



Vanguard Networks Applications Ware

SYSLOG Client User Manual

Notice

©2010 Vanguard Networks
25 Forbes Boulevard
Foxboro, Massachusetts 02035
(508) 964-6200
All rights reserved
Printed in U.S.A.

Restricted Rights Notification for U.S. Government Users

The software (including firmware) addressed in this manual is provided to the U.S. Government under agreement which grants the government the minimum “restricted rights” in the software, as defined in the Federal Acquisition Regulation (FAR) or the Defense Federal Acquisition Regulation Supplement (DFARS), whichever is applicable.

If the software is procured for use by the Department of Defense, the following legend applies:

Restricted Rights Legend

Use, duplication, or disclosure by the Government
is subject to restrictions as set forth in
subparagraph (c)(1)(ii) of the
Rights in Technical Data and Computer Software
clause at DFARS 252.227-7013.

If the software is procured for use by any U.S. Government entity other than the Department of Defense, the following notice applies:

Notice

Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in FAR 52.227-19(C).

Unpublished - rights reserved under the copyright laws of the United States.

Proprietary Material

Information and software in this document are proprietary to Vanguard Managed Solutions, LLC (or its Suppliers) and without the express prior permission of an officer, may not be copied, reproduced, disclosed to others, published, or used, in whole or in part, for any purpose other than that for which it is being made available. Use of software described in this document is subject to the terms and conditions of the Software License Agreement.

This document is for information purposes only and is subject to change without notice.

Part No. T0299-01, Rev. A

Publication Code TK

First Printing July 2010

Manual is current for Release 7.3 of Vanguard Applications Ware.

To comment on this manual, please send e-mail to vntechsupport@vanguardnetworks.com

Overview	1
Introduction	1
Before Using This Manual	1
Trademarks	1
Related Vanguard Information	1
Introduction to SYSLOG	2
What is SYSLOG?	2
Application of the Vanguard Networks SYSLOG Client Feature	2
SYSLOG Message Types	3
SYSLOG Client Theory of Operation	4
SYSLOG Message Format	5
SYSLOG Message Details	5
SYSLOG Message Header	6
Supported Facility Codes	7
Facility Code Setting	8
Supported Severity Codes	8
Filtering SYSLOG Messages Based on Severity	8
Logged Alarm Priority Level to SYSLOG Message Severity Level Mapping	9
Alarm Throttling and Node Record Alarm Selection	9
Version Number	9
Timestamp	9
Hostname	9
APP-Name	10
PROC-ID	10
MSG-ID	10
Vanguard Networks SYSLOG Message Header Example	10
IANA-defined Structured Data Field	11
Vanguard Networks Private Structured Data Field	11
SYSLOG Message Text Field	12
SYSLOG Messages	13
Event Type SYSLOG Message	13
Authorization Type SYSLOG Message	13
Accounting Type SYSLOG Message	14
Traffic Monitor SYSLOG Messages	14
SYSLOG Message Congestion Control	15
Configuration of the SYSLOG Parameters	16
Introduction	16
Configuring the SYSLOG Client Feature	16
Configure Menu	16
Configuring SYSLOG Menus	17
Introduction	17
Configuration	17
SYSLOG Configure Menu	17
SYSLOG Global Parameters Configuration	17
SYSLOG Server Parameters Configuration	18
Statistics	22
Introduction	22
Types of SYSLOG Statistics Menus	22
Access and Reset Statistics	22

Contents (continued)

- SYSLOG Statistics Menu 22
- Access Server Statistics 22
- Detailed SYSLOG Server Statistics Menu 23
- Description of Terms 24
- SYSLOG Boot Menu 25
- SYSLOG Global Boot Description 25
- SYSLOG Server Boot Description 25
- SYSLOG Configuration Examples 26
- Basic SYSLOG Configuration Example 2 6
- Traffic Logging SYSLOG Configuration Example 27

Overview

Introduction

The purpose of this document is to describe the Vanguard Networks SYSLOG Client feature. The SYSLOG Client feature is the implementation of the SYSLOG Protocol and is compliant with RFC5424. The SYSLOG Client feature is available for the Vanguard Networks 7300, 6800, and 3400 routers starting in Release 7.3.R00A with the purchase of the Security Services Add-on license.

Before Using This Manual

Before using this manual you should have experience with IP-Routing and familiarity with the Vanguard Networks Products.

Trademarks

The following are trademarks or registered trademarks of their respective companies or organizations:

- Vanguard and Vanguide are trademarks or registered trademarks of Vanguard Networks, LLC

Related Vanguard Information

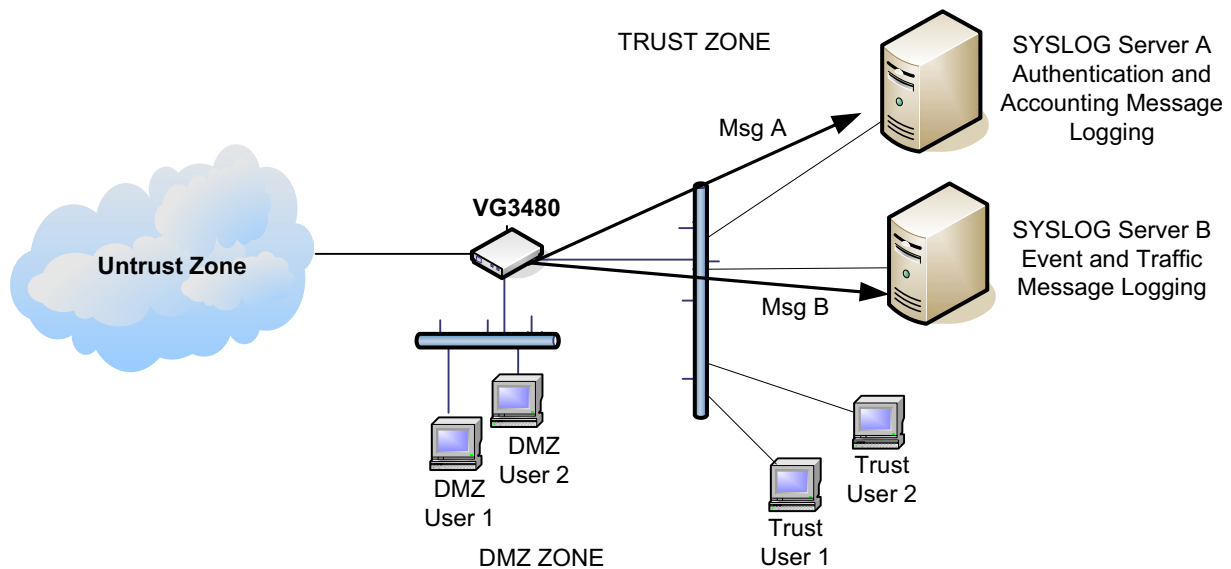
Refer to these related Vanguard Applications Ware documents for additional information:

- Vanguard Networks Basic Protocols Manual (Part No. T0113)
- Vanguard Networks Router Basics Manual (Part No. T0100-01)
- Vanguard Networks IP and LAN Feature Protocols Bridging P/N T0100-02
- Vanguard Networks IP Routing Basics Manual (Part No. T0100-03)
- Vanguard Networks IP and LAN Feature Protocols Manual (Part No. T0100-03)
- Vanguard Networks SNMP/MIB Management Manual (Part No. T0106-04)
- Vanguard Networks Alarms and Reports Manual (Part No. T0005) for details on alarms and reports generated by this feature

Introduction to SYSLOG

What is SYSLOG? SYSLOG is a standardized scheme for generating and sending events from a device, or a client, to a collector, or a server. It specifies the format of the event messages. Because the event message format is standardized and the event messages are stored in a centralized collector, Network Administrators are able to conveniently access and analyze the events.

Application of the Vanguard Networks SYSLOG Client Feature The Vanguard Networks SYSLOG Client feature enables the Vanguard Network Router Products to send SYSLOG messages to up to two SYSLOG servers. It categorizes the SYSLOG messages into four message types: Authentication, Accounting, Event, and Traffic-Monitoring, and is capable of directing these SYSLOG messages based on their message types. For instance, in Figure 1, the Vanguard Networks 3480 is configured to send Authentication and Accounting SYSLOG messages to server A in addition to sending Event and Traffic-monitoring messages to server B.



The 3480 sends SYSLOG Messages to Hosts A and B:

Msg A) Authentication and Accounting Type SYSLOG messages

Msg B) Event and Traffic Type SYSLOG Messages

Figure 1. Application of the Vanguard Networks SYSLOG Client Feature

**SYSLOG Message
Types**

There are four types of SYSLOG messages:

The Authentication SYSLOG Messages contain information about users that are logging-in, users that are attempting to login, and users that are logging-out from the User Interface of the Vanguard Networks Router.

The Accounting SYSLOG Messages contain information about any configuration changes including modifying or booting parameters, loading software images, enabling/disabling links, or any other modification to the configuration.

The Event SYSLOG Messages correspond to Alarms in the Alarm Log like LINK-UP or LINK-DOWN Alarms.

The Traffic-monitoring SYSLOG Messages correspond to the Traffic Logging messages generated by the Vanguard Networks Firewall Application.

**SYSLOG Client
Theory of
Operation**

Figure 2 shows a simplified IP Network containing a SYSLOG client (VN3480) and a SYSLOG server (Host A). In Figure 2, the SYSLOG client is sending a SYSLOG Message through the IP Network to the SYSLOG server. (The SYSLOG Message is described in detail in the next section.)

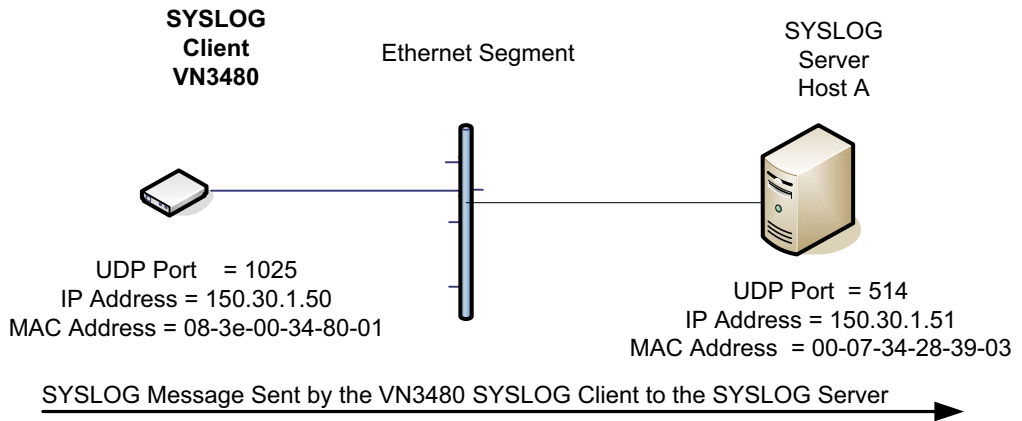


Figure 2. SYSLOG Sample Network Connection

The SYSLOG client is sending the SYSLOG message using User Datagram Protocol (UDP). It is sending the SYSLOG message destined to the SYSLOG server's UDP Port, 514, and the SYSLOG server's IP Address, 150.30.1.51. Both the UDP Port and IP address of the SYSLOG server are configurable from the SYSLOG Server Menu of the VN3480.

The source IP Address and source UDP Port of the SYSLOG message, in figure 2, are 150.30.1.50 and 1025, respectively. The source IP address is configurable in the VN3480 SYSLOG Server Menu. The UDP Port number is automatically assigned when the UDP session is initialized.

SYSLOG Message Format

Figure 3 shows a break-out of the SYSLOG frame in Figure 2. Within this frame are the Ethernet MAC Header, the IP Header, the UDP Header, and the SYSLOG Message. As shown in Figure 3, the SYSLOG Message contains three parts: Message Header, the Structured Data Field, and the Message Text Field.

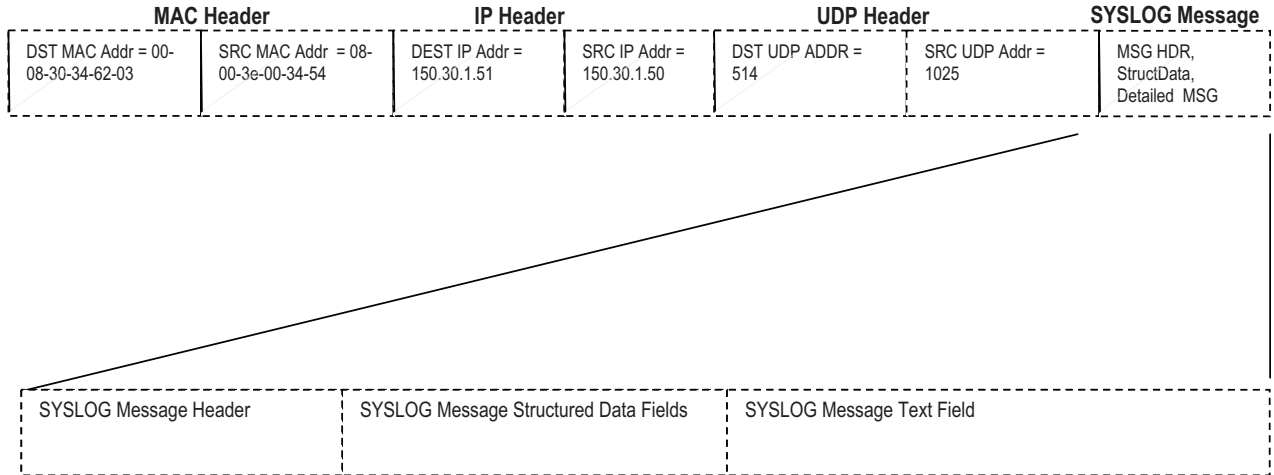


Figure 3. SYSLOG Message from Figure 2.

SYSLOG Message Details

Figure 4 shows the details of the SYSLOG Message. The SYSLOG Message consists of the SYSLOG Message Header, the Structured Data Field, and the Message Text field. These three portions of the SYSLOG Message are described in more detail in the following sections.

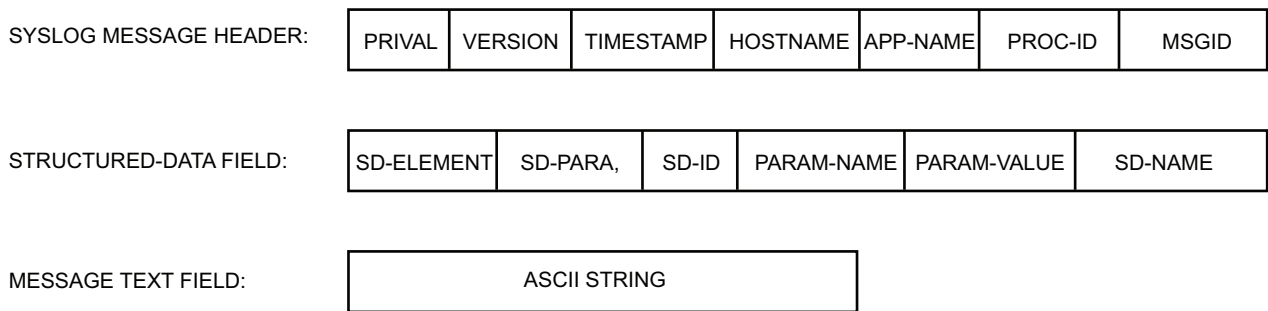


Figure 4. SYSLOG Message Contents

SYSLOG Message Header

Figure 5 shows the SYSLOG Message Header. The SYSLOG Message Header consists of the PRIVAL Field, the Version Number, the Time Stamp, the Hostname, the APP-Name, the PROC-ID, and the MSG-ID. The following sections describe these fields in more detail.

PRIVAL	VERSION	TIMESTAMP	HOSTNAME	APP-NAME	PROC-ID	MSGID
--------	---------	-----------	----------	----------	---------	-------

Figure 5. SYSLOG Message Header

PRIVAL Field

The PRIVAL (Priority Value) field consists of the Facilities Code and the Severity Code. The following calculation shows how the Facilities Code and Severity Code are combined to form the PRIVAL field. It is calculated as follows:

$$\text{PRIVAL} = \langle \text{nnn} \rangle = \text{Facility} \times 8 + \text{Severity (converted to ASCII)}.$$

For example, if the Facility is LOCAL4, 20d, and the severity is 5, PRIVAL is $20 \times 8 + 5 = 165d$. When converted to ASCII, it becomes 31h,36h,35h (where h= hexadecimal). Further, the PRIVAL is enclosed in <> brackets. So, in this example, the PRI field in Figure 5 is:

<165>

Supported Facility Codes

Table 1 shows all of the possible Facility Codes defined by RFC5424. The first Column, “Numerical Code”, is the decimal representation of the facility code. The column labeled “Vanguard Networks Applications Ware Facility Code” is a list of the possible facility codes that the Vanguard Networks SYSLOG Client sends in the PRIVAL field of the SYSLOG Message.

Table 1. Facility Codes sent by Vanguard Networks SYSLOG Client

Numerical Code	Description	Vanguard Networks Applications Ware Supported Facilities
0	kernel messages	KERNEL
1	user-level messages	NA
2	mail system	NA
3	system daemons	NA
4	security/authorization msgs	AUTHORIZATION
5	ONS SYSLOG specific Events	NA
6	line printer subsystem	NA
7	network news subsystem	NA
8	UUCP subsystem	NA
9	clock daemon	NA
10	security/authorization msgs	SECURITY
11	FTP daemon	NA
12	NTP subsystem	NA
13	log audit (note 1)	LOG_AUDIT
14	log alert (note 1)	LOG_ALERT
15	clock daemon (note 2)	NA
16	local use 0 (local0)	LOCAL0
17	local use 1 (local1)	LOCAL1
18	local use 2 (local2)	LOCAL2
19	local use 3 (local3)	LOCAL3
20	local use 4 (local4)	LOCAL4
21	local use 5 (local5)	LOCAL5
22	local use 6 (local6)	LOCAL6
23	local use 7 (local7)	LOCAL7

Facility Code Setting

The Facility Code, in the PRIVAL field, is determined by either “SYSLOG Facility Code Override Parameter” or by the mapping shown in Table 3. If the Facility Code Override is set to “None”, then the mapping shown in Table 2 is used to determine the Facility Code. From Table 2, if the Message Type is “Event” then the Facility Code is set to LOG_ALERT. If the Message Type is Authorization, then the Facility Code is set to Authorization. If the Message Type is Accounting or Traffic, then the Facility Code is set to LOG AUDIT.

If the “SYSLOG Facility Code Override” is set to a value other than NONE, then the SYSLOG Facility Code Override is always sent with this override value.

Table 2. Logged Alarm Severity to SYSLOG Severity

SYSLOG Message Type	Facility Code
Event	LOG ALERT
Authorization	LOG AUTHORIZATION
Accounting	LOG AUDIT
Traffic	LOG AUDIT

Supported Severity Codes

Table 3 shows all of the possible Severity Codes supported by the Vanguard Networks SYSLOG Client feature. These are the possible values that can appear in the Severity portion of the PRIVAL field in the SYSLOG message sent by the SYSLOG Client feature.

Table 3. SYSLOG Severity Codes and Descriptions

Numerical Code	Description	Vanguard Networks Applications Ware Supported Facilities
0	Emergency: system is unusable	EMERGENCY
1	Alert: action must be taken immediately	ALERT
2	Critical: critical conditions	CRITICAL
3	Error: error conditions	ERROR
4	Warning: warning conditions	WARNING
5	Notice: normal but significant condition	NOTICE
6	Informational: informational messages	INFORM
7	Debug: debug-level messages	DEBUG

Filtering SYSLOG Messages Based on Severity

The “SYSLOG Severity” Parameter in the “SYSLOG Server Configuration” is used to specify, based on the severity field of the SYSLOG message, which messages to send and which messages to block. If the Severity in the SYSLOG message PRIVAL field is not configured as a value within the SYSLOG Severity Parameter, the SYSLOG Message will not be sent to the SYSLOG server.

Logged Alarm Priority Level to SYSLOG Message Severity Level Mapping

When a Logged Alarm is sent as a SYSLOG Message by the SYSLOG Client feature, the Logged Alarm Level is mapped to a SYSLOG Severity Level according to Table 4. As shown in Table 4, a High Level Alarm is sent as a SYSLOG Message with the SYSLOG Severity level set to Alert. The Medium Level Alarm is sent as a SYSLOG Message with the SYSLOG Severity level set to Critical. The Connection Level Alarm is sent as SYSLOG Severity of Notice. And, the Low Level Alarm is sent as SYSLOG Severity of Informational.

Table 4. Logged Alarm Severity to SYSLOG Severity

<i>Logged Alarm</i>		<i>SYSLOG Severity</i>
<i>Numerical Code</i>	<i>Description</i>	
1	High	Alert: action must be taken immediately
2	Medium	Critical: critical conditions s
3	Connection	Notice: normal but significant condition
4	Low	Informational: informational messages

Alarm Throttling and Node Record Alarm Selection

Alarm Filtering is accomplished by the setting of the Alarm Throttling Configuration and the Node Record Alarm Selection configuration. This filtering results in the corresponding SYSLOG message being filtered. This impacts Event, Authentication, and Accounting message types. Traffic Monitoring SYSLOG Messages are controlled with the Firewall Policy configuration parameter, “Traffic Monitoring”.

Version Number

As shown in Figure 4, following the PRIVAL field in the SYSLOG Message Header is the Version Number. The SYSLOG Client supports Version 1. Therefore, the Version Number field of the SYSLOG Message Header is set to ASCII 1, or 31H.

Timestamp

The Timestamp comes after the Version Number in the SYSLOG Message Header. If the Universal Time Zone (UTC) parameter in the Node Record is set to EST, the timestamp will appear in the following format:

2010-01-25T19:20:50.00-05:00,

If the Universal Time Zone parameter is set to GMT, the timestamp will appear in the following format:

2010-01-25T19:20:50.00.

Hostname

The Hostname comes after the Timestamp in the SYSLOG Message Header. The hostname is the the Domain Name that is configured in the Node Record. It is transmitted in the Hostname field of the SYSLOG Message Header. If the Domain Name in the Node Record is blank, then the Default Router IP Address is transmitted in the Hostname field of the SYSLOG Message Header. The Hostname is limited to 255 alphanumeric characters or less. For example,

vn3480a.vanguard.com

APP-Name

The APP-Name comes after the Hostname. The APP-Name is set to the Vanguard Networks Applications Ware module that generated the SYSLOG message. For instance, if the SYSLOG Message is from the Vanguard Networks Applications Ware BGP Module, then the SYSLOG application name will be:

BGP

PROC-ID

The PROC-ID comes after the APP-Name. It is always set to the Nil-Value in the SYSLOG Message Header:

MSG-ID

The MSG-ID represents the Vanguard Applications Ware Module, a period, and the Vanguard Networks Applications Ware report number. For example:

BGP.5 stands for the BGP module's fifth message.

Vanguard Networks SYSLOG Message Header Example

Figure 6 shows an example of an actual SYSLOG Message Header. In this example, the PRIVAL is 165 which represents a Facility Code of 20 decimal, or "LOCAL4", and a severity of 5, or SYSLOG_NOTICE.

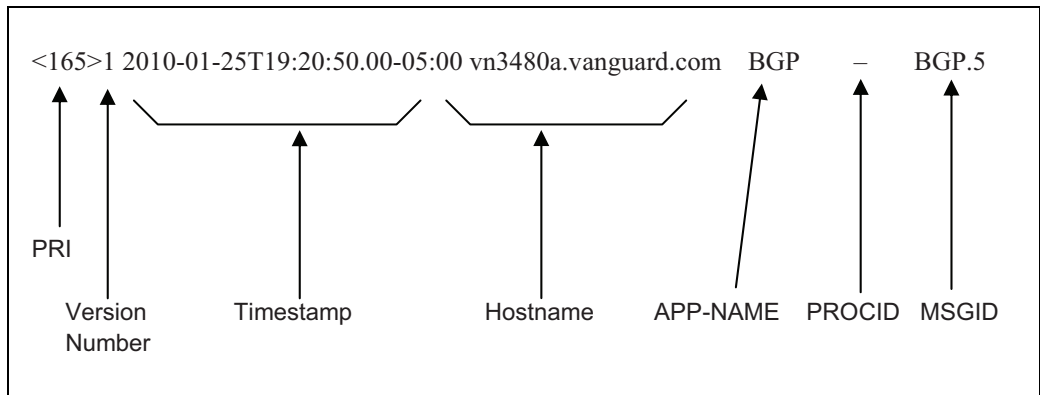


Figure 6. Sample VN SYSLOG Message Header Format

Also, in this example, the Version Number is 1 and the timestamp is January 25, 2010 at 7:20:50 p.m. The Hostname is from the Domain Name configured in the Node Record. The APP-NAME is BGP because the Vanguard Networks Applications Module that generated the SYSLOG message was BGP. The PROCID is transmitted as the NILVALUE, because the Process ID field is not support by the Vanguard Networks Router. The MSG-ID is BGP.5 because this message is from the BGP module and the message number is the fifth BGP message in BGP's message list.

IANA-defined Structured Data Field

Following the SYSLOG Message Header are the IANA-defined Structured Data fields of the SYSLOG message. Vanguard Networks SYSLOG Client sends three standard, IANA-defined, Structured Data Fields with each SYSLOG message: the origin IP, the enterpriseID, and the swVersion. Vanguard Networks SYSLOG Client sets the origin IP field to the source IP Address in the SYSLOG configuration, in this example 150.30.1.50. It sets the enterprise ID to 449 which is registered to Codex and grandfathered to Vanguard Networks. (See <http://www.iana.org/assignments/enterprise-numbers>.) Finally, the Vanguard Networks SYSLOG Client sets the swVersion structured data parameter to a string such as "V7.3.R00A (28-Jan-2010 17:07) Size =4721692 bytes". Figure 7 shows an example of the IANA defined Structured Data Parameters.

```
[origin ip="150.30.1.50"][enterpriseid="449"][swVersion="V7.3.R00A (28-Jan-2010 17:07) Size =4721692 bytes"]
```

Figure 7. IANA defined Structured Data Field

Vanguard Networks Private Structured Data Field

Following the IANA-defined structured data fields, the Vanguard Networks SYSLOG client transmits two private Structured Data Fields. The first is the vnstats@449 Structured Data Field. This Structured Data Field is in ASCII and provides the nodeName, the CPU Utilization, and the Buffer Counts for the Vanguard Networks Router. An example is illustrated in Figure 8.

```
[vnstats@449 nodeName="node101" cpu="50" cpuUtMax="50" pBuffer cur/max="344/1650" dbuffer cur/max="120/18984"]
```

Figure 8. Example of vnstats@449 Structured Data Field

The second Vanguard Networks Structured Data Field specifies the type of message being sent. It is either `vnevent@449`, `vnauth@449`, `vnaccount@449`, or `vntraffic@449` depending on the type of SYSLOG Message: event, authorization, accounting, or traffic, respectively. Table 5 shows examples of these Structure Data Fields. The trap number is included as a parameter for each of these Structured Data Fields.

Table 5. List of Structured Data Fields representing message type

Message Type	Vanguard Networks Message Type Structured Data Field
Authentication	<code>vnauth@449 TrapNumber="105001"</code>
Accounting	<code>vnaccount@449 TrapNumber="205002"</code>
Event	<code>vnevent @449 TrapNumber = "301003"</code>
3Traffic	<code>vntraffic@449 TrapNumber="403002"</code>

SYSLOG Message Text Field

Figure 9 shows a typical SYSLOG Message Text Field. This follows after the Structured Data Field of the SYSLOG message. The message text in the SYSLOG Message shown here is equivalent to what appears in the Vanguard Networks Router Alarm Log.

(1) node1 2010-02-25 11:52:43 BGP.12 BGP Peer Established

Figure 9. Sample ONS SYSLOG MSG Text Field

SYSLOG Messages

Event Type SYSLOG Message

Figure 10 shows a SYSLOG message including the SYSLOG Message header, the IANA-defined structured data fields, the Vanguard Networks defined private structured data field, vnstats, the private structured data field indicating that this message is an Event Type message, and the message field. An Event Type SYSLOG message is generated when a Vanguard Applications Ware Alarm is generated and stored in the Logged Alarm Database. If the Logged Alarm Severity is enabled in the Node Record Parameter “Alarm Selection” and the Logged Alarm is not throttled in the Alarms Throttling configuration, the SYSLOG Message for the Logged alarm will be generated.

```
<165>1 2010-02-28T19:20:50.00-05:00 vn3480a.vanguard.com BGP - BGP.12
  [origin ip="150.30.1.50" enterpriseld=449 swVersion="V7.3.R00A (28-Jan-2010 17:07)"]
  [vnstats@449 nodeName="node101" cpuUt="50" cpuUtMax="50" pbuffer cur/max="344/1650" dbuffer cur/max="120/18984"]
  [vnevent@449 TrapNumber="501002"]
  (1) node1 2010-02-25 11:52:43 BGP.12 BGP Peer Established
```

Figure 10. Sample VN Event SYSLOG message

Authorization Type SYSLOG Message

Figure 11 shows an example of an Authorization SYSLOG message. It is generated when a user logs in, when a user attempts to login but is unsuccessful, and when a user logs-out of the Vanguard Networks Router User Interface. The Authorization Alarm message is generated for CTP access, Telnet Access, SSH Access, and HTML Access. The Authorization Type SYSLOG messages are generated when a Vanguard Applications Ware Authorization Alarm is generated and stored in the Logged Alarm Database. All Vanguard Applications Ware Authorization Alarms are assigned a HIGH Severity. If the “High” Logged Alarm Severity Selection is configured in the Node Record Parameter, “Alarm Selection”, and the Authorization Alarm is not being throttled via the Alarms Throttling Configuration Menu, the SYSLOG Message will be generated.

```
<33>1 2010-01-28T19:20:50:52-04:00 vn3480a.vanguard.com CTP - CTP.12
  [origin ip="150.30.1.50"] [ enterpriseld=449] [swVersion="V7.2.R00A (28-Jan-2010 17:07)"]
  [vnstats@449 nodeName="node101" cpuUt="50" cpuUtMax="50" pbuffer cur/max="344/1650" dbuffer cur/max="120/18984"]
  [vnauth@449 TrapNumber=5004]
  "(1) node1 23-Jan-2010 19:20:50 CTP: Login Authorized for User Leah Privilege = High-Level"
```

Figure 11. Sample VN Authorization SYSLOG message

Accounting Type SYSLOG Message

Accounting SYSLOG messages are generated for all system administrative activities such as configuration changes, booting, image transfer, and image corruption. The “Configuration Change Alarm” Parameter in the Node Record must be set to Enabled for the Accounting Type SYSLOG Messages to be generated. Figure 12 shows an example of a Vanguard Networks Accounting SYSLOG message. All Vanguard Applications Ware Accounting Alarms are assigned a HIGH Severity. If the “High” Logged Alarm Severity Selection is configured in the Node Record Parameter, “Alarm Selection”, and the Accounting Alarm is not being throttled via the Alarms Throttling Configuration Menu, the SYSLOG Message will be generated.

```
<165>1 2010-01-28T19:20:50:52-04:00 vn3480a.vanguard.com CTP - CTP.4
  [origin ip="150.30.1.50" enterpriseld=449][swVersion="V7.2.R00A (28-Jan-2010 17:07)"]
  [vnstats@449 nodeName="node101" cpuUt="30" cpuUtMax="50" pbuffers cur/max="334/31650" dbuffer cur/max="120/18010"]
  [vnaccount@449 TrapNumber = 5005]
  "(1) node1 23-Jan-2010 19:20:50 CTP: Configuration Changed: 1st prompt=Boot Port menu path=Main.7.1"
```

Figure 12. Sample VN Accounting SYSLOG Message

Traffic Monitor SYSLOG Messages

Traffic Monitor SYSLOG messages are generated by the Vanguard Networks Firewall feature. Figure 13 shows an example of a Traffic Monitoring SYSLOG message sent by the Vanguard Networks SYSLOG Client. Traffic Monitoring SYSLOG Messages are generated if the “Traffic Logging” parameter is configured in the Firewall Policies Configuration Menu. The Message Text portion of the Traffic Type SYSLOG message is stored in the Firewall Traffic Log. For more information about Traffic Monitoring refer to “Vanguard Networks IP Routing Basics Manual (Part No. T0100-03)”.

```
<165>1 2010-06-17T19:20:50:52-04:00 vn3480a.vanguard.com FIREWALL - FIREWALL-548000
  [origin ip="150.30.1.50" enterpriseld=449][swVersion="V7.2.R00A (28-Jan-2010 17:07)"]
  [vnstats@449 nodeName="node101" cpuUt="30" pbuffers="3050" dbuffers="28010"]
  [vntraffic@449 TrapNumber= 548000]
  "start_time=2010-06-18 13:44:30 ingress_zone=Untrust egress_zone=Control-Plane
  policy_num=2 policy_action=Deny sent=0 recvd=0 src=150.30.7.1 dst=150.30.7.2 proto=1 icmp_type=5 icmp_code=1 reason=Creation"
```

Figure 13. Sample Traffic Monitoring SYSLOG message

**SYSLOG Message
Congestion
Control**

The SYSLOG Client feature supports one message queue for each server. If the message queue reaches the High Queue Threshold, the SYSLOG messages with Severity of 4 through 7 (Warning, Notice, Informational, and Debug) are dropped and not enqueued. The "MSG Q-Threshold Exceeded" statistic is incremented when a SYSLOG message is dropped due to the queue threshold being reached. The maximum queue size is 2000. If the maximum queue size reaches 2000, then all additional messages are dropped and not enqueued. The "MSG Q-Limit Exceeded" statistic is incremented when a SYSLOG message is dropped due the Message queue limit being exceeded.

Configuration of the SYSLOG Parameters

Introduction

To set up a Vanguard Networks SYSLOG Client feature, configure the following:

- SYSLOG Global Parameters
- SYSLOG Server Parameters
- Router (see Note)

■ **Note**

For details on configuring your node for IP Routing operation, refer to:
 Vanguard Router Basics Manual (Part No. T0100-01)
 Vanguard IP Routing Basics Manual (Part No. T0100-03)

Configuring the SYSLOG Client Feature

Follow the steps in the table below to configure the SYSLOG Client feature related parameters:

<i>Action</i>	<i>Result</i>
Select Configure (6) from the CTP Main menu.	The Configure Menu Displays

Configure Menu

Figure 14 below is a sample of Vanguard Networks Configuration Menu.

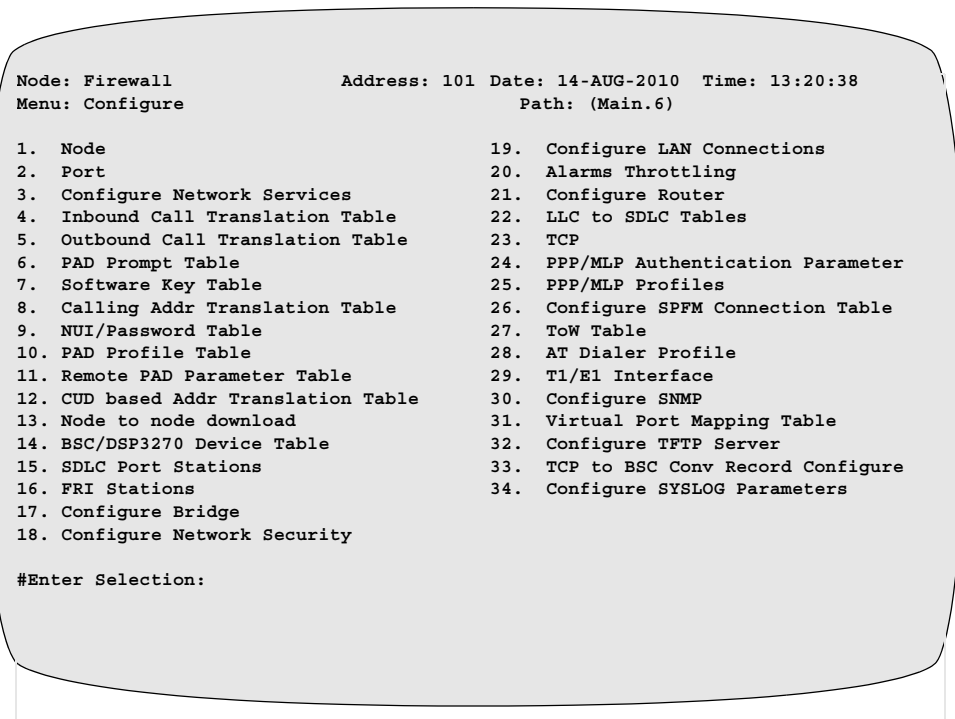


Figure 14. Typical Vanguard Networks Configuration Menu

Configuring SYSLOG Menus

Introduction

The SYSLOG Global Parameters and SYSLOG Server Parameters are required configuration for the SYSLOG Client feature to function.

Configuration

Follow these steps to configure the SYSLOG Parameters Records:

Step	Action	Result
1	Select Configure from the CTP Main menu.	The Configure menu displays.
2	Select SYSLOG Parameters from the Configure menu.	1. SYSLOG Global Parameters 2. SYSLOG Server Parameters
3	At the prompt, enter the number: 1. SYSLOG Global Parameters 2. SYSLOG Server Parameters	The SYSLOG Global Parameters and SYSLOG Server Parameters are detailed in the following sections.

SYSLOG Configure Menu

Figure 15 below shows the SYSLOG Configure Menus.

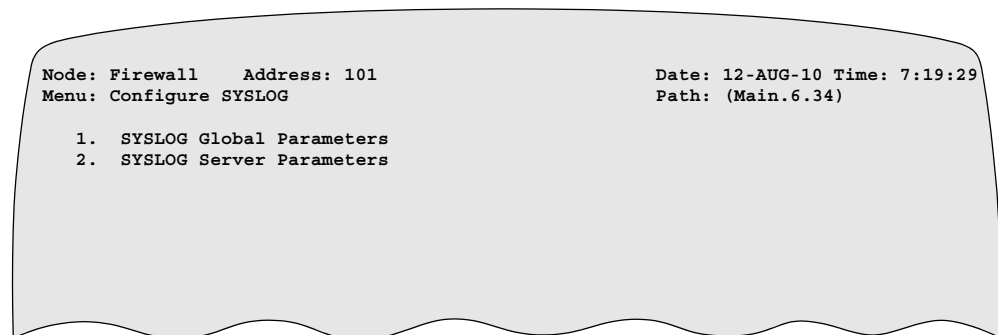


Figure 15. SYSLOG Configure Menu

SYSLOG Global Parameters Configuration

The table below describes the SYSLOG Global Parameters Configuration.

SYSLOG Global Enable

Range	ENABLED, DISABLED
Default	DISABLED
Description	Enable/Disable SYSLOG in this router. Setting this parameter to DISABLED will result in no SYSLOG Messages being sent to the SYSLOG Server(s).
Boot Effect	Booting of this parameter results in the resetting of all of the SYSLOG sessions, and could result in lost SYSLOG Messages.

SYSLOG Server Parameters Configuration

The table below describes the SYSLOG Server Parameters Configuration.

Entry Number

Range	1-2
Default	1
Description	Entry number used to reference this table record.

Enable/Disable this SYSLOG Server Connection

Range	ENABLED, DISABLED
Default	DISABLED
Description	Enable/Disable this SYSLOG Server Connection. Setting this parameter to DISABLED will result in no SYSLOG Messages being sent to the SYSLOG Server
Boot Effect	Bootting of this parameter results in the resetting of this SYSLOG session, and could result in lost SYSLOG Messages.

SYSLOG Protocol

Range	UDP
Default	UDP
Description	This SYSLOG Server Connection uses UDP.

SYSLOG Server IP Address

Range	A valid IP address in dotted notation.
Default	0.0.0.0
Description	The IP Address of the SYSLOG Server..

Server UDP Port Number

Range	256-65535
Default	514
Description	The UDP Port number of the SYSLOG Server.

SYSLOG Source Address

Range	A valid IP Address in dotted notation.
Default	0.0.0.0
Description	The Source IP Address of this UDP connection. If 0.0.0.0 is entered, the Internal IP Address in IP Router Parameters is used.

SYSLOG Traffic Type

Range	EVENT, TRAFFIC, AUTHENTICATION, ACCOUNTING.
Default	EVENT+TRAFFIC+AUTHENTICATION+ACCOUNTING
Description	The SYSLOG Type parameter selects the type of SYSLOG messages to forward across this SYSLOG Server connection: EVENT - Forward Alarm messages TRAFFIC - Forward Traffic messages AUTH - Forward Authentication messages ACCOUNTING - Forward Accounting messages Any combination of above specified by summing (e.g. EVENT+TRAFFIC+...).

SYSLOG Facility Code Override

Range	NONE, KERNEL, AUTHORIZATION, SECURITY, AUDIT, ALERT, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7.
Default	NONE

SYSLOG Facility Code Override *(continued)*

Description	This is the Facility Override value. It overrides the internally generated Facility Field of all SYSLOG Messages being sent to the SYSLOG Server.
	NONE - The Internally generated facility code is sent in the SYSLOG message. The Internally generated facility code is not overridden.
	KERNEL - A facility code of 0 is sent in the SYSLOG message.
	AUTHORIZATION - A facility code of 4 is sent in the SYSLOG message.
	SECURITY - A facility code of 10 is sent in the SYSLOG message.
	LOG_AUDIT - A facility code of 13 is sent in the SYSLOG message.
	LOG_ALERT - A facility code of 14 is sent in the SYSLOG message.
	LOCAL0 - A facility code of 16 is sent in the SYSLOG message.
	LOCAL1 - A facility code of 17 is sent in the SYSLOG message.
	LOCAL2 - A facility code of 18 is sent in the SYSLOG message.
	LOCAL3 - A facility code of 19 is sent in the SYSLOG message.
	LOCAL4 - A facility code of 20 is sent in the SYSLOG message.
	LOCAL5 - A facility code of 21 is sent in the SYSLOG message.
	LOCAL6 - A facility code of 22 is sent in the SYSLOG message.
	LOCAL7 - A facility code of 23 is sent in the SYSLOG message.

SYSLOG Severity

Range	EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORM, DEBUG
Default	EMERGENCY+ALERT+CRITICAL+ERROR+WARNING+NOTICE

SYSLOG Severity *(continued)*

Description	<p>The SYSLOG severity parameter selects the severity of the SYSLOG message to forward to the SYSLOG Server. Below are the selections with the corresponding mapping to the Logged Alarm Severity:</p> <p>EMERGENCY ALERT (HIGH) CRITICAL (MED) ERROR WARNING NOTICE (CONN) INFORM (LOW) DEBUG</p> <p>■ Note For TRAFFIC LOGGING Messages to be sent to the SYSLOG Server, you must include NOTICE in this Severity selection.</p> <p>■ Note Any combination of above may be specified by summing (e.g. EMERGENCY+ALERT+ . . .).</p>
-------------	---

SYSLOG High Queue Threshold

Range	100-1500.
Default	1500
Description	<p>The high queue threshold of the SYSLOG message queue. When this message queue threshold is reached, any new Informational and Debug messages are dropped and not sent to the SYSLOG Server.</p>

Statistics

Introduction

This section describes how to access SYSLOG Statistics.

Types of SYSLOG Statistics Menus

You can access these SYSLOG Statistics Menu Options:

- SYSLOG Server Statistics
- Reset SYSLOG Server Statistics by Server Number

Access and Reset Statistics

Follow these steps to generate and reset statistics:

Step	Action	Result
1	Select Status/Statistics for the Control Terminal Port (CTP) Main Menu.	The Status/Statistics menu displays.
2	Select SYSLOG Statistics from the Status/statistics Menu.	The SYSLOG Statistics menu displays

SYSLOG Statistics Menu

Figure 16 below shows the SYSLOG Statistics Menu.

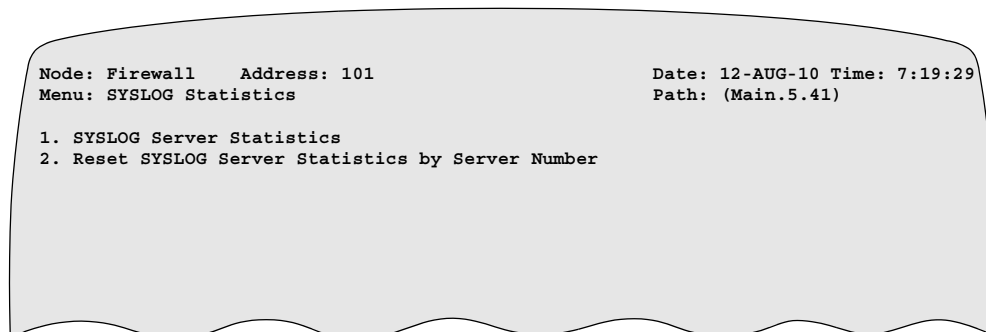


Figure 16. SYSLOG Statistics Menu

Access Server Statistics

Follow these steps to access server statistics:

Step	Action	Result
1	Select SYSLOG Server Statistics from the SYSLOG Statistics Menu.	The SYSLOG Server Number displays.
2	Select the SYSLOG Server Number: 1-2 .	The Detailed SYSLOG Statistics menu displays

**Detailed SYSLOG
Server Statistics
Menu**

Figure 17 below shows the Detailed SYSLOG Statistics Menu.

```

Node: Firewall      Address: 101          Date: 28-JUN-2010  Time: 15:19:11
Detailed SYSLOG Server Statistics:      Server Number 1      Page: 1 of 1

Connection Type:      UDP          Current State: ACTIVE
Server IP Address:    150.30.1.50      Server Port: 514
Local IP Address:     150.30.1.51          Local Port: 1025

Last Statistics Reset: 28-JUN-2010 14:02:21

Total Messages Sent:      11          Total Messages Dropped:      0
Traffic Messages Sent:    0          MSG Q-Threshold Exceeded:    0
Event Messages Sent:     10         MSG Q-Limit Exceeded:       0
Auth Messages Sent:       1          Out of Buffer Errors:        0
Accounting Messages Sent: 0          Out of Memory Errors:       0
Total Transmitted Bytes:  4304       Length Errors:               0
                                         UDP Socket Errors:          0

Current MSG Queue Size:   0          MAX MSG Queue Size:         9
                                         at 28-JUN-2010 14:02:45
    
```

Figure 17. Detailed SYSLOG Server Statistics Menu

Description of Terms

Screen Term	Description
Accounting Messages Sent	Total number of Accounting Type SYSLOG Messages sent
Auth Messages Sent	Total number of Authentication Type SYSLOG Messages sent
Connection Type	MAC Address of the station whose address was placed in the table
Current MSG Queue Size	The current size of the SYSLOG message queue
Current State	Status of the entry: Learned, Local.
Event Messages Sent	Total number of Event Type SYSLOG Messages sent
Length Errors	Total number of messages dropped because the messages exceeded the available buffer's size.
Local IP Address	IP Address of the SYSLOG Client
Local Port	IP Address of the LOCAL Port
MAX MSG Queue Size	The maximum size of the SYSLOG message queue
MSG Q-Limit Exceeded	Number of messages dropped due to Message Queue is Full
MSG Q-Threshold Exceeded	Number of messages dropped due to Message Queue Threshold is exceeded
Out of Buffer Errors	Total number of messages dropped due to an out of packet buffer condition
Out of Memory Errors	Total number of messages dropped to to an out of memory condition.
Server IP Address	IP Address of the SYSLOG Server
Server Port	UDP Port Number of the SYSLOG Server
Time of MAX MSG Queue Size	The time that the message queue hit its max size.
Total Messages Dropped	Total Number of SYSLOG Messages dropped due to errors
Total Messages Sent	Total Number of SYSLOG Messages sent to the SYSLOG Server
Total Transmitted Bytes	Total number of bytes transmitted in the form of SYSLOG Messages to the SYSLOG Server.
Traffic Messages Sent	Total Number of Traffic Monitoring messages sent
UDP Socket Errors	Total number of messages dropped because the socket to UDP was disconnected.

SYSLOG Boot Menu

Figure 18 below shows the SYSLOG Boot Menu.

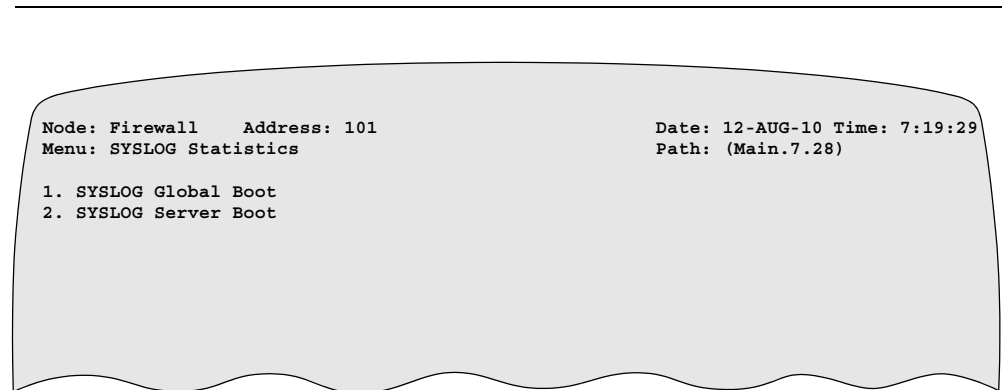


Figure 18. SYSLOG Boot Menu

SYSLOG Global Boot Description

The SYSLOG Global Boot activates the Global and Servers' SYSLOG Parameters and restarts all of the SYSLOG Servers. Note that Booting may result in lost SYSLOG messages.

SYSLOG Server Boot Description

The SYSLOG Server Boot activates the SYSLOG Server's Parameters and restarts the SYSLOG Server. Note that Booting may result in lost SYSLOG messages.

SYSLOG Configuration Examples

Basic SYSLOG Configuration Example

Figure 19 shows a basic SYSLOG Configuration Example. In this example, the 3460 is connected to the Kiwi SYSLOG server through an IP Connection via the 3460's Ethernet Port 23.

In the Node Record, the "Configuration Change Alarm" parameter is set to Enabled to allow configuration change alarms to be logged to the alarm log and to allow configuration change alarms to be forwarded to the SYSLOG server. Also, in Figure 21, the "SYSLOG Global Enable" is set to ENABLED, and the SYSLOG Server Parameters for Server 1, are configured such that the SYSLOG Messages are sent to the Kiwi SYSLOG Server (UDP Port 514, IP Address 172.16.1.253).

All SYSLOG Message Types (Event, Traffic, Authentication, and Accounting) are being sent to the SYSLOG Server. Only SYSLOG Messages of the following severities are forwarded to the SYSLOG Server: EMERGENCY, ALERT, CRITICAL, and ERROR. Because the "SYSLOG Source Address", in the "SYSLOG Server Parameters", is set to 0.0.0.0, the "Internal IP Address" in the "IP Parameters" configuration is used for the SYSLOG Source Address for the UDP connection to the Kiwi SYSLOG server.

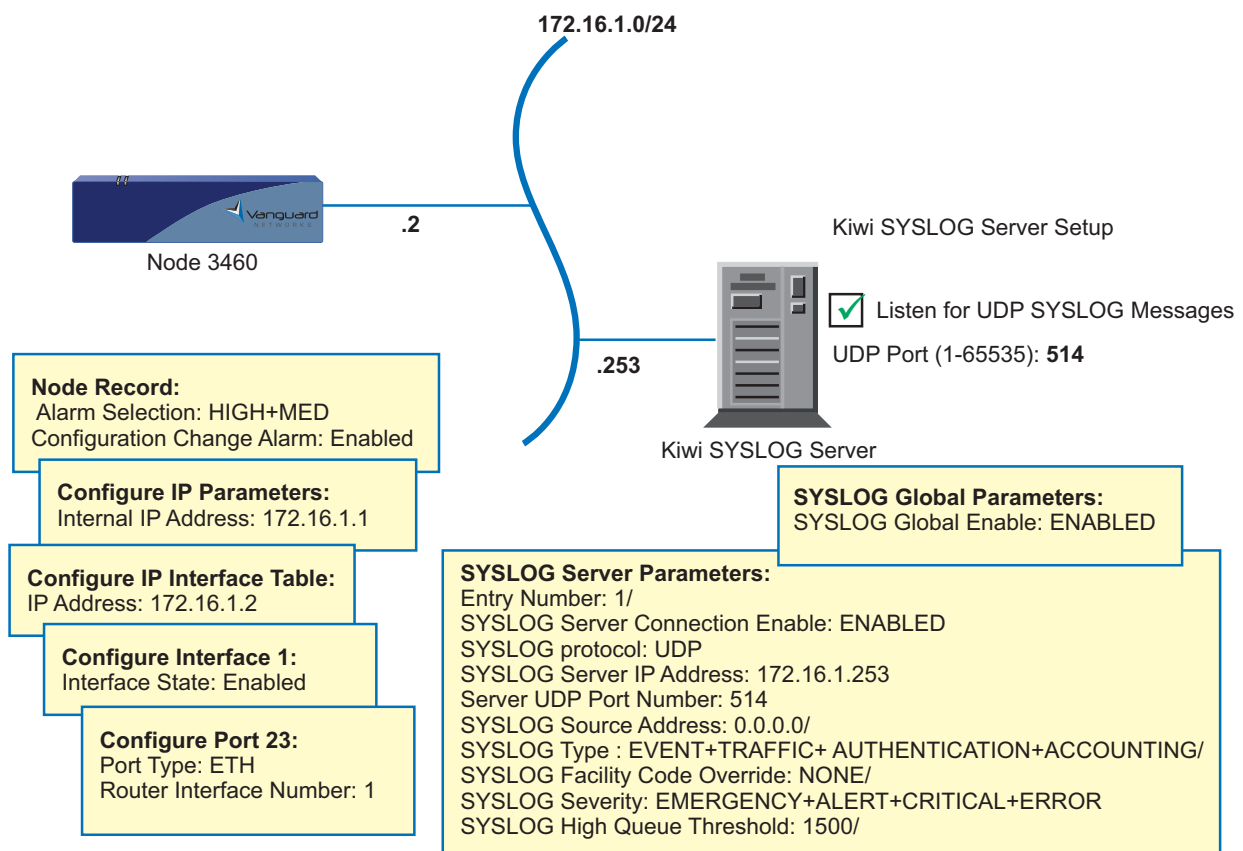


Figure 19. SYSLOG Basic Configuration Example

**Traffic Logging
SYSLOG
Configuration
Example**

Figure 20 shows an example of SYSLOG application where Traffic Logging is enabled in the Firewall Policies.

In this example, the "Firewall State" in the "Firewall Global Parameters", is ENABLED, and the "Traffic Logging" parameter in the "Firewall Policy" Configuration is set to "START+END". In addition, the SYSLOG Severity is configured for "NOTICE". The Firewall Monitor Events that are logged to the Firewall Log are sent in a SYSLOG Message to the SYSLOG server with this configuration.

SYSLOG Configuration Examples

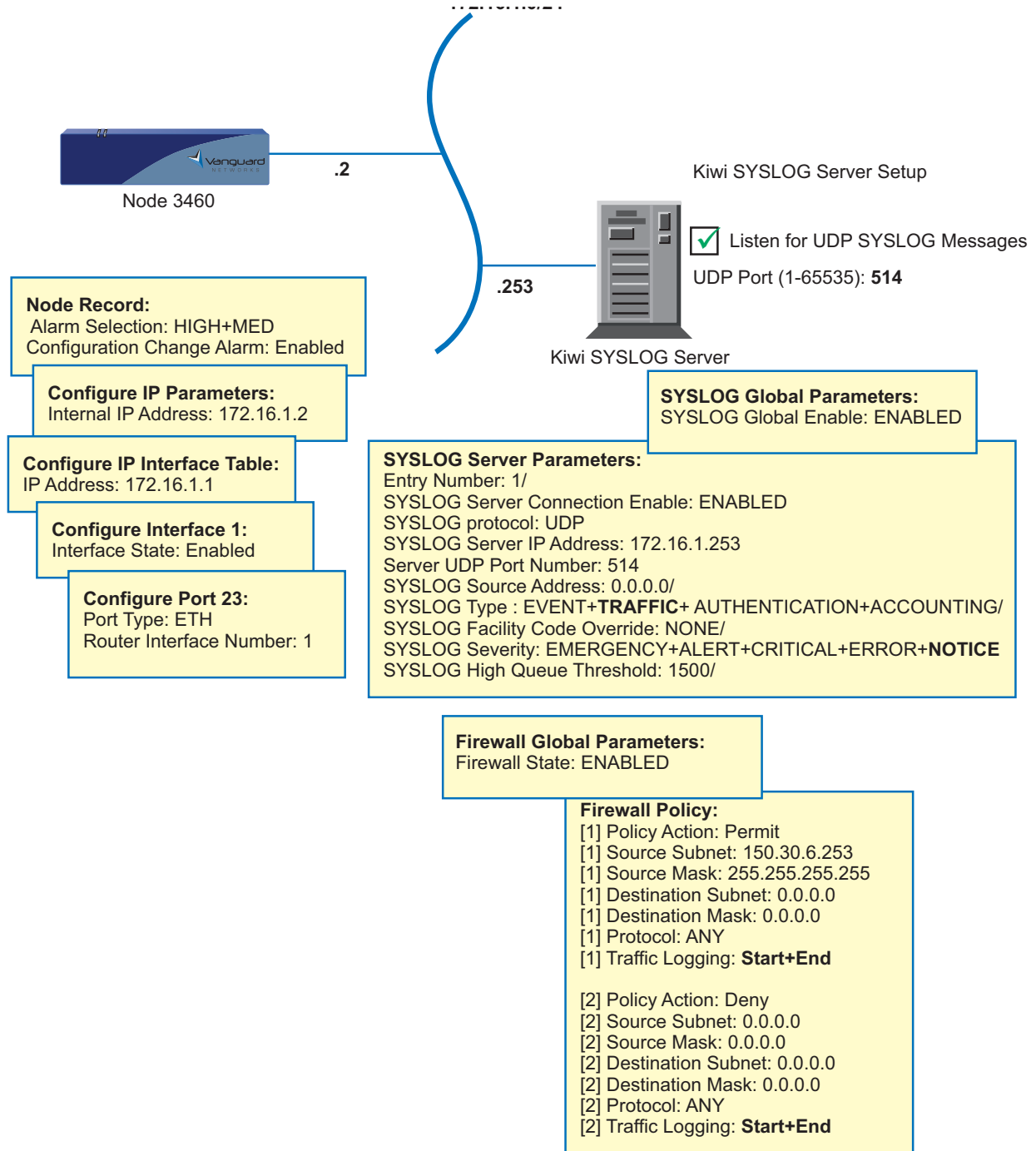


Figure 20. Traffic Logging SYSLOG Configuration Example

A

Accounting Type Message [1-14](#)
Alarm Throttling [1-9](#)
Application of the Vanguard Networks SYSLOG Client
 Feature [1-2](#)
Appliction of Vanguard Networks SYSLOG Client
 Feature [1-2](#)
Authorization Type Message [1-13](#)

B

Basic Configuration Example [1-26](#)
Boot Menu [1-25](#)

C

Configuration Examples [1-26](#)
Configuration Parameters [1-16](#)
Configure Menu [1-16](#)
Configuring SYSLOG Menus [1-17](#)

D

Description of Terms [1-24](#)
Detailed Server Statistics Menu [1-23](#)

E

Event Type Message [1-13](#)

F

Facility Code Setting [1-8](#)
Filtering SYSLOG Messages Based on Severity [1-8](#)

G

Global Parameters Configuration [1-17](#)

I

IANA-defined Structured Data Field [1-11](#)
Introduction to SYSLOG [1-2](#)

M

Message Congestion Control [1-15](#)
Message Details [1-5](#)
Message Format [1-5](#)
Message Header [1-6](#)
Message Header Example [1-10](#)
Message Text Field [1-12](#)
Message Types [1-3](#)

O

Overview [1-1](#)

P

Private Structured Data Field [1-11](#)

S

Server Parameters Configuration [1-18](#)
Server Statistics [1-22](#)
Severity Level [1-9](#)
Statistics [1-22](#)
Statistics Menu [1-22](#)
Supported Facility Codes [1-7](#)
Supported Severity Codes [1-8](#)
SYSLOG Messages [1-13](#)

T

Theory of Operation [1-4](#)
Traffic Logging Configuration Example [1-27](#)
Traffic Monitor Message [1-14](#)