



APPENDIX **B**

Understanding Syslog Formats

Devices are expected to comply with the following rules while sending Syslogs:

- Device should include PRI as recommended by RFC 3164
- Device could optionally send Timestamp information in RFC recommended format in the header. The RFC recommendation does not include the TIMEZONE information. Hence, it is assumed that the device sends the local time and that the device and Server are in the same time zone.
- Device could optionally send Hostname information in the header.
- To support devices that are in different time zones than the server, IOS allows configuring the devices to send the Time Information along with TZ, optionally, in the message part of the Syslog packet.

Such timestamps should be prefixed with some separator character (like * or :), so the Syslog daemons (such as unix syslogd) do not treat them as header information. This could cause unix syslogd to misinterpret the time information, because they ignore the TZ part of the Timestamp.

Considering the above, devices should send Syslogs in one of the following formats:

Format A

```
<187> [timestamp in RFC prescribed format] [device dns name | ip address] [Dummy Value/Counter : ] [ {:|*} mmm dd hh:mm:ss TimeZone ] %FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: description
```

Format B

```
<187> [timestamp in RFC prescribed format] [device dns name | ip address] [Dummy Value/Counter : ] [ {:|*} yyyy mmm dd hh:mm:ss TimeZone <-|+> hh:mm] %FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: description
```

Examples of good syslog messages: [as sent by the device]

```
<187>%PIX-4-106023 description
```

```
<187>Mar 23 10:21:03 %PIX-4-106023 description
```

```
<187>*Mar 23 12:12:12 PDT %PIX-4-106023 description
```

```
<187>Mar 23 10:21:03 *Mar 23 12:12:12 PDT %PIX-4-106023 description
```

```
<187>Mar 23 10:21:03 *2003 Mar 23 12:12:12 PDT -8:00 %PIX-4-106023 description
```

```
<187>Mar 23 10:21:03 93: *2003 Mar 23 12:12:12 PDT -8:00 %PIX-4-106023 description
```

The device ensures that the device IP address or DNS name if defined is maintained in the message header as the source IP address or source DNS name irrespective of the interface out of which the Syslog message is sent.

The Syslog message is sent on the network to the NMS (Network management station) using UDP. The UDP socket sent to, will be the UDP socket for syslog (514).

The payload of the message will be preceded by the logging facility code enclosed in angle braces (<>) that the receiving Syslog daemon uses for routing the message. Logging facility at the logging system is mapped to a log file on the system. The logging facility codes map as follows:

- (5<<3) = Syslog
- (23-16<<3) = Local 0 to Local 7

The combination FACILITY-[SUBFACILITY]-SEVERITY-MNEMONIC must be UNIQUE for a given message, so that Syslog Analyzer can provide non-trivial syslog support.

See the section, “[Enabling and Tracking Syslogs Using Syslog Analyzer and Collector](#)” for details.