Syslog Client

bintec-Dm 753-I

Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents. 1

Chapter 1 Introduction 2

1.1 Introducing the Syslog Protocol 2

1.2 Syslog Messages 2

1.2.1 [PRI] Field 2

1.2.2 [HEADER] Field 3

1.2.3 [MSG] Field 3

1.3 Syslog protocol in the Router 4

Chapter 2 Configuration 5

2.1 Configuring the Syslog client facility 5

2.1.1 ? (HELP) 5

2.1.2 BUFFER-SIZE 6

2.1.3 ENABLE. 6

2.1.4 FACILITY 6

2.1.5 HOSTNAME-PRIORITY 7

2.1.6 INITIAL-DELAY 7

2.1.7 LIST 8

2.1.8 NO 8

2.1.9 SERVER 11

2.1.10 SEVERITY. 13

2.1.11 SOURCE-ADDRESS 14

2.1.12 TIMESTAMP 14

2.1.13 EXIT 15

2.2 Notification of events as syslog messages 15

Chapter 3 Monitoring. 18

3.1 Monitoring the Syslog client facility 18

3.1.1 ? (HELP) 18

3.1.2 LIST 18

3.1.3 EXIT 19

Chapter 4 Example. 20

4.1 Syslog client configuration example 20

I Related Documents

bintec-DM 704-I Configuration and Monitoring

Chapter 1 Introduction

1.1 Introducing the Syslog Protocol

The Syslog Protocol is described under RFC 3164 (*The BSD syslog protocol*). It provides a transport mechanism for devices to send event notification messages across IP networks to message collectors, also known as Syslog servers. This protocol is characterized by its simplicity:

- No acknowledgement of message receipt is required.
- No stringent coordination is required between the client or transmitter and the server or receiver. In fact, the transmission of Syslog messages may be started without a server being configured or physically present.

Syslog uses the UDP protocol (*User Datagram Protocol*) as transport mechanism and has port 514 assigned. Even though the source port can be different, it should also be 514 to show the message comes from Syslog.

In the Syslog architecture or operating model, three roles can be distinguished: client or transmitter, server or receiver, and relay. The relay receives messages from the client and retransmits them either to a server or to another relay. In some cases, the device executing the function of relay has to previously modify the messages. In a device acting as a collector (or server), any packet destined to the UDP 514 port will be treated as a Syslog message. However, it is recommended to adhere to an established format. If a relay receives a packet that matches this format, it must retransmit it without making any changes. However, if the packet does not adhere to the defined format, the relay must modify it before re-transmitting it.

In each specific operation system or application, the programmer or developer must decide at what point, or under what circumstances, an event notification message is considered relevant and should be generated. These messages can be classified under one of several categories. This classification is generally based on the facility that generated the event and the severity of the message. This way, the task of message filtering is simplified and the most important and time-sensitive messages are dealt with first.

1.2 Syslog Messages

A Syslog message can be considered as being made up of three parts:

1.2.1 [PRI] Field

The PRI field must consist of three, four, or five characters, beginning with '<' and ending with '>', with a number known as the priority value between the two. This represents both the facility and the severity, and is made up of one, two or three decimal integers. The code set used is a seven-bit ASCII in an eight-bit field (i.e. ASCII codes as defined in the *USA Standard Code for Information Interchange*): the '<' character is defined as the Augmented Backus-Naur Form (ABNF) %d60 and the '>' character corresponds to the ADNF %d62 value. The digits indicating the priority take ABNF values between %d48 ('0') and %d57 ('9').

Facilities and severities are numerically coded with decimal values. Some of the operating system demons and processes have been assigned a facility value. Those that have not had a value explicitly assigned can use one of the facility values reserved for local use (*local use x*), or the *user-level* (1) facility. The following table shows facilities whose values have been specifically assigned, together with their corresponding numerical codes:

Numerical Code	*Facility*
0	*kernel messages*
1	*user-level messages*
2	*mail system*
3	*system daemons*
4	*security/authorization messages*
5	*messages internally generated by Syslog*
6	*line printer subsystem*
7	*network news subsystem*
8	*UUCP subsystem*
9	*clock daemon*
10	*security/authorization messages*
11	*FTP daemon*
12	*NTP subsystem*

13	*log audit*
14	*log alert*
15	*clock daemon*
16	*local use 0 (local0)*
17	*local use 1 (local1)*
18	*local use 2 (local2)*
19	*local use 3 (local3)*
20	*local use 4 (local4)*
21	*local use 5 (local5)*
22	*local use 6 (local6)*
23	*local use 7 (local7)*

As for the severity level indicator, the decimal values associated to each level are as follows:

Numerical Code	*Severity*
0	*Emergency* : system is unusable
1	*Alert* : action must be taken immediately
2	*Critical* : critical conditions
3	*Error* : error conditions
4	*Warning* : warning conditions
5	*Notice* : normal but significant condition
6	*Informational* : informational messages
7	*Debug* : debug-level messages

The priority value must be introduced into the corresponding message field (preceded by ‘<’ and ended with ‘>’) and is calculated by first multiplying the facility numerical value by 8 and then adding the integral numerical value associated to the severity. The first digit following the ‘<’ character will never be a ‘0’, unless the priority value is 0.

1.2.2 [HEADER] Field

This contains a *timestamp* and an indication of the *hostname* or IP address of the device that sends the message, each one in a field and in this order, both ending with a blank space character (ABNF%d32).

- **The [TIMESTAMP]** field contains the local time in “Mmm dd hh:mm:ss” format (without quotation marks). “Mmm” indicates the first three characters for each month (in English), with the first character in uppercase (i.e. the possible values are: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec), “dd” is the day of the month (if the day of the month is less than 10, then a space must be inserted before the number), and “hh:mm:ss” is the local time in 24-hour format.
- The **[HOSTNAME]** field contains the *hostname* or the IP address, the *hostname* (NOT the domain name) being the preferred value. This field cannot contain any blank spaces. If the device does not have a *hostname*, use its IP address. If a device has multiple IP addresses, the IP address from which the message is transmitted will be usually selected (although an address configured independently from the interface used to send the message can also be used). The format for IP addresses is decimal notation with periods.

1.2.3 [MSG] Field

The [MSG] part includes additional information on the process that generates the message. There is no set ending for this part, which generally contains visible characters in seven bit ASCII code. I.e. ABNF BCHAR values (those between %d33 and %d126) and spaces (SP value %d32). Other code sets may be used, depending on the type of receiver that acquires the messages (always limiting the set of permitted characters to visible characters and the blank space).

Two fields can be seen within the [MSG] part:

- **The [TAG] field** : name of the program or process that generated the message. This is a string of ABNF alphanumeric characters that must not exceed 32 characters. Any non-alphanumeric character will terminate this string and indicate the beginning of the next field.
- **The [CONTENT] field**: details of the message. As already mentioned, the first character in this field will be the first non-alphanumeric character found in the [MSG] part. The first character is usually ‘[‘, ‘:’ or a blank space.

1.3 Syslog protocol in the Router

When the **Syslog client** functionality is implemented in the **router**, the device will be capable of sending notifications to the configured server(s) in Syslog message format. The selection of the situations or operating points where a Syslog message must be generated is common to the rest of event notification methods. This means that, in addition to being able to enable events for viewing purposes (such as traces and the transmission of SNMP traps), you can also enable transmission in Syslog message format.

Whenever it has been determined that a notification must be created (i.e. there is an associated event), first check that this specific event can be sent as a Syslog message and then verify that this function has been enabled (default is disabled). If so, the severity configured through the corresponding parameter (default 6: *Informational*) is compared with that associated to the event. If it is equal or inferior to the established level (compare the numerical codes), the process to send the Syslog message with the appropriate information to the server will be started. The correspondence between the event *logging-level* (type of event or filtering level) and its severity is as follows:

Numerical Code	*Severity*	*Logging-Level*
0	*Emergency*	UI-ERROR
1	*Alert*	CI-ERROR
2	*Critical*	UE-ERROR
3	*Error*	CE-ERROR
4	*Warning*	U-INFO
5	*Notice*	U-TRACE
6	*Informational*	C-INFO
7	*Debug*	C-TRACE, P-TRACE

The packet sent to each configured Syslog server is built taking the following data into account:

(1) The destination port is UDP 514.

(2) The source port is also UDP 514.

(3) The destination address will be that of the Syslog server configured by the user (either through an IP address or through a *hostname*).

(4) The source address will be that specified through the corresponding configuration parameter. By default, the packet output interface address is used.

(5) The [PRI] field is determined based on the severity associated to the specific event (according to that corresponding with its *logging-level*) and the value configured for the facility. By default this is 23 (*local7*).

(6) The *timestamp* corresponds to the time in the format configured through the corresponding configuration parameter. Its value is obtained from the BIOS or from an NTP server, adding or subtracting the offset and the daylight saving time (if they have been configured and where applicable).

There are two possible formats:

- Local time in “Mmm dd hh:mm:ss” format (without quotation marks). “Mmm” indicates the first three characters for the month of the year (in English), with the first character in uppercase (i.e. the possible values are: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec), “dd” is the day of the month (if the day of the month is less than 10, then a space must be inserted before the number), and “hh:mm:ss” is the local time in 24-hour format. This format is described under RFC 3164.
- UTC time in “yyyy-mm-ddThh:mm:ss.msZ” format (without quotation marks). “yyyy” indicates the year, “mm” is the month, “dd” is the day of the month and “hh:mm:ss.ms” is the time in hours, minutes, seconds and milliseconds. This format is described under RFC 5424.

(7) In the [HOSTNAME] field, the device *hostname* is entered if it has been configured and *hostname-priority* has not been configured. If there is no *hostname*, or if the *hostname-priority* command configures the IP as priority and you have used the *source-address* command to configure a source IP address, the IP configured will be sent. If the device has no *hostname* configured, or if the *hostname-priority* command sets IP as priority in the *hostname* field and no IP *source-address* is configured, the device's *global-address* will be sent.

(8) Finally, in the [MSG] field, you include the event constituent text, starting with the subsystem this pertains to and which generates it. Said subsystem constitutes the [TAG] field.

Chapter 2 Configuration

2.1 Configuring the Syslog client facility

This section describes the steps required to configure the Syslog client.

In order to access the Syslog client configuration environment, enter one of the following commands:

```
*process 4
Config>feature syslog

-- SYSLOG client configuration --
SYSLOG config>
```

Or:

```
*CONFIG
Config>feature syslog

-- SYSLOG client configuration --
SYSLOG config>
```

Once you have accessed the Syslog client configuration menu, the following commands will be available:

Command	Function
? (HELP)	Lists the available commands or their options.
BUFFER-SIZE	Establishes the size of the buffer where the messages waiting to be sent are stored.
ENABLE	Enables the Syslog client functionality.
FACILITY	Configures the facility associated with the Syslog messages. This parameter, together with the event severity originating the message, is used to calculate the priority.
HOSTNAME-PRIORITY	Configures which value will be sent in the hostname field for Syslog messages.
INITIAL-DELAY	Initial delay prior to sending the messages periodically.
LIST	Displays the Syslog client configuration.
NO	Deletes a previously configured Syslog server or restores the default values of the configuration parameters.
SERVER	Adds a Syslog server as destination for the messages transmitted by the client.
SEVERITY	Establishes the severity level.
SOURCE-ADDRESS	Source IP address in the outgoing Syslog messages.
TIMESTAMP	Timestamp options for syslog messages.
EXIT	Exits the Syslog client configuration menu.

2.1.1 ? (HELP)

Lists the valid commands at the level where the router is programmed. You can also use this command after a specific command to list the available options.

Syntax:

```
SYSLOG config>?
```

Example:

```
SYSLOG config>?
  buffer-size        Set size of buffer used to store messages before sending
  enable             Enable syslog client
  facility           Facility parameter for syslog messages
  hostname-priority Configure the priority of the hostname
  initial-delay      Set initial delay before starting periodic sending
  list               List syslog client configuration parameters
  no                 Negate a command or set its defaults
  server            Configure a syslog server
  severity          Set severity level
  source-address    Set source ip address of syslog messages
  timestamp         Timestamp options for syslog messages
  exit              Exit syslog configuration menu
SYSLOG config>
```

2.1.2 BUFFER-SIZE

Establishes the size of the buffer where messages waiting to be sent are stored. Any situation related to an associated event where the Syslog message notification format is complied with results in it being saved in a buffer to be periodically extracted and sent to the configured servers. When selecting the buffer size, please bear in mind that more memory is used the higher the value (making buffer saturation and a loss of events more likely). The range of values allowed is <2..10000>.

Syntax:

```
SYSLOG config>buffer-size ?
  <2..10000>    Value in the specified range
SYSLOG config>
```

Example:

```
SYSLOG config>buffer-size 60
SYSLOG config>
```

Note

We recommend that the default value for this parameter is not modified (256 messages) except where absolutely necessary.

Command history:

Release	Modification
11.00.07	This command was modified as of version 11.00.07. Its default value has been incremented from 50 to 256 messages and its value range has incremented from 2..100 to 2..10000.
11.01.02	This command was modified as of version 11.01.02. Its default value has been incremented from 50 to 256 messages and its value range has incremented from 2..100 to 2..10000.

2.1.3 ENABLE

Enables the Syslog client functionality. This is disabled by default.

Syntax:

```
SYSLOG config>enable ?
  <cr>
SYSLOG config>
```

Example:

```
SYSLOG config>enable
SYSLOG config>
```

2.1.4 FACILITY

Configures the facility associated to the Syslog messages. This parameter, together with the event severity that originates the message, is used to calculate the priority. Some of the demons and operating system processes have a standard facility value assigned. Those that do not have an explicitly assigned value can use the facility values reserved for local use. With regard to the **router**, the permitted values for the facility (which are configurable) are:

Numerical Code	*Facility*
16	*local use 0 (local0)*
17	*local use 1 (local1)*
18	*local use 2 (local2)*

19	*local use 3 (local3)*
20	*local use 4 (local4)*
21	*local use 5 (local5)*
22	*local use 6 (local6)*
23	*local use 7 (local7)*

The facility value is 23 by default (*local7*).

Syntax:

```
SYSLOG config>facility ?
  local0     Local use 0 (local0)
  local1     Local use 1 (local1)
  local2     Local use 2 (local2)
  local3     Local use 3 (local3)
  local4     Local use 4 (local4)
  local5     Local use 5 (local5)
  local6     Local use 6 (local6)
  local7     Local use 7 (local7)
SYSLOG config>
```

Example:

```
SYSLOG config>facility local0
SYSLOG config>
```

2.1.5 HOSTNAME-PRIORITY

Configures which value will be sent in the hostname field for Syslog messages. Normally, the default value is the hostname set in the router. However, if the *hostname-priority* command is configured, the option selected will substitute the default value.

If *hostname-priority* is configured, an IP address will be used (regardless of whether there is a *hostname* or not). This IP address will be the one configured as *source-address* or, if none has been configured, the device's *global-address*. If, however, *hostname-priority* is not configured, the *hostname* (or, failing this, the configured *source-address*) will be used. If no *source-address* has been configured either, the device's *global-address* will be sent.

Syntax:

```
SYSLOG config>hostname-priority ?
  ip   IP address always will be set in the hostname field
SYSLOG config>
```

Example:

```
SYSLOG config>hostname-priority ip
SYSLOG config>
```

Command history:

Release	Modification
11.01.06	The "hostname-priority" command was introduced as of version 11.01.06

2.1.6 INITIAL-DELAY

Sets an initial delay before starting a periodic search in the buffer for Syslog messages waiting to be transmitted, in order to process the transmission to the configured servers. Default is one second before the first reading of the message buffer begins. Through this parameter, you can specify a waiting period between 1 and 4294967295 seconds. You obviously need to be extra careful when selecting the value for this parameter. A high value may mean the loss of events over a long period of time.

Syntax:

```
SYSLOG config>initial-delay ?
  <1..4294967295>    Value in the specified range
SYSLOG config>
```

Example:

```
SYSLOG config>initial-delay 25
SYSLOG config>
```

Note

A certain delay must be configured before transmitting notification messages, particularly if the events generated can be sent in this format within the first few seconds of device startup. Otherwise, we recommend that the default value is not modified (1 second).

2.1.7 LIST

Allows you to view the Syslog client facility configuration information.

Syntax:

```
SYSLOG config>list ?
  <cr>
SYSLOG config>
```

Example:

```
SYSLOG config$list

Syslog client global configuration:

Syslog client status: ENABLED
Facility: 23 (Local7)
Severity: 6 (Informational)
Source IP address: 1.2.3.4

Syslog servers configured:

IP address       Domain name                      Vrf              Source-Address
---------------  ------------------------------  ---------------  ---------------
192.168.214.152                                                   1.2.3.4
192.168.214.152                                  test             10.20.30.40
0.0.0.0          test.domain.com                 test2

Storage and sending parameters:

Buffer size: 50 messages
Initial delay: 1 sec.
Timestamp format: Local time 'Mmm dd hh:mm:ss'
Hostname priority: hostname
```

Command history:

Release	Modification
11.00.07	This command was modified as of version 11.00.07. The value of the new configuration command "timestamp" is displayed.
11.01.02	This command was modified as of version 11.01.02. The value of the new configuration command "timestamp" is displayed.
11.01.06	The "hostname-priority" option was introduced as of version 11.01.06.

2.1.8 NO

Deletes a previously configured server or reestablishes the default values for some of the Syslog client configuration parameters.

Syntax:

```
SYSLOG config>no ?
  buffer-size       Set size of buffer used to store messages before sending
  enable            Enable syslog client
  facility          Facility parameter for syslog messages
  hostname-priority Configure the priority of the hostname
  initial-delay     Set initial delay before starting periodic sending
  server            Configure a syslog server
  severity          Set severity level
  source-address    Set source ip address of syslog messages
  timestamp         Timestamp options for syslog messages
SYSLOG config>
```

2.1.8.1 no buffer-size

Configures the buffer size used to store the Syslog messages waiting to be sent to its default value: 256 messages.

Syntax:

```
SYSLOG config>no buffer-size ?
  <cr>
SYSLOG config>
```

Example:

```
SYSLOG config>no buffer-size
SYSLOG config>
```

2.1.8.2 no enable

Disables the Syslog client functionality so that events are not reported through this protocol. This facility is disabled by default.

Syntax:

```
SYSLOG config>no enable ?
  <cr>
SYSLOG config>
```

Example:

```
SYSLOG config>no enable
SYSLOG config>
```

2.1.8.3 no hostname-priority

Restores the default value for the hostname field in Syslog messages (i.e. hostname of the router, whenever it exists).

Syntax:

```
SYSLOG config>no hostname-priority ?
  <cr>
SYSLOG config>
```

Example:

```
SYSLOG config>no hostname-priority
SYSLOG config>
```

Command history:

Release	Modification
11.01.06	This command was introduced as of version 11.01.06.

2.1.8.4 no facility

Restores the default value for the parameter indicating the facility associated to the Syslog messages: 23 (*local7*).

Syntax:

```
SYSLOG config>no facility ?
  <cr>
SYSLOG config>
```

Example:

```
SYSLOG config>no facility
SYSLOG config>
```

2.1.8.5 no initial-delay

Sets the default value for the initial delay before sending the Syslog messages stored in the buffer: 1 second.

Syntax:

```
SYSLOG config>no initial-delay ?
  <cr>
SYSLOG config>
```

Example:

```
SYSLOG config>no initial-delay
SYSLOG config>
```

2.1.8.6 no server

Allows you to delete a Syslog server from those previously added as destinations for messages generated by the client. Servers can be identified through their IP address or their domain name.

Syntax:

```
SYSLOG config$no server ?
  <a.b.c.d>         IP address of the logging host used as syslog server
  <1..255 chars>    Domain name of the logging host used as syslog server
  vrf               Type the name of the vrf to configure
SYSLOG config$
```

Example 1:

```
SYSLOG config>no server 172.24.51.5
SYSLOG config>
```

To delete a server configured for a specific vrf, use the "vrf" option.

Example 2:

```
SYSLOG config$no server vrf test 172.24.51.5
```

Command history:

Release	Modification
11.00.06	The "vrf" option was introduced as of version 11.00.06
11.01.02	The "vrf" option was introduced as of version 11.01.02

2.1.8.7 no severity

Restores the default value for the severity level: 6 (*Informational*).

Syntax:

```
SYSLOG config>no severity ?
  <cr>
SYSLOG config>
```

Example:

```
SYSLOG config>no severity
SYSLOG config>
```

2.1.8.8 no source-address

Deletes the IP address defined as the Syslog message source (when originally configured).

Syntax:

```
SYSLOG config$no source-address ?
  <a.b.c.d>    Ipv4 format
  vrf          Type the name of the vrf to configure
SYSLOG config$
```

Example 1:

```
SYSLOG config>no source-address 192.168.100.1
SYSLOG config>
```

To delete the source-address configured for a specific vrf, use the "vrf" option.

Example 2:

```
SYSLOG config$no source-address vrf test 192.168.100.2
```

Command history:

Release	Modification
11.00.06	The "vrf" option was introduced as of version 11.00.06
11.01.02	The "vrf" option was introduced as of version 11.01.02

2.1.8.9 no timestamp

Restores the default format for the [TIMESTAMP] field: *RFC3164* (Local time in "Mmm dd hh:mm:ss").

Syntax:

```
SYSLOG config$no timestamp ?
    format          Specifies the format of timestamp on log messages
SYSLOG config$
```

Example 1:

```
SYSLOG config>no timestamp format
SYSLOG config>
```

Command history:

Release	Modification
11.00.07	This command was introduced as of version 11.00.07
11.01.02	This command was introduced as of version 11.01.02

2.1.9 SERVER

Configures a Syslog server as destination for the messages generated and sent by the client.

Syntax:

```
SYSLOG config$server <server> ?
       port Server port
       <cr>
SYSLOG config$
```

Note

Please note if server port is not added, it will use the main Syslog port.

There is no limit to the number of Syslog servers that can be added.

Command history:

Release	Modification
11.00.06	The "vrf" option was introduced as of version 11.00.06
11.01.02	The "vrf" option was introduced as of version 11.01.02

2.1.9.1 IP Address

IP address of the logging host used as a syslog server.

Syntax:

```
SYSLOG config$server <ip address> ?
```

```
      port Server port
      <cr>
SYSLOG config$
```

Example:

```
SYSLOG config$ server 172.24.51.5 port 514
```

Note

Please note that servers added this way will be used by the main vrf.

Command history:

Release	Modification
11.01.11	The "port" option was introduced as of version 11.01.11

2.1.9.2 Domain name

Domain name of the logging host used as a Syslog server.

Syntax:

```
SYSLOG config$server <domain name> ?
      port Server port
      <cr>
SYSLOG config$
```

Example:

```
SYSLOG config$ server pruebas.id.teldat.es port 514
```

Note

Please note that servers added this way will be used by the main vrf.

Command history:

Release	Modification
11.01.11	The "port" option was introduced as of version 11.01.11

2.1.9.3 VRF

You may configure servers for specific VRFs through the "vrf " option.

Syntax:

```
SYSLOG config$server vrf <vrf name> <option> ?
      port Server port
      <cr>
SYSLOG config$
```

Example:

```
SYSLOG config$ server vrf test <IP Address>|<Domain name> ?
       port Server port
       <cr>
SYSLOG config$
```

2.1.9.3.1 VRF IP Address

Configure IP Address servers for specific vrfs.

Syntax:

```
SYSLOG config$ server vrf test <IP Address> ?
       port Server port
       <cr>
```

```
SYSLOG config$
```

Example:

```
SYSLOG config$ server vrf test 172.24.51.5 port 514
```

Command history:

Release	Modification
11.01.11	The "port" option was introduced as of version 11.01.11

2.1.9.3.2 VRF Domain name

Configure Domain name servers for specific vrfs.

Syntax:

```
SYSLOG config$ server vrf test <Domain name> ?
       port Server port
       <cr>
SYSLOG config$
```

Example:

```
SYSLOG config$ server vrf test pruebas.id.teldat.es port 514
```

Command history:

Release	Modification
11.01.11	The "port" option was introduced as of version 11.01.11

2.1.9.4 Port

Domain name of the logging host used as a Syslog server.

Syntax:

```
SYSLOG config$server <server> ?
       port   Server port
       <cr>   default
```

Examples:

```
SYSLOG config$ server pruebas.id.teldat.es port 234
```

```
SYSLOG config$ server 172.24.51.5 port 221
```

```
SYSLOG config$ server vrf test pruebas.id.teldat.es port 514
```

> **Note**
>
> Please note that if no port is added, the Syslog server's default port (514) will be used.

Command history:

Release	Modification
11.01.11	The "port" option was introduced as of version 11.01.11

2.1.10 SEVERITY

Assigns a value to the parameter that indicates the managed severity level in Syslog messages for events which, on top of being sent through this protocol (as well as through the Syslog client functionality), have a severity whose numeric code is below or equal to that established. Event severity is closely linked to the *logging-level* (type of event or filtering level), as shown below:

Numerical Code	*Severity*	*Logging-Level*
0	*Emergency*	UI-ERROR
1	*Alert*	CI-ERROR
2	*Critical*	UE-ERROR

3	*Error*	CE-ERROR
4	*Warning*	U-INFO
5	*Notice*	U-TRACE
6	*Informational*	C-INFO
7	*Debug*	C-TRACE, P-TRACE

For further information on the types of events, please see manual bintec-Dm704-I Configuration and Monitoring.

Syntax:

```
SYSLOG config>severity ?
  emergency        System is unusable
  alert            Immediate action needed
  critical         Critical conditions
  error            Error conditions
  warning          Warning conditions
  notice           Normal but significant conditions
  informational    Informational messages
  debug            Debug-level messages
SYSLOG config>
```

Example:

```
SYSLOG config>severity error
SYSLOG config>
```

2.1.11 SOURCE-ADDRESS

Configures the source IP address in the outgoing Syslog messages. When *hostname priority* is configured, or if no *hostname* has been configured, the *source-address* will also appear in the [HOSTNAME] field when specified (otherwise, the device's *global-address* will be sent).

Syntax:

```
SYSLOG config>source-address ?
  <a.b.c.d>     Ipv4 format
  vrf           Type the name of the vrf to configure
SYSLOG config>
```

Example 1:

```
SYSLOG config>source-address 10.65.23.25
SYSLOG config>
```

Source addresses set this way will be used by the main vrf. To configure the source IP address to be used by a specific vrf, use the "vrf " option.

Example 2:

```
SYSLOG config$source address vrf test 10.65.23.25
SYSLOG config$
```

Command history:

Release	**Modification**
11.00.06	The "vrf" option was introduced as of version 11.00.06
11.01.02	The "vrf" option was introduced as of version 11.01.02

2.1.12 TIMESTAMP

Configures the [TIMESTAMP] field, under the HEADER of Syslog messages.

Syntax:

```
SYSLOG config>timestamp ?
  format          Specifies the format of timestamp on log messages.
SYSLOG config>
```

Command history:

Release	Modification
11.00.07	This command was introduced as of version 11.00.07
11.01.02	This command was introduced as of version 11.01.02

2.1.12.1 FORMAT

Configures the format of the [TIMESTAMP] field. This can be established as *RFC3164* (Local time in the format of "Mmm dd hh:mm:ss") or *RFC5424* (UTC in the format of "yyyy-mm-ddThh:mm:ss.msZ, where 'ms' is milliseconds").

By default, its value is *RFC3164*.

Syntax:

```
SYSLOG config>timestamp format ?
  RFC3164          Local time 'Mmm dd hh:mm:ss'
  RFC5424          UTC 'yyyy-mm-ddThh:mm:ss.msZ'
SYSLOG config>
```

Example:

```
SYSLOG config>timestamp format RFC3164
SYSLOG config>
```

Command history:

Release	Modification
11.00.07	This command was introduced as of version 11.00.07
11.01.02	This command was introduced as of version 11.01.02

2.1.13 EXIT

Exits the Syslog client facility configuration menu and returns to the main configuration menu (*Config*>).

Syntax:

```
SYSLOG config>exit
```

Example:

```
SYSLOG config>exit
Config>
```

2.2 Notification of events as syslog messages

Apart from configuring the Syslog client functionality, you also need to indicate which events will be notified through Syslog messages. This is done from the Events Logging System (ELS) configuration menu.

Syntax:

```
*p 4
Config>event

-- ELS Config --
ELS config>enable ?
  all                  Events as traps, syslog messages and on screen
  condition-debug      Enable a trace used for debugging of conditional events
  trace                Events on screen
  syslog               Events as syslog messages
  snmp-trap            Events as traps. Habil event for all trap groups
  snmp-trap-group1     Events as traps for group 1
  snmp-trap-group2     Events as traps for group 2
  snmp-trap-group3     Events as traps for group 3
  snmp-trap-group4     Events as traps for group 4
  filter               Enables events filtering
ELS config>enable syslog ?
  subsystem     An entire subsystem with a filter level
  groups        An entire group
  event        An individual event
ELS config>
```

As you can see in the syntax, a specific event, a complete subsystem, or a group made up of certain events selected by the user can be enabled to be sent to one or several Syslog servers. If you introduce these commands from the configuration process (CONFIG or P 4), you will need to save the configuration and restart the device in order to activate the changes of the new configuration.

Example:

```
ELS config>enable syslog subsystem ppp all
ELS config>
```

In this example, all the PPP subsystem events have been enabled so they are notified in Syslog message format. However, message transmission to the Syslog server (or servers) is only carried out when the severity regarding the logging-level, filtering level or type of event is lower or equal to the one established in the Syslog client configuration. To learn if this is so, numerical codes are compared. Obviously, said functionality must be enabled.

Important

If you have established a DEBUG severity level in the Syslog client functionality, THE IP SUBSYSTEM EVENTS whose filtering level or logging-level is TRACE, MUST NOT BE ENABLED to be sent in Syslog messages. Since the Syslog protocol is based on UDP, transmitting these messages will create a high number of events of this type and could saturate the buffer (with the resulting loss of messages).

To disable previously configured individual events, complete subsystems or groups of events for transmission in Syslog message format, simply use the **DISABLE** command.

Syntax:

```
*p 4
Config>event

-- ELS Config --
ELS config>disable ?
  all                 Events as traps, syslog messages and on screen
  trace               Events on screen
  syslog              Events as syslog messages
  snmp-trap           Events as traps. Habil event for all trap groups
  snmp-trap-group1    Events as traps for group 1
  snmp-trap-group2    Events as traps for group 2
  snmp-trap-group3    Events as traps for group 3
  snmp-trap-group4    Events as traps for group 4
ELS config>disable syslog ?
  subsystem    An entire subsystem with a filter level
  groups       An entire group
  event        An individual event
ELS config>
```

Example:

```
ELS config>disable syslog subsystem ppp all
ELS config>
```

An individual event, a complete subsystem, or a group of events to be notified via Syslog messages can be enabled from the Events Logging System (ELS) monitoring menu, in accordance with the P 3 (or MONITOR) process.

Syntax:

```
*p 3
Console Operator

+event

-- ELS Monitor --

ELS+enable ?
  all                 Events as traps, syslog messages and on screen
  filter              Enables events filtering
  snmp-trap           Events as traps. Habil event for all trap groups
  snmp-trap-group1    Events as traps for group 1
  snmp-trap-group2    Events as traps for group 2
  snmp-trap-group3    Events as traps for group 3
  snmp-trap-group4    Events as traps for group 4
  syslog              Events as syslog messages
  trace               Events on screen
ELS+enable syslog ?
  event        An entire subsystem with a filter level
  groups       An entire group
  subsystem    An entire subsystem with a filter level
ELS+
```

In this case, changes take immediate effect. From this point on, events enabled to be sent using the Syslog protocol will begin to be transmitted in Syslog message format when the situation arises. This happens when the following conditions are met: the Syslog client functionality is enabled, the established severity level has a numeric code equal to, or higher than, the one associated to the event (depending on its *logging-level*), etc.

Example:

```
ELS+enable syslog subsystem ppp all
ELS+
```

Just like with the ELS configuration menu, you can also use Syslog messages to dynamically disable the notification for individual events, complete subsystems or groups of events. This takes immediate effect:

Syntax:

```
*p 3
Console Operator

+event

-- ELS Monitor --

ELS+disable ?
  all                 Events as traps, syslog messages and on screen
  filter              Enables events filtering
  snmp-trap           Events as traps. Habil event for all trap groups
  snmp-trap-group1    Events as traps for group 1
  snmp-trap-group2    Events as traps for group 2
  snmp-trap-group3    Events as traps for group 3
  snmp-trap-group4    Events as traps for group 4
  syslog              Events as syslog messages
  trace               Events on screen
ELS+disable syslog ?
  event        An entire subsystem with a filter level
  groups       An entire group
  subsystem    An entire subsystem with a filter level
ELS+
```

Example:

```
ELS+disable syslog subsystem ppp all
ELS+
```

For further information on how to enable and disable events, subsystems or groups of events, or the different ways in which these can be notified, please see manual bintec-Dm704-I Configuration and Monitoring.

Chapter 3 Monitoring

3.1 Monitoring the Syslog client facility

In order to access the monitoring menu associated to the Syslog client facility, you need to introduce the **FEATURE SYSLOG** command in the general monitoring menu (+).

```
+feature syslog
-- SYSLOG client console --
SYSLOG+
```

Once you have accessed the Syslog client monitoring environment, you can enter the following commands:

Command	Function
? (HELP)	Lists the available commands or options.
LIST	Displays Syslog client monitoring information.
EXIT	Exits the Syslog client monitoring menu.

3.1.1 ? (HELP)

Lists the valid commands at the level where the router is programmed. You can also use this command after a specific command to list the available options.

Syntax:

```
SYSLOG+?
```

Example:

```
SYSLOG+?
  list    Show monitoring information
  exit
SYSLOG+
```

3.1.2 LIST

Displays information on the active Syslog client configuration, as well as the relevant statistics.

Syntax:

```
SYSLOG+list
```

Example:

```
SYSLOG+list

Syslog client active configuration:

Syslog client status: ENABLED
Facility: 23 (Local7)
Severity: 6 (Informational)
Source IP address: 1.2.3.4

Active syslog servers:

IP address       Domain name                     Vrf              Source-Address
--------------- ------------------------------ ---------------  ---------------
192.168.214.152                                                   1.2.3.4
192.168.214.152                                  test             10.20.30.40
0.0.0.0          test.domain.com                 test2

Syslog client statistics:

Total number of transmitted messages:                 42
Emergency messages:                                   0
```

```
Alert messages:                                   0
Critical messages:                                0
Error messages:                                   0
Warning messages:                                 21
Notice messages:                                  0
Informational messages:                           0
Debug messages:                                   0
Events with severity greater than established level:  650
Lost messages due to buffer overflow:             0

SYSLOG+
```

As you can see, on executing the **LIST** command from the Syslog client monitoring menu, data on the active configuration for said function is displayed:

- *Syslog client status*: If the facility is enabled or not.
- *Facility*: Facility value associated to the Syslog message.
- *Severity*: Established severity level. This value, together with the facility value, is used to calculate the priority of the Syslog message.
- *Source IP address*: Whenever this parameter has been configured, it shows the source IP address indicated in the outgoing messages. If said address does not appear, the packets exit the router with the interface source address through which they are transmitted. When *hostname priority* is configured, or if no *hostname* has been configured, this *source-address* will also appear in the [HOSTNAME] field when specified (otherwise, the device's *global-address* will be sent). This value refers to the main vrf.
- Servers that receive the messages sent by the client. In cases of servers identified by their domain name, if one of the configured DNS servers in charge of the translation manages to obtain the IP address, this will be displayed next to the name.

A series of statistics are also saved:

- Total number of transmitted messages (considering all the messages sent to the configured servers).
- Number of events corresponding to each type of message (depending on the severity) generated by the client. In this case, each event (instead of every transmitted message) is counted. This means that the same message sent to several servers increases the counter associated to the filtering level or severity by one.
- Events whose severity level is greater than the one established (identified through the comparison of their numerical codes) and therefore do not transmit a Syslog message to each configured server. As in the previous case, only the events generated (and not the number of messages sent) are counted.
- Number of events that could not be notified due to saturation of the buffer where pending Syslog messages are stored. This counter increases with each message lost, regardless of the number of notifications that each event generates based on the number of servers the message had to be sent to.

If the Syslog client functionality is disabled (i.e. no messages are generated) these statistics will always take a value of 0.

3.1.3 EXIT

Exits the Syslog client monitoring menu and returns to the main monitoring menu (+).

Syntax:

```
SYSLOG+exit
```

Example:

```
SYSLOG+exit
+
```

Chapter 4 Example

4.1 Syslog client configuration example

This section shows how to configure the Syslog client functionality:

```
log-command-errors
no configuration
set data-link astm serial0/0
set data-link x25 serial0/1
set data-link x25 serial0/2
time summer-time recurring 4 sun mar 02:00 4 sun oct 03:00
;
;
network ethernet0/0
; -- Ethernet Interface User Configuration --
   ip address 172.24.78.118 255.255.0.0
;
;
;
;
exit
;
;
;
network x25-node
; -- X25-node interface configuration --
   no ip address
;
exit
;
event
; -- ELS Config --
   enable syslog event GW.001
   enable syslog event GW.021
   enable syslog event GW.023
   enable syslog subsystem TCP ALL
   enable syslog subsystem UDP ALL
   enable syslog subsystem ARP ALL
exit
;
;
protocol ip
; -- Internet protocol user configuration --
   route 0.0.0.0 0.0.0.0 172.24.0.98
;
;
exit
;
;
feature ntp
; -- NTP Protocol user configuration --
   protocol
   peer address 1 172.24.51.36
exit
;
feature dns
; -- DNS resolver user configuration --
   server 172.24.51.36
exit
;
feature syslog
; -- SYSLOG client configuration --
   enable
   buffer-size 60
   facility local0
   initial-delay 25
   server pruebas.id.bintec.es
   server 172.24.51.5
   severity error
   source-address 10.65.23.25
exit
;
dump-command-errors
end
; --- end ---
Config>
```

In this case, the severity level has been established in *error* (3). This means enabled events whose filtering level or *logging-level* is UI-ERROR, CI-ERROR, UE-ERROR, CE-ERROR or ALWAYS will be notified as Syslog messages. In this specific example, Syslog messages are sent to servers identified by IP address 172.24.51.5 and domain name pruebas.id.bintec.es (provided that the latter has been previously resolved by one of the configured DNS servers, in this case the one with IP address 172.24.51.36). These messages are generated when situations arise that result in events GW.001, GW.021, GW.023 (as well as those pertaining to the ARP, TCP, and UDP subsystems whose filtering type or level is one of those previously specified). The facility, together with the severity level of each specific event, is used to calculate the priority value assigned to the message. In this case, it will be *local0* (16) and source address 10.65.23.25.

In this example, a 25-second initial delay has been set before the process of reading the buffer begins and any pending messages found there are transmitted. This is because GW.001 and GW.021 events have been enabled on startup (GW.001 indicates device startup and GW.021 that the interface is up) and the user wants to make sure they are correctly transmitted and not lost before the device has finished booting. Please bear in mind that if these startup events have not been enabled, you do not need to modify the default value for this parameter (initial-delay).

The default size of the message storage buffer has also been changed (from 50 to 60 messages). However, as previously mentioned, you do not usually have to modify this default value.

As for the rest of the configuration, it is essential to configure at least one DNS server to resolve domain names for the Syslog servers identified. Using the NTP protocol to find out the current date and time is not required as, in cases where this functionality is not enabled, the local clock on the device is used to fill-in the [TIMESTAMP] field on the Syslog message. The same thing happens with daylight saving, configured in the example for general information.