

## Chapter 59

# Logging Facility

Introduction .....	59-2
Format of Log Messages .....	59-3
Secure Router Log Protocol (SRLP) .....	59-4
Net Manage Message Protocol .....	59-4
Processing Log Messages .....	59-4
Output Definitions and Message Filters .....	59-4
Destinations .....	59-6
Configuring Output Definitions .....	59-8
Configuring Message Filters .....	59-9
Configuration Example .....	59-10
Command Reference .....	59-13
add log output .....	59-14
add log receive .....	59-17
create log output .....	59-19
delete log output .....	59-23
delete log receive .....	59-23
destroy log output .....	59-24
disable log .....	59-24
disable log generation .....	59-24
disable log output .....	59-25
disable log reception .....	59-25
enable log .....	59-26
enable log generation .....	59-26
enable log output .....	59-27
enable log reception .....	59-27
flush log output .....	59-28
purge log .....	59-28
set log output .....	59-29
set log receive .....	59-35
set log utcoffset .....	59-36
show log .....	59-37
show log counter .....	59-43
show log output .....	59-45
show log queue .....	59-50
show log receive .....	59-51
show log status .....	59-53

## 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 or NVS memory, 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. All log messages are spooled in NVS, when available, until processed to ensure that no information is lost during a power failure or a system restart.

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 or NVS.
- 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 NVS, 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. 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. The following table describes data fields that the log message contains.

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.
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 <a href="#">“Module Identifiers and Names” on page B-2 of Appendix B, Reference Tables</a> 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 <a href="#">“Log Message Types and Subtypes” on page B-11 of Appendix B, Reference Tables</a> 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 <a href="#">“Log Message Types and Subtypes” on page B-11 of Appendix B, Reference Tables</a> 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.

The following table describes severity levels of log messages.

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.
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 59-37](#)), 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 or NVS, 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 NVS or RAM, the queue represents the actual log messages stored in NVS or RAM. The [show log command on page 59-37](#) 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 you can create two or more output definitions with the same destination (for example, 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 destination. This flexibility could potentially cause problems for output definitions that store messages in RAM or NVS.

If multiple queues are stored in RAM or NVS, which one is displayed by the **show log** command? The conflict is solved by two special output definitions: **temporary** and **permanent**. 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. The **permanent** output definition accepts a destination of NVS. Messages processed by this output definition can be displayed by the **show log=permanent** command. The **permanent** output definition is available on routers with NVS.

## Destinations

### Storage in RAM or NVS Memory

Log messages may be stored in the router's RAM or NVS 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 one time can be configured. When the number of messages reaches the maximum, the oldest message is deleted to make room for a new one.

Log messages stored in NVS **are** retained over a power failure or router restart. The only limit on the number of messages that can be stored in NVS is the amount of NVS available. The maximum number of messages that may be stored in NVS at one time can be configured. When the number of messages reaches the maximum, the oldest message is deleted to make room for a new one.

Some router models do not have NVS memory. The **permanent** output definition is not available on these models and 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.

### 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 59-37](#) 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 59-1](#)) and the log message severity is translated into a syslog "level" ([Table 59-2 on page 59-7](#)). 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 59-1: 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		Licensing 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 59-2: 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 59-1).

Figure 59-1: 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 59-2](#)), 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 59-2: 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 4-32 of Chapter 4, Configuring and Monitoring the System.

## Configuring Output Definitions

Logging is enabled by default and the two special output definitions: **temporary** and **permanent**.

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.

The **permanent** output definition contains a log message filter that matches all log messages of severity 3 or greater, and stores up to 20 messages in NVS. The **permanent** output definition is available on routers with NVS.

To create an output definition, use the **create log output command** on page 59-19.

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 59-25. To enable them, use the **enable log output command** on page 59-27.

To modify an existing output definition, use the **set log output command** on page 59-29.

To delete an output definition, use the **destroy log output command** on page 59-24.

To display the currently configured output definitions, use the **show log output command** on page 59-45.



## 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 59-14](#).

To modify an existing log message filter, use the [set log output command on page 59-29](#).

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 59-3](#)).

Table 59-3: 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 or equal to 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 59-19](#).

To display log message filters definitions that are currently configured, use the [show log output command on page 59-45](#).

## Configuration Example

The following example shows how to configure the Logging facility in a wide area network environment (Figure 59-3, Table 59-4 on page 59-10). 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 and NVS memory. 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 59-3: Example configuration for a basic Logging facility.

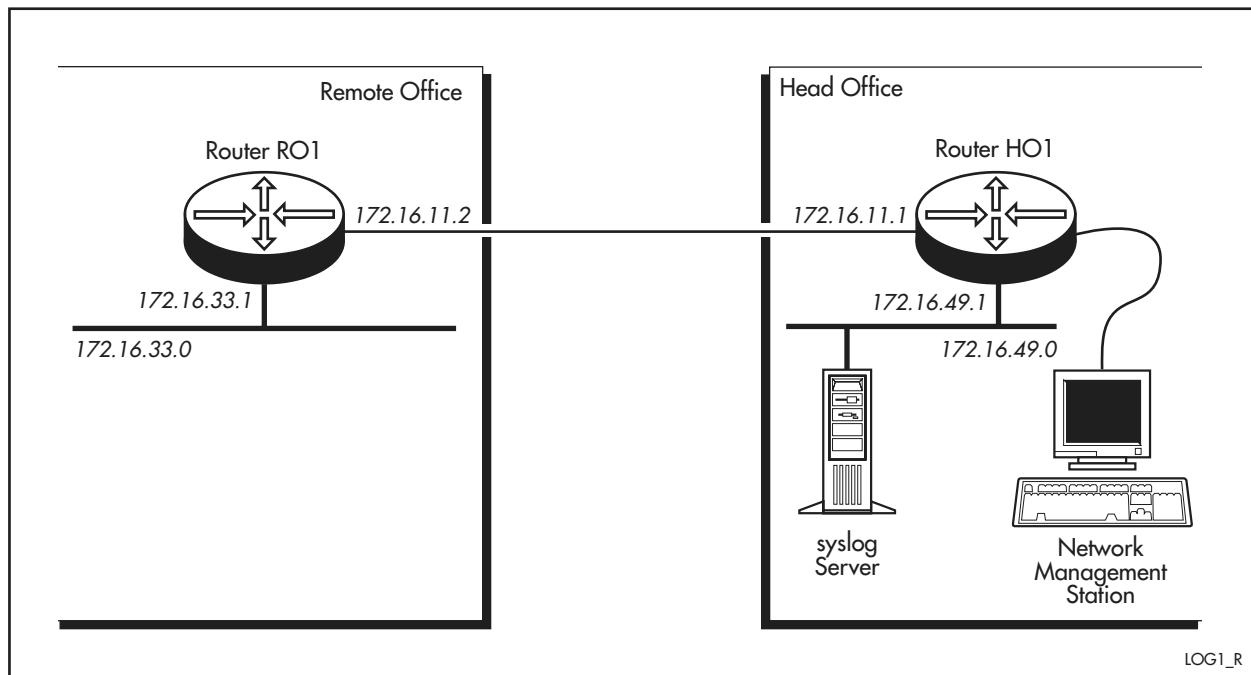


Table 59-4: Example configuration parameters for a basic Logging facility

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 log 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** and **permanent** output definitions are automatically defined by the system to match all log messages of severity 3 or greater and to store the log messages in RAM or NVS respectively. Since this is exactly what is required in this example, there is no need to specify these output definitions any further, except to limit the number of messages stored in NVS. The **permanent** output definition is available on routers with NVS.

By default, the only limit on the number of log messages stored in NVS memory is the amount of NVS memory available. The Logging facility uses all available NVS memory. It is a good idea to limit the number of messages stored in NVS. As a guide, 1 Kbyte of NVS memory holds approximately 10 log messages:

```
set log output=permanent messages=100
```

Some router models do not have NVS memory. The **permanent** output definition is not available on these models and 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 21, 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 lxiv of [About this Software Reference](#) 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|Permanent|*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 59-3 on page 59-9](#)).
- *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 B-2 of Appendix B, Reference Tables for a complete list.
- *string* is a 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 B-11 of Appendix B, 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 B-11 of Appendix B, 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.

This command requires a user with security officer privilege when the router is in security mode.

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. If **permanent** is specified, the filter is added to the special **permanent** output definition. The **permanent** output definition is available on routers with NVS.

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 59-3 on page 59-9](#)). 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 59-3 on page 59-9](#)). 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 59-3 on page 59-9](#)). 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 59-3 on page 59-9](#)). 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 B-2 of Appendix B, 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 59-3 on page 59-9](#)). 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 B-11 of Appendix B, 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 B-11 of Appendix B, 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 59-3 on page 59-9). 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 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|Permanent|output-id}  
 DEStination={Email|Memory|Nvs|ASYN|Router|Syslog}  
 [ASYN=port-number] [FACILITY={DEFAULT|LOCAL1..LOCAL7}]  
 [FORMat={Full|MSGOnly|Summary}] [LOCal={NONE|1..15}]  
 [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}]`

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 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 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.
- *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 59-14](#).

The **output** parameter specifies the index number of the output definition to be created, or one of the special output definitions **temporary** or **permanent**. The **permanent** output definition is available on routers with NVS. 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 NVS option stores log messages in NVS memory. The NVS option is valid when **output** is set to **permanent**. 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 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 **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. If **none** is specified, the router selects a source from the current available interfaces instead. The default is **none**.

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** are processed immediately and flush (process) queued messages. If the **destination** parameter is set to **asyn** or **syslog**, or the **output** parameter is set to **temporary**, **maxqueueseverity** cannot 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 **nvs** or **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 **messages** 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 **nvs**, **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 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** cannot 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** or **nvs**. 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, or the offset from UTC/GMT of the time zone where the times should be shown. This parameter is not valid when **destination** is **memory** or **nvs**. The default is **local**. Time zones are in the following table.

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
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

Time Zone Name	Offset from GMT	Description
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 | Permanent | *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. If **permanent** is specified, the filter is deleted from the special **permanent** output definition. The **permanent** output definition is available on routers with NVS.

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|Permanent|*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 one of the special output definitions **temporary** or **permanent**. The **permanent** 4output definition is available on routers with NVS. 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 | Permanent | 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** or **permanent** is specified, the special **temporary** or **permanent** output definition is disabled. The specified output definition must exist. The **permanent** output definition is available on routers with NVS. If no value is specified, log message output definitions 1 to 20 are disabled and generate no output. The **temporary** and **permanent** output definitions are 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 | Permanent | 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** or **permanent** is specified, the special **temporary** or **permanent** output definition is enabled. The **permanent** output definition is available on routers with NVS. If no value is specified, log message output definitions 1 to 20 are enabled and generates output. The **temporary** and **permanent** output definitions are 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 | Permanent | *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. The **permanent** output definition is available on routers with NVS. 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 | Permanent | *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. The **permanent** output definition is available on routers with NVS. All log messages stored in memory and NVS 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|Permanent|*output-id*}  
 [ASyn=*port-number*] [DEStination={Email|Memory|Nvs|ASYN|Router|Syslog}] [FACILITY={DEFAULT|LOCAL1..LOCAL7}]  
 [FORMat={Full|MSGOnly|SUMMARY}] [LOCal={NONE|1..15}]  
 [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*}]

SET LOG OUTput={Temporary|Permanent|*output-id*}  
 FILTER=*filter-id* [ACTion={Process|Ignore}] [ALL]  
 [Date=[*op*] *dd-mmm-yyyy*] [DEVice=[*op*] *device*]  
 [File=[*op*] *filename*] [LOCal={NONE|1..15}] [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*]

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 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.
- *local* creates up to 15 local interfaces.
- *ipadd* is an IP address in dotted decimal notation.
- *email-address* is a 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 (see table in [create log output](#) command).
- *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 59-3 on page 59-9](#)).
- *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 B-2 of Appendix B, Reference Tables for a complete list).
- *string* is a 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 B-11 of Appendix B, 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 B-11 of Appendix B, Reference Tables for a complete list).

**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.

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 msgtest="%PPP Inter".

The **output** parameter specifies the index number of the output definition to be created, or one of the special output definitions **temporary** or **permanent**. The **permanent** output definition is available on routers with NVS. 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 **nvs** option stores log messages in NVS memory. The **nvs** option is valid when **output** is set to **permanent**. 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 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** are processed immediately and flush (process) queued messages. If the **destination** parameter is set to **asyn** or **syslog**, 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 **nvs** or **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 **messages** 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** to **nvs**, **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** cannot 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 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** cannot be specified. 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** or **nvs**. 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 over 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 over 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, or the offset from UTC/GMT of the time zone where the times should be shown. This parameter is not valid when **destination** is **memory** or **nvs**. 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 59-3 on page 59-9). The default is to match any source file.

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. If **none** is specified the router will select a source from the current available interfaces instead. The default is **none**.

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 59-3 on page 59-9). 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 B-2 of Appendix B, 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 B-11 of Appendix B, 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 B-11 of Appendix B, 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 59-3 on page 59-9). The default is to match any log message type.

**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 modify the number of log messages stored in permanent storage (NVS), use the command:

```
set log out=p mess=50
```

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 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 accepts syslog messages. The **both** option is equivalent to specifying **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** because 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 (see table in [create log output](#) command)
- *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 to which the router's clock is set) 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 a recognised time zone, 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.

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 utc=01:00:00
```

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

```
set log utc=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 59-3 on page 59-9](#)).
- *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 B-2 of [Appendix B, Reference Tables](#) for a complete list.
- *string* is a 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 B-11 of [Appendix B, 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 B-11 of [Appendix B, Reference Tables](#) for a complete list).
- *time-zone-name* is the name of a recognised time zone (see table in [create log output](#) command).
- *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 NVS) 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 59-3 on page 59-9](#)). 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 59-4 on page 59-40, Table 59-5 on page 59-40). The **full** parameter displays the entire log message in multiple lines, with a blank line between messages (Figure 59-5 on page 59-41, Table 59-6 on page 59-41).

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 B-2 of Appendix B, 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 59-3 on page 59-9). 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 59-4 on page 59-40, Table 59-5 on page 59-40). 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 B-11 of Appendix B, 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 59-3 on page 59-9). 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 59-3 on page 59-9). 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 B-11 of Appendix B, 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 59-3 on page 59-9). 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, 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 59-4: 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 59-5: Parameters in 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 <a href="#">“Module Identifiers and Names” on page B-2 of Appendix B, Reference Tables</a> for a complete list.
Type	Message type. See <a href="#">“Log Message Types and Subtypes” on page B-11 of Appendix B, Reference Tables</a> for a complete list.
SType	The message subtype. See <a href="#">“Log Message Types and Subtypes” on page B-11 of Appendix B, Reference Tables</a> 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 <i>“filter-number/entry-number Pass Fail src-ipadd&gt;dest-ipadd protocol src-port&gt;dest-port packet-size:data-size”</i> . For log messages of type IPFILT/DUMP, the message text contains the first 32 octets of the packet.



Figure 59-5: Example output from the **show log full** command

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

Table 59-6: Parameters in 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 <a href="#">"Module Identifiers and Names" on page B-2 of Appendix B, Reference Tables</a> for a complete list.
Type	Message type. See <a href="#">"Log Message Types and Subtypes" on page B-11 of Appendix B, Reference Tables</a> for a complete list.
SType	Message subtype. See <a href="#">"Log Message Types and Subtypes" on page B-11 of Appendix B, Reference Tables</a> for a complete list.
Dev	Device (such as asynchronous port or TTY session) that triggered the log message.

Table 59-6: Parameters in output of the **show log full** command (Continued)

Parameter	Meaning
Origin	Whether the origin of the log message is the local address or 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 59-6, Table 59-7).

Figure 59-6: 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 PE .....21 (NVS)
Messages processed via OD TE .....21 (Memory)

```

Table 59-7: Parameters in 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 this router received via syslog.

Table 59-7: Parameters in output of the **show log counter** command (Continued)

Parameter	Meaning
Messages Received (Old protocol)	Number of log messages this router received via the Net Manage logging protocol.
Messages Received (New protocol...)	Number of log messages this router received via the Secure Router Log Protocol (SRLP).
Messages Rejected (Syslog)	Number of log messages this router received via syslog that were rejected.
Messages Rejected (Old protocol)	Number of log messages this router received via the Net Manage logging protocol that were rejected.
Messages Rejected (New protocol...)	Number of log messages this router received via the Secure Router Log Protocol (SRLP) that were rejected.
Messages Rejected (Module...)	Number of log messages this router received that were rejected because the Logging facility was 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 this router received that were rejected because log message reception was disabled.
Messages Rejected (Bad...)	Number of log messages this router received that were rejected because they had invalid parameter values.
Messages with invalid time	Number of messages with an invalid timestamp.
Messages Transmitted (Syslog)	Number of log messages this router transmitted via syslog.
Messages Transmitted (New...)	Number of log messages this router transmitted via the Secure Router Log Protocol (SRLP).
Messages Retransmitted...	Number of log messages this router retransmitted via the Secure Router Log Protocol (SRLP).
ACKs Sent (New protocol)	Number of acknowledgements this router transmitted for log messages received via the Secure Router Log Protocol (SRLP).
ACKs Sent (Old protocol)	Number of acknowledgements this router transmitted for log messages received via the Net Manage logging protocol.
ACKs Received (New protocol...)	Number of acknowledgements this router received for log messages transmitted via the Secure Router Log Protocol (SRLP).
Message transmissions failed...	Number of retransmissions of log messages via the Secure Router Log Protocol (SRLP) that have failed.
Messages processed via OD <i>n</i> (type)	Number of messages processed by a specific 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 | Permanent | 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 59-7, Table 59-8 on page 59-46).

The **output** parameter specifies the index number of the output definition to be displayed, or one of the special output definitions **temporary** or **permanent**. If a value is not specified, the default is to display all output definitions. The **permanent** output definition is available on routers with NVS.

If **full** is specified, detailed information about each output definition is displayed, including details about all message filters (Figure 59-8 on page 59-47, Table 59-9 on page 59-47). The **filter** and **full** parameters are mutually exclusive—only one may be specified in a 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 a command.

Figure 59-7: 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--
PE	NVS			0020	----		YY---
TE	Memory			0200	----		YY---

Table 59-8: Parameters in output of the **show log output** command

Parameter	Meaning
OD#	Index number of the output definition.
Type	Whether the destination for log messages processed by this output definition is memory, NVS, 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 <b>port</b> .
Server	IP address of the router or host where log messages are to be directed by this output definition when the type field is <b>router</b> or <b>syslog</b> .
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.
Fmt	Whether the format of messages processed by this output definition is full or summary. If the type is <b>syslog</b> , then FMT is normal or extended.
Email Address	Email address where log messages are to be directed by this output definition when the type field is <b>email</b> .
ESQMP	For <b>enabled</b> , <b>secure</b> , and <b>queueonly</b> , the value is either yes, no, or not applicable (dash). For <b>maxqueueseverity</b> , the value is a severity level from 0 to 7. For <b>password</b> , the value is a dash (password not set) or an asterisk (password set).

Figure 59-8: 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
Type ..... NVS
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 59-9: Parameters in output of the **show log output full** command

Parameter	Meaning
Output Definition	Index number of the output definition, Temporary or Permanent.
Enabled	Whether the output definition is enabled and processes log messages matching any of the associated filters.
Type	Whether the destination for log messages processed by this output definition is memory, NVS, port, router, or syslog.

Table 59-9: Parameters in output of the **show log output full** command (Continued)

Parameter	Meaning
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 <b>router</b> or <b>syslog</b> .
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 <b>syslog</b> .
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 <b>all</b> (matches all messages) or more conditions. The action is either <b>process</b> or <b>ignore</b> .
Port	Asynchronous port number on the router where log messages are to be directed by this output definition when the type field is <b>port</b> .
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 <b>email</b> .
Password	Password attached to log messages for authentication purposes if messages are to be 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 filt=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

**Description** This command displays information about messages in log message queues and the messages that have been transmitted via SRLP but are awaiting acknowledgement (Figure 59-9, Table 59-10).

Figure 59-9: Example output from the **show log queue** command

Queue	RAM Messages	NVS Messages	Type	
-----				
01	0000/0100	0007/0010	Router	
PE	0000/0020	0020/0020	NVS	
TE	0021/0200	0000/0000	Memory	
-----				
Outstanding SRLP Messages (Sent but not acknowledged)				
OD#	Message ID	Last Attempt	Attempts	Delay
-----				
01	73	0	0	0
01	74	0	0	0
01	75	0	0	0
01	76	0	0	0
01	77	0	0	0
01	78	0	0	0
01	79	0	0	0

Table 59-10: Parameters in output of the **show log queue** command

Parameter	Meaning
Queue	Whether the output definition with which this queue is associated is PE (permanent) or TE (temporary), or an 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	Number of messages currently stored in NVS and the maximum number of messages that may be stored in NVS.
Type	Whether the destination for log messages in this queue is memory, NVS, 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.
Attempts	Number of attempts made to retransmit the message.
Delay	Seconds between each retransmission.

**Examples** 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 59-10, Table 59-11).

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 59-10: 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 59-11: Parameters in 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 59-11, Table 59-12).

Figure 59-11: 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 59-12: Parameters in output of the **show log status** command

Parameter	Meaning
Log Module Status	Whether the Logging facility is enabled.
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](#)

