------------

Log Module Status ..................... Enabled
Log Message Generation ................ Enabled
Log Message Reception (via network) ... Enabled
Log Message Output .................... Enabled
Local Time Offset (from UTC) .......... 12:00:00 (NZST)
Next Message ID ....................... 12
Number of Output Definitions .......... 2
```

Table 33-15: Parameters in the output of the **show log status** command

Parameter	Meaning
Log Module Status	Whether the Logging facility is enabled or disabled.
Log Message Generation	Whether log messages are to be generated by modules in this router.
Log Message Reception	Whether log messages are to be received from the network by this router.
Log Message Output	Whether output definitions are enabled and are to generate output.
Local Time Offset (from UTC)	Offset of local time from UTC time from +23:59:59 to -23:59:59.
Next Message ID	Unique message identifier to be assigned to the next log message the Logging facility processes.
Number of Output Definitions	Number of output definitions currently defined.

Examples To display the current status of the Logging facility, use the command:

```
sh log sta
```

Related Commands

disable log
disable log generation
disable log output
disable log reception
enable log
enable log generation
enable log output
enable log reception
show log