



---

# Vanguard Applications Ware Basic Protocols

## SNMP/MIB Management

# Notice

---

©2008 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Unpublished - rights reserved under the copyright laws of the United States.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 Networks. (or its Suppliers) and without the express prior permission of an officer of Vanguard Networks, 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 Vanguard Networks Software License Agreement.

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

Part No. T0106-04, Rev J

Publication Code: TK

First Printing: November 1998

Manual is current for Release 7.3 of Vanguard Applications Ware.

To comment on this manual, please send e-mail to [vntechsupport@vanguardnetworks.com](mailto:vntechsupport@vanguardnetworks.com)



## Contents (continued)

---

How SNMP Works .....	2
How Vanguard Implements SNMP .....	4
Network Access Products MIB .....	6
Syntax and Access Categories for MIB Objects .....	8
Supported RFCs for Vanguard Networks MIBs .....	11
Connecting to an SNMP Management System .....	13
Configuring the SNMP Agent Module .....	14
SNMP Agent Record Parameters .....	16
Configuring the SNMP Communities Record .....	19
SNMP Communities Record Parameters .....	20
Configuring the SNMPv3 Agent .....	22
SNMPv3 Configuration Examples .....	34
Viewing SNMP Statistics .....	37
Resetting SNMP Agent Statistics .....	42
Trap Throttling .....	43
Changing Priority .....	45
V.54 Loopback Test Using SNMP .....	48
SNMP Agent Table Worksheets .....	50
SNMP Communities Table Worksheet .....	51

**Contents (continued)**

---

# Simple Network Management Protocol

---

## Overview

### Introduction

This manual describes the Simple Network Management Protocol (SNMP) and the Management Information Database (MIB) as implemented for Vanguard products.

### About SNMP

SNMP is the standard connectionless Internet protocol used to manage networks. SNMP lets network management stations monitor SNMP-manageable devices such as Vanguard products in a network regardless of device vendor and manufacturer. SNMP is transported over UDP/IP.

### Related Documentation

You should also familiarize yourself with these Applications Ware documents:

- *Vanguard Basic Configuration Manual* (Part Number T0113)
- *IP and LAN Feature Protocols Manual* (Part Number T0100)

### In This Manual

Topic	See Page
How SNMP Works .....	2
How Vanguard Implements SNMP .....	4
Network Access Products MIB .....	6
Syntax and Access Categories for MIB Objects .....	8
Supported RFCs for Vanguard Networks MIBs .....	11
Connecting to an SNMP Management System .....	13
Configuring the SNMP Agent Module .....	14
SNMP Agent Record Parameters .....	16
Configuring the SNMP Communities Record .....	19
SNMP Communities Record Parameters .....	20
Configuring the SNMPv3 Agent .....	22
SNMPv3 Configuration Examples .....	34
Viewing SNMP Statistics .....	37
Resetting SNMP Agent Statistics .....	42
Trap Throttling .....	43
Changing Priority .....	45
V.54 Loopback Test Using SNMP .....	48
SNMP Agent Table Worksheets .....	50
SNMP Communities Table Worksheet .....	51

## How SNMP Works

### Components

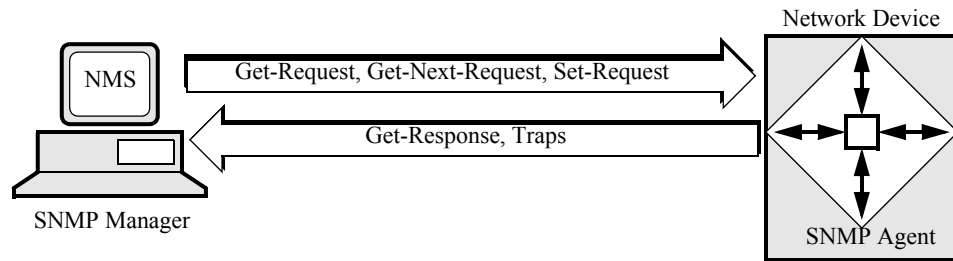
SNMP is made up of three components:

<b>Component</b>	<b>Description</b>
Manager	A network management system workstation that network devices respond and report to.
Agent	Software residing in a device such as a Vanguard that answers requests from the SNMP manager.
Management Information Base (MIB)	A database repository for information about device parameters and network data. There is a MIB for both the Agent and the Manager.

Refer to the “How Vanguard Implements SNMP” section on page 4 for more details on how Vanguard Networks implements SNMP for device management.

### How SNMP Works

SNMP uses Protocol Data Units (PDUs) to send requests and responses between managers and agents to exchange MIB information, as shown in Figure 1.



**Figure 1. SNMP Operations Between Manager and Agent**

A manager uses such requests to get a MIB value from an agent or store a value into an agent. An agent generates unsolicited traps or sends get-responses to manager requests.

### About PDUs

SNMP uses the following five Protocol Data Units to send requests and responses.

<b>Type of PDU</b>	<b>Function</b>
GetRequest	Retrieves a value from a specific MIB object.
GetNextRequest	Retrieves a series of values from a group until all objects in the group are retrieved.
SetRequest	Alters a value in a specific MIB object.
GetResponse	Replies to a <i>GetRequest</i> , <i>GetNext</i> , or <i>SetRequest</i> sent by the Network Management System (NMS).
traps	An unsolicited message sent by an SNMP agent to an SNMP manager indicating that some event has occurred.

---

**PDU Encoding**

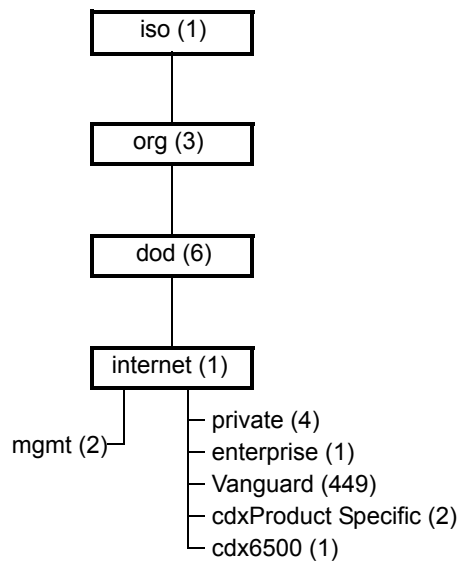
PDU's are encoded according to the Abstract Syntax Notation (ASN.1) Basic Encoding Rules (BER).

---

**Internet-Standard MIB Hierarchy**

The MIB structure is logically represented by a tree structure, beginning with the root, International Organization for Standardization (ISO).

Figure 2 shows an overview of the Internet-standard MIB hierarchy.



**Figure 2. Top Levels of the MIB Hierarchy**

---

**Object Names and Identifiers**

Branches beneath the ISO root have short text strings called *group names* to help you identify them.

Numeric labels called *object identifiers* identify the path between the root and the object.

---

## How Vanguard Implements SNMP

---

### Introduction

The Vanguard implementation of SNMP lets you view many of the statistics and configuration parameters for your Vanguard networking device.

To use an SNMP NMS to manage Vanguard networking devices, you must have the following software components:

- SNMP Agent
- Device MIB
- Management MIB

---

### SNMP Agents

A Vanguard must contain an SNMP Agent before you can manage it from an SNMP manager. SNMP Agents consist of one or more software programs that run inside a network device. It is the SNMP Agent's job to:

- Handle any incoming and outgoing SNMP messages.
- Forward SNMP traps to designated management workstations.
- Control the Device MIB.
- Provide an interface between the network device's operating software and the network management workstation(s).

---

### Device MIBs

Having an SNMP Agent alone does not make a device SNMP compliant. It must also have a Device Management Information Base (MIB) which:

- Contains a list of device parameters called "objects."
- Provides a road map used by the SNMP Agent to locate configuration, testing, and statistical collection objects within the network device.

---

### Management MIB

Your SNMP NMS must contain a Management MIB which:

- Contains a compiled image of all device MIBs it is currently managing
- Is automatically recompiled upon loading of the Vanguard Applications Ware SNMP Module.

---

### How the Vanguard Uses MIBs

The SNMP agent and MIB files are customized for each Vanguard product. Only those MIB objects for features present in the software image option loaded on the Vanguard are included. This means the code size for the SNMP agent module is significantly reduced.

---

### How MIBs Are Updated

The SNMP agent module and MIB files are automatically updated when you load new operating software (containing software image options) into a Vanguard device. This means updated MIB files are included in each new release of the operating software for Vanguard devices.

---

## SNMP Support

The Vanguard MIB files let you control and monitor your network nodes from an SNMP network manager.

This means you can control SETs on some parameters.

Applications Ware SET PDUs let you invoke controls and actions such as node boots, port boots, and station resets. Most objects allow for control GETs for device monitoring.

---

## SNMP Security

Vanguard Applications Ware security is based on the SNMP “community name,” which is passed in the PDU as part of the general SNMP header. The name is used to verify that the manager requesting the information or action is authorized to do so. Authorization for SETs and GETs can be done using a single community name.



### Caution

It is strongly recommended that independent community names be used for private networks.

---

## Trap Generation and Filtering

Community name configuration is also used to generate traps. You can also filter traps by changing a trap’s severity level. You can configure each device to send trap messages to up to 10 separate SNMP managers, with one community name.

Trap filtering is also allowed at the community level. Trap filtering is based on the same criteria as Control Terminal Port events and alarms.

Trap levels are High, Medium, Low, Connection, and Code. You can also send duplicate traps to another SNMP manager on a different community by configuring the manager under a different community name.

The SNMP agent on Vanguard products can be configured to throttle repetitive traps. This allows the node to generate only a specific number of traps over a specified time interval. Throttling repetitive traps helps reduce network congestion.

---

## Network Access Products MIB

### Introduction

The Vanguard Networks Network Access Products MIB for Vanguard consists of a set of MIB objects, also called primary objects, that are private extensions of the Internet branch.

MIB objects are the specific values stored in the groups within the MIB files. MIB objects can be read through get-requests to provide information on network devices and interfaces.

### MIB Extensions

Figure 3 depicts the Vanguard Networks products private enterprise MIB extensions for Vanguard.

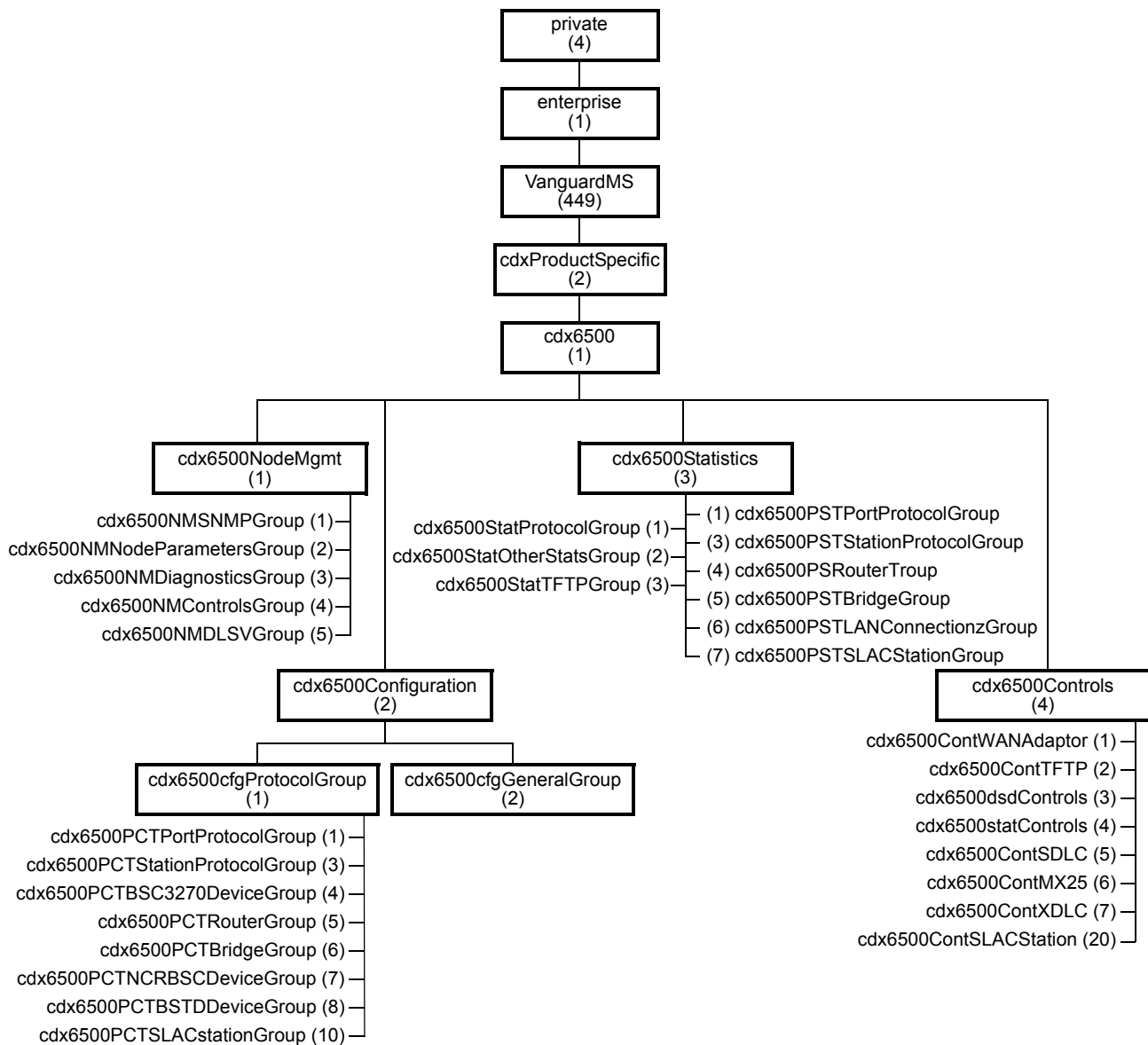


Figure 3. MIB Group Hierarchy

---

**Object Identifier for a MIB** The object identifier for the Vanguard Networks private enterprise MIB is rooted at 1.3.6.1.4.1.449.2.1, or *iso.org.dod.internet.private.enterprisecdxProductSpecific.cdx6500*. Refer to Figure 3 for an illustration of this string.

---

**How You Use a MIB** Basically, a MIB is used for SNMP management of your networking devices. The MIB enables you to use SNMP to manage a device in your network in any of the following ways:

<b>Management area</b>	<b>Involves...</b>
Configuration	monitoring and controlling the configuration of network devices
Performance	measurement of traffic flow across the network, calculating the number of packets that are successfully transmitted against those that are dropped to optimize efficiency
Fault	running diagnostic tests on the network, analyzing the results, and isolating and resolving problems
Security	controlling access to network resources through the use of authentication techniques and authorization policies

---

## Syntax and Access Categories for MIB Objects

### Introduction

This section describes the syntax and access categories used to explain each MIB object within the Vanguard MIB.

### Syntax in Relation to MIB Objects

The syntax describes the format in which the information, or value, is presented after a request for information is issued to a device with a MIB object.

### SNMP Display of Hex or ASCII Data

Most SNMP objects are represented using the syntax type OCTET STRING. Generally, an SNMP manager application does not know whether an octet string should be displayed in hexadecimal or as ASCII characters.

The Vanguard Networks 9000-UX SNMP manager uses the following algorithm to determine the display of characters:

- If all bytes are printable ASCII characters, the octet string is printed as an ASCII string.
- If any byte is a non-printing character, the octet is printed as a hexadecimal.

Therefore, the output of an SNMP manager may appear in an unexpected format. For example, a MAC address that happens to contain bytes that are all ASCII characters is printed in ASCII, not hexadecimal.

### Syntax Format

This table describes syntax format types:

<i>Name</i>	<i>Type</i>	<i>Description</i>
Counter	non-negative integer	increases until it reaches some maximum value; then it rolls back to zero
Display String	printable ASCII string	typically a name or description
Integer	numeric value	an actual number, for example, the clock speed on an interface; an arbitrary number that represents a non-numeric value
Network Address		represents an address for an interface or device
Object Identifier		sequence of numeric labels on the nodes along a path from the root to the object
TimeTicks	non-negative integer	counts hundredths of a second since an event

**Examples**

<i>MIB Object</i>	<i>Syntax Format</i>	<i>indicates...</i>
cdx6500frdtepCharinTotal	Counter	the number of characters received since the last boot or statistics reset
cdx6500dsdDropRemoteAddr	Display String	the statistics parameter for the DSD option subchannel remote address

**Object Access**

This table identifies the classifications of access modes of MIB objects:

<i>A MIB Object classified as...</i>	<i>...can be used to...</i>
Read-only	monitor information only
Read/Write	monitor information and set a new value for the MIB object as well
Write-only	set a new value for the MIB object

**Community Name Access**

SNMP operations are allowed based on the access privileges granted by the community name and by the MIB-object access modes. These operations are permitted:

<i>Type</i>	<i>MIB Object Access Mode</i>			
	<i>Not Accessible</i>	<i>READ ONLY</i>	<i>READ/WRITE</i>	<i>WRITE ONLY</i>
<i>Community Access Privileges</i>				
READ ONLY	None	GET, GET-NEXT	GET, GET-NEXT	None
READ WRITE	None	GET, GET-NEXT	GET, GET-NEXT, SET	SET

---

**SNMP SET**

The SNMP Set function allows you to change the values of MIB object variables. The SNMP Set function:

- Resides in each node of a network that serves as an SNMP agent.
- Allows an SNMP manager to change the values of MIB object variables through an SNMP Set request to the host agent.
- Changes the values of MIB object variables that have Read/Write access. MIB object variables that have Read-only access cannot be changed using SNMP Set.
- Requires that the SNMP Communities Record ACCESS privileges are set to READ WRITE.
- Requires that SNMP Agent parameter, SNMP Set Control is set to ON.

**Supported Read/Write Vanguard MIBs**

Objects within the following Vanguard MIBs have Read/Write access:

- bridge.mib
- cdx.mib
- eth.mib
- frdte.mib
- fri.mib
- isdn.mib
- pad.mib
- router.mib
- x25.mib

---

**Additional Syntax Details**

Refer to RFC 1155 and RFC 1212 for additional details on syntax.

---

## Supported RFCs for Vanguard Networks MIBs

### List of RFCs

Vanguard MIB files adhere to these Request For Comments (RFCs):

<b>RFC</b>	<b>Title</b>	<b>Description</b>
RFC 1155	<i>Structure and Identification of Management Information for TCP/IP-based Internets</i> , May 1990	Describes the common structures and identification scheme for the definition of management information for use with TCP/IP-based internets. Formal structure descriptions are given using Abstract Syntax Notation One (ASN.1). Refer to ISO Standards 8824 and 8825 for a description of ASN.1 and its basic encoding rules.
RFC 1157	<i>A Simple Network Management Protocol (SNMP)</i> , May 1990	Describes the SNMP architecture and supported operations.
RFC 1212	<i>Concise MIB Definitions</i> , March 1991	Describes the format for producing concise and descriptive MIB modules.
RFC 1213	<i>Management Information Base for Network Management of TCP/IP-based Internets: MIB-II</i> , March 1991	This RFC describes the Internet standard MIB II for use with network management protocols in TCP/IP-based internets. <b>■Note</b> Applications Ware Release 5.2 and after offers the following enhancements to this RFC: <ul style="list-style-type: none"> <li>• The return value of the ifDescr variable includes the physical port number in the string. Therefore, for example, if you configure physical port 26 as FRI, and its associated ifIndex is 7, the corresponding entry in the ifDescr table looks as follows: ifDescr.7 = "Port_26, FRI /6520 Router Node." The return value for the ifDescr object takes the format: ifDescr.ifIndex : Port_&lt;Number&gt;,&lt;Port Type&gt;/VanguardMS/Product Name ifDescr.ifIndex : LCON_&lt;Number&gt;, /VanguardMS/Product Name</li> <li>• This enhancement is only available for the following interface types: X.25, Frame Relay, Ethernet, MX25, Token Ring, BRI/PRI, T1/E1, SDLC, XDLC, and LCONs.</li> <li>• The return value of the ifOperStatus object conforms to its definition in RFC 1213. Therefore, the possible return values are only up(1), down(2), or test(3). The correspondence between the ifOperStatus object in RFC 1213 and the state of the physical interface as shown on the CTP is described in the table following this RFC list.</li> </ul>

<b>RFC</b>	<b>Title</b>	<b>Description (continued)</b>
RFC 1231	<i>IEEE 802.5 Token Ring MIB, May 1991</i>	Describes the managed objects used for managing subnetworks which use the IEEE 802.5 Token Ring technology.
RFC 1286	<i>Definitions of Managed Objects for Bridges, December 1991</i>	Describes the supported objects in all types of bridges.
RFC 1315	<i>Management Information Base for Frame Relay DTEs, April 1992</i>	Describes support of MIB-II Frame Relay Management Information objects to accommodate Frame Relay DTE.  <b>■Note</b> There is one known limitation, where no set operation is supported on six read-write objects in the following range: 1.3.6.1.2.1.10.32.1.1.3 to 1.3.6.1.2.1.10.32.1.1.8.
RFC 1398	<i>Definitions of Managed Objects for the Ethernet-like Interface Types, January 1993</i>	Describes the MIB for use with network management protocols in TCP/IP-based internets along with the objects for managing Ethernet-like objects.
RFC 1850	<i>OSPF Version 2 Management Information Base, November 1995</i>	Describes objects for managing the Open Shortest Path First Routing Protocol.

**RFC 1213  
ifOperStatus  
Correspondence  
With Physical  
Interface**

The following table lists the correspondence between the RFC 1213 ifOperStatus object and the physical interface as shown on the CTP.

<b>Port Type</b>	<b>CTP</b>	<b>ifOperStatus</b>
X.25, MX25	Up	Up
XDLC, SDLC	Down, Disabled, Busyout	Down
	Anything Else	Test
FRI, Ethernet	Enabled	Up
TR, BRI, T1, E1	Disabled	Down
	Anything Else	Test
LCONs	Connected	Up
	Not Connected	Down
	Awaiting Call, Calling, Etc.	Test

**How to Get a Copy  
of the MIB**

MIB files are included in the Vanguard Applications Ware. When you obtain new operating software for Vanguard products, the SNMP agent and the MIB files are automatically updated in the device.

Operating software containing MIB files is also available from the Vanguide CD-ROM, which accompanies most Vanguard products.

## Connecting to an SNMP Management System

### What You Must Configure

---

Many different ways exist to configure a Vanguard product node for connection to an SNMP network management system. Configure the following records and tables in the Vanguard node before you manage the device from a network manager:

- Software Authorization Key (Vanguard Applications Ware Release 5.2 and earlier)
- Physical LAN Port
- Router interfaces
- IP addresses and masks
- Routing parameters
- General IP parameters
- IP router configuration options
- LAN/WAN interconnection table
- IP router configuration parameters
- SNMP Agent
- SNMP Communities

### Connecting

---

Depending on how you want to connect a node to an SNMP management system, you can configure some or all of these parameters to suit your network's needs.

Refer to the *IP and LAN Feature Protocols Manual* (Part Number T0100) and *Vanguard Basic Configuration Manual* (Part Number T0113).

Refer to the “Configuring the SNMP Agent Module” section on page 14 and the “Configuring the SNMP Communities Record” section on page 19 for details on SNMP-specific procedures.

---

## Configuring the SNMP Agent Module

### Introduction

These SNMP Agent records must be configured in your Vanguard:

- the SNMP Agent record
- the SNMP Communities record

**Note**

Configuring Trap Throttling parameters is optional.

### Before You Begin

Consider the following guidelines before you configure your Vanguard for SNMP management:

- The SNMP-UDP connection Subaddress in the SNMP Agent menu should remain at the default of 161 unless there are specific network requirements.
- If there is a lot of activity at initialization time, you may enter a UDP Retry Timer time period larger than the 120-second default value. Increasing this time period reduces the number of registration request time-outs. This parameter is under the SNMP Agent menu.
- You can configure up to 10 SNMP communities, with up to 10 SNMP managers per community.
- You can include an SNMP manager in more than one community.

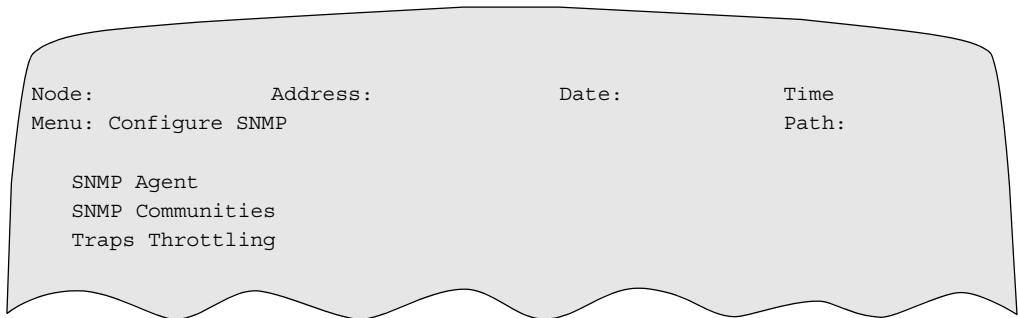
### SNMP Agent Record

This record allows you to configure the SNMP agent resident within the operating software for your Vanguard. Follow these steps to configure the SNMP agent for the node.

<b>Step</b>	<b>Action</b>	<b>Result</b>
1	Select <b>Configure-&gt;SNMP</b> from the Main CTP menu.	The Configure SMNP menu appears as shown in Figure 4.
2	Select <b>SNMP Agent</b> from the Configure SNMP menu to access the menu parameters available for configuring the SNMP Agent.	The SNMP Agent Record and its parameters appear as shown in Figure 5. A prompt appears asking you to configure the next parameter.

**Configure SNMP Menu**

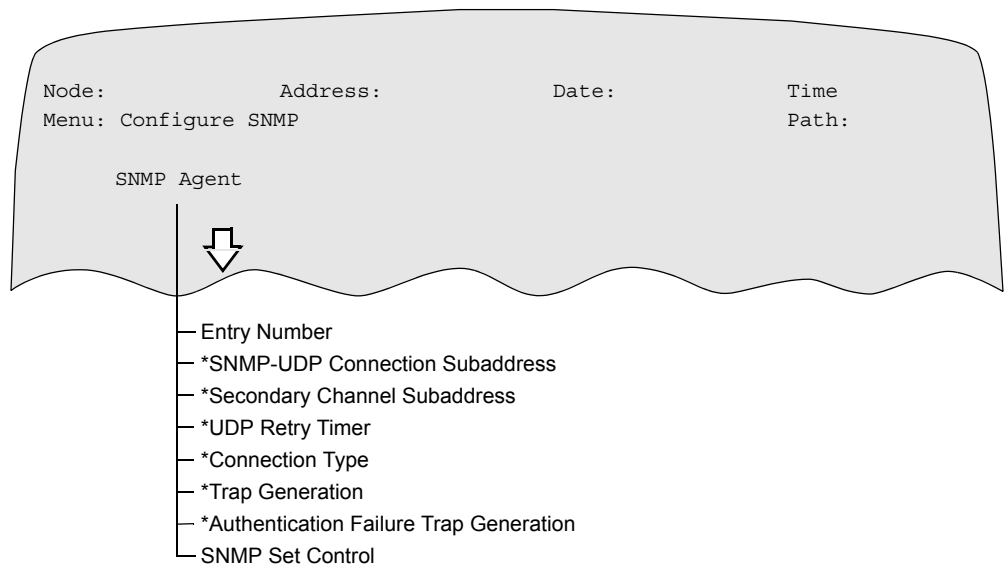
Figure 4 shows the Configure SNMP menu.



**Figure 4. Configure SNMP menu**

**What You See in the SNMP Agent Record**

Figure 5 shows the parameters available from the SNMP Agent Record. Refer to the “SNMP Agent Record Parameters” section on page 16 for details on these parameters.



**Figure 5. SNMP Agent Record**

## SNMP Agent Record Parameters

### Parameters

You can configure these parameters from the SNMP Agent Record:

#### Entry Number

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

#### SNMP-UDP Connection Subaddress

Range:	0 to 3 decimal digits
Default:	161
Description:	This is the UDP port registration number. This indicates to the UDP protocol which port SNMP uses to register.  <b>■ Note</b> Perform a node boot for changes to this parameter to take effect.

#### Secondary Channel Subaddress

Range:	0 to 3 decimal digits
Default:	(blank)
Description:	Enter the Secondary Subaddress of the agent. Use the space bar to blank this field.  <b>■ Note</b> Perform a node boot for changes to this parameter to take effect.

#### UDP Retry Timer (seconds)

Range:	1 to 255 seconds
Default:	120
Description:	Indicates the number of seconds between registration attempts.  <b>■ Note</b> Perform a node boot for changes to this parameter to take effect.

### Connection Type

Range:	APAD, UDP, SIP_L, SIP_W
Default:	UDP
Description:	<p>Type of port that is connected to the SNMP Agent.</p> <ul style="list-style-type: none"> <li>• APAD: Used for a PAD connection</li> <li>• UDP: Used for a UDP connection</li> <li>• SIP_L: Used to force LAN packets for saving conversions.</li> <li>• SIP_W: Used to force WAN packets for saving conversions.</li> </ul> <p><b>■ Note</b> Perform a node boot for changes to this parameter to take effect.</p>

### Trap Generation

Range:	Disabled, Enabled
Default:	Disabled
Description:	<p>Determines whether the Vanguard generates normal SNMP traps. This must be enabled to generate traps.</p> <p><b>■ Note</b> Perform a node boot for changes to this parameter to take effect.</p>

### Authentication Failure Trap Generation

Range:	Disabled, Enabled
Default:	Disabled
Description:	<p>Determines if the Vanguard generates an authentication failure trap. This trap is generated if an SNMP manager that is not from a registered community or which does not have the correct privileges tries to gain access to the node's network management database. Menu choices for this record include:</p> <ul style="list-style-type: none"> <li>• Configure</li> <li>• List</li> <li>• Examine</li> <li>• Delete</li> </ul> <p>Specify Enabled to generate an authentication failure trap.</p> <p><b>■ Note</b> Perform a node boot for changes to this parameter to take effect.</p>

### Trap Type

Range:	RFC, ENTERPRISE_SPECIFIC
Default:	RFC
Description:	<p>Specifies the trap type:</p> <p>RFC: The node generates generic traps according to the RFC. All other traps are generated as enterprise specific.</p> <p>ENTERPRISE_SPECIFIC: The node generates all traps as enterprise specific.</p> <p>This function is applicable only when generic traps are generated and there exists a corresponding enterprise specific trap. Enterprise specific traps contain text descriptions.</p> <p><b>Note</b> Perform a table and node record boot for changes to this parameter to take effect.</p>

### SNMP Set Control

Range:	ON, OFF
Default:	OFF
Description:	<p>Specifies the ON/OFF flag for SNMP Set operation:</p> <p>ON: Enables SNMP Set operation.</p> <p>OFF: Disables SNMP Set operation.</p> <p>This parameter enables the SNMP Set function. It allows SNMP management software to change object variables that have Read/Write access in the MIB files.</p> <p><b>Note</b> The ACCESS privileges parameters in the SNMP Communities Record Parameters must be set to READ WRITE to use this function.</p>

## Configuring the SNMP Communities Record

**Introduction** You can configure up to 10 SNMP communities, including up to 10 SNMP managers per SNMP community.

**Function** Through the SNMP Communities record, you can:

- configure SNMP communities by name.
- list the SNMP managers that comprise the community.
- define Access Privileges and Trap Category associated with the community.

**Identifying Existing Community Name** To learn which community names already exist, select List from the main menu.

**Changing a Community Name** You can change a community name:

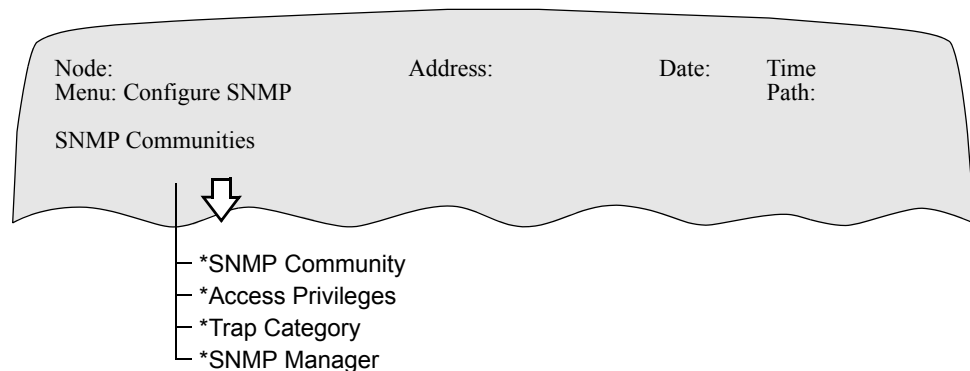
- by overwriting the existing record.
- by entering a new community. The entry 0.0.0.0 matches any IP address.

**Configuring the SNMP Communities Record** Follow these steps to configure the SNMP Communities record for your Vanguard.

Step	Action	Result
1	From the Main CTP menu, select <b>Configure-&gt;SNMP</b> .	The Configure SMNP menu appears as shown in Figure 4.
2	Select <b>SNMP Communities</b> from the Configure SNMP menu to access the menu parameters available for configuring the SNMP Communities Record.	The SNMP Communities Record and its parameters appear as shown in Figure 6. A prompt appears asking you to configure the next parameter.

**What You See In The SNMP Communities Record**

Figure 6 shows the parameters in the SNMP Communities Record.



**Figure 6. SNMP Communities Record**

## SNMP Communities Record Parameters

### Parameters

You can configure the following parameters from the SNMP Communities Record:

**■ Note**

Unless otherwise indicated, you must perform a node boot for changes to these parameters to take effect.

### SNMP Communities

Range:	1 to 16 alphanumeric characters (use the space bar to blank the field).
Default:	(blank) (Enter a valid name here.)
Description:	<p>Specifies an SNMP community name used for authenticating an SNMP request.</p> <p>This community name is either the name of the current record, or it can be used to enter a new name, establishing a new record.</p> <p><b>■ Note</b> Duplicate community names are not allowed. Duplicate IP addresses within the community are not allowed.</p>

### ACCESS Privileges

Range:	READ ONLY, READ WRITE
Default:	READ ONLY
Description:	<p>Determines the community access privilege of the SNMP managers in this community.</p> <p>In conjunction with the access mode of each MIB parameter, determines the SNMP operations (GET, GET-NEXT, SET, or none) that the SNMP manager can perform on a MIB parameter.</p>

### Trap Category

Range:	NONE, HIGH, MED, CONN, LOW, CODE, DEBUG
Default:	NONE
Description:	<p>Specify the type of SNMP traps that members of this community are allowed to receive. These SNMP traps are translated from Applications Ware events. The parameter values are as follows:</p> <ul style="list-style-type: none"> <li>• NONE: receive no traps</li> <li>• HIGH: receive high severity traps</li> <li>• MED: receive medium severity traps</li> <li>• LOW: receive low severity traps</li> <li>• CONN: receive connection traps</li> <li>• CODE: receive traps from Vanguard Networks 6xxx communications processors</li> <li>• DEBUG: receive traps for debugging only</li> </ul> <p>Specify any combination of the above by summing: HIGH + MED + CONN...etc.</p> <p><b>■ Note</b> Setting all categories on a single device floods a network with trap traffic. Do not use LOW, CONN, CODE, or DEBUG together unless you need them. Start with MED+HIGH.</p>

### SNMP Manager #1

Range:	A valid SNMP address in dotted notation.
Default:	(blank) (Specify a valid address here.)
Description:	<p>Specifies the IP address of an SNMP Manager that is a member of this community.</p> <p>Represents the IP address (in dotted notation) of the (sub)network for which an SNMP Manager information packet is to be accepted. Checks are done for duplicate community names and duplicate managers.</p> <p>Valid entries are x.x.x.x, where x is an integer between 0 and 255. For example: 1.11.111.1 or 0.27.7.255</p>

## Configuring the SNMPv3 Agent

### Introduction

SNMPv3 (version 3) is supported as of release 7.1 on all Vanguard router products. SNMP version 1 is still supported on all platforms as well. Vanguard software builder allows for the selection of either version 1 or version 3. The two versions are mutually exclusive to each other ie only one or the other can be selected for inclusion in a software image.

SNMP version 3 provides for secure access between the agent and the SNMP manager.

Configuring SNMPv3 parameters are described later in this section.

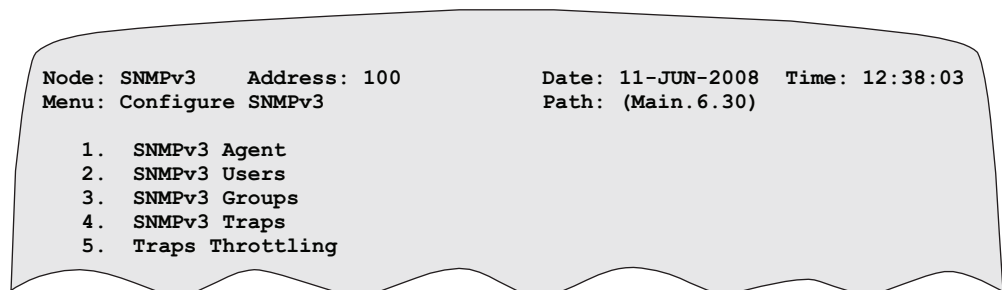
### Configuring the SNMPv3

Follow these steps to access to configure the SNMPv3 for your Vanguard.

<b>Step</b>	<b>Action</b>	<b>Result</b>
<b>1</b>	From the Main CTP menu, select <b>Configure-&gt;SNMPv3.</b>	The SNMPv3 Configure Menu and its parameters appear as shown in Figure 7. A prompt appears asking you to configure the next parameter.

### What You See in the Configure SNMPv3 Menu

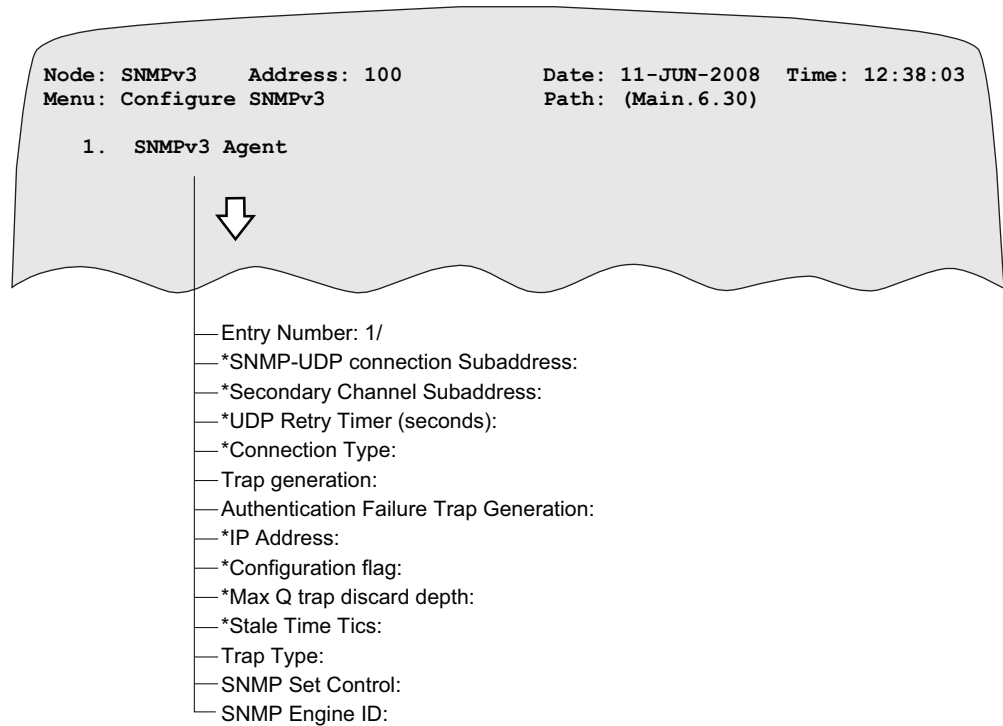
Figure 7 shows the SNMPv3 Menu under the configure SNMPV3 menu.



**Figure 7. Configure SNMPv3 Menu**

**Configure SNMPv3 Agent Menu**

Figure 8 shows the SNMPv3 Agent Menu under configure SNMPV3.



**Figure 8. SNMPv3 Agent Menu**

**Configure SNMPv3 Agent Parameters**

Below are the configurable parameters available under the SNMPv3 Agent Menu.

**Entry Number**

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

**\*SNMP-UDP connection Subaddress**

Range	0-3 BCD digits, use the space character to blank field
Default	161
Description	Enter the Subaddress of the port.
Boot Type	A change to this parameter requires a node boot to take effect.

**\*Secondary Channel Subaddress**

Range	0-3 BCD digits, use the space character to blank field
Default	(blank)
Description	Enter the Secondary Subaddress of the port.
Boot Type	A change to this parameter requires a node boot to take effect.

**\*UDP Retry Timer (seconds)**

Range	1-255
Default	10
Description	The amount of time, in seconds, between call attempts.
Boot Type	A change to this parameter requires a node boot to take effect.

**\*Connection Type**

Range	APAD,UDP,SIP_W,SIP_L
Default	UDP
Description	The type of port that is connected to the SNMP Agent. APAD -- for a PAD connection UDP -- for a UDP connection SIP_W -- for Management only IP forcing the use of WAN packets to save conversions SIP_L -- for Management only IP forcing the use of LAN packets
Boot Type	A change to this parameter requires a node boot to take effect.

**Trap generation**

Range	DISABLE,ENABLE
Default	DISABLE
Description	The Enable / Disable flag for the generation of all Traps. ENABLE -- to generate normal Traps DISABLE -- to suppress the generation of all Traps
Boot Type	SNMP boot

**Authentication Failure Trap Generation**

Range	DISABLE,ENABLE
Default	DISABLE

**Authentication Failure Trap Generation** (continued)

Description	The Enable / Disable flag for the generation of Authentication Traps. ENABLE -- to generate Authentication Failure Traps DISABLE -- to suppress the generation of Authentication FailureTraps
Boot Type	SNMP Boot

**\*IP Address**

Range	A valid IP address
Default	blank
Description	Input the IP address for this node. Valid entries are X.X.X.X where X is an integer between 0 and 255.
Boot Type	<b>Note</b> A change to this parameter requires a node boot to take effect.

**Trap Type**

Range	RFC,ENTERPRISE_SPECIFIC
Default	RFC
Description	This attribute gives choice between generic traps as defined in RFC or corresponding enterprise specific traps to be generated by node. This attribute is applicable only when generic traps are being generated and there exists a corresponding enterprise specific trap. The enterprise specific traps contain text like description which found to be very user friendly.
Boot Type	SNMP Boot

**SNMP Set Control**

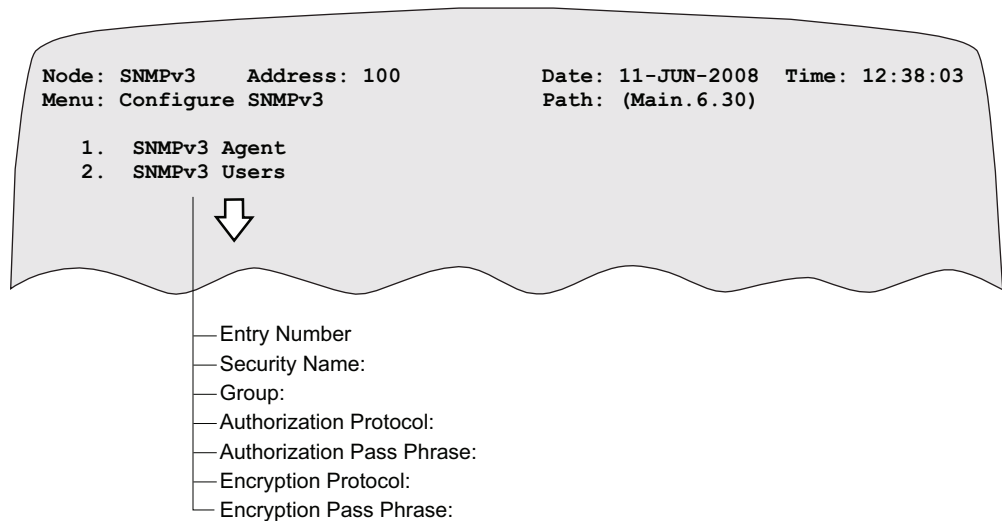
Range	ON,OFF
Default	OFF
Description	The ON/OFF flag for the SNMP SET Operation. ON -- to enable snmp set operation OFF -- to disable snmp set operation
Boot Type	SNMP Boot

### SNMP Engine ID

Range	A valid Engine ID
Default	blank
Description	The string identifying the local SNMP engine. This is an ASCII string, representing hexadecimal characters, from 10 to 64 characters long. Its length must be an even number. For example, '80000e50e134a7b8023b'.
Boot Type	SNMP Boot

### Configure SNMPv3 Users Menu

Figure 9 shows the SNMPv3 Users Menu under configure SNMPV3.



**Figure 9. SNMPvs Users Menu**

### Configure SNMPv3 User Parameters

Below are the configurable parameters available under theSNMPv3 Users Menu.

#### Entry Number

Range	1-8
Default	1
Description	Entry number used to reference this table record.
Boot Type	SNMP Boot

#### Security Name

Range	0-32 alphanumeric characters, use the space character to blank field
-------	----------------------------------------------------------------------

**Security Name** (continued)

Default	(blank)
Description	The security name for the user is a human-readable string representing the user in a format that is Security Model independent. In practice it can be identical to the user name.
Boot Type	SNMP Boot

**Group**

Range	0-4
Default	0
Description	The group id is the number of the group to which the user belongs. The value can range between 0 and 4. 0 means no group association has been made. 1 through 4 correspond to the groups that can be configured under the SNMPv3 Groups menu.
Boot Type	SNMP Boot

**Authorization Protocol**

Range	MD5, SHA
Default	MD5
Description	The protocol to be used for authorization. This can be either MD5 or SHA. The pass phrase will be hashed to form a key with the chosen protocol and the key will be used as proof of user authorization.
Boot Type	SNMP Boot

**Authorization Pass Phrase**

Range	0-128 alphanumeric characters, use the space character to blank field
Default	(blank)
Description	A memorable phrase known only to the user, between 1 and 128 characters long, which will serve to generate an authorization key.
Boot Type	SNMP Boot

**Encryption Protocol**

Range	DES
Default	DES

**Encryption Protocol (continued)**

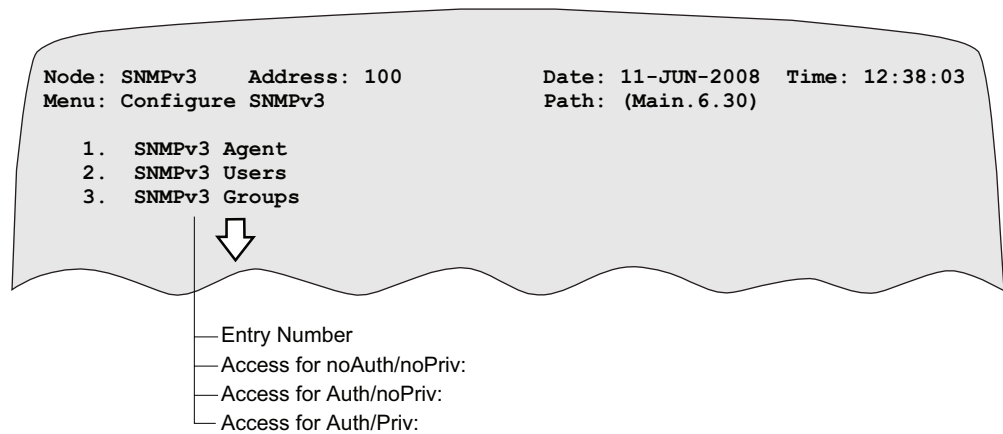
Description	The protocol to be used for encryption of PDUs. Encryption will only be performed if Privacy is turned on for communication.
Boot Type	SNMP Boot

**Encryption Pass Phrase**

Range	0-128 alphanumeric characters, use the space character to blank field
Default	(blank)
Description	A memorable phrase known only to the user, between 1 and 128 characters long, which will serve to generate an encryption key.
Boot Type	SNMP Boot

**Configure SNMPv3 Group Menu**

Figure 10 shows the SNMPv3 Group Menu under configure SNMPV3.



**Figure 10. SNMPv3 Groups Menu**

**Configure SNMPv3 Group Parameters**

Below are the configurable parameters available under the SNMPv3 Group Menu.

**Entry Number**

Range	1-4
Default	1
Description	Entry number used to reference this table entry
Boot Type	SNMP Boot

**Access for noAuth/noPriv**

Range	NONE,READ-ONLY,READ-WRITE
Default	NONE
Description	The level of access allowed when a PDU arrives from a group member, and it has no authorization and no privacy enabled. This could be none, read-only, or read-write.
Boot Type	SNMP Boot

**Access for Auth/noPriv**

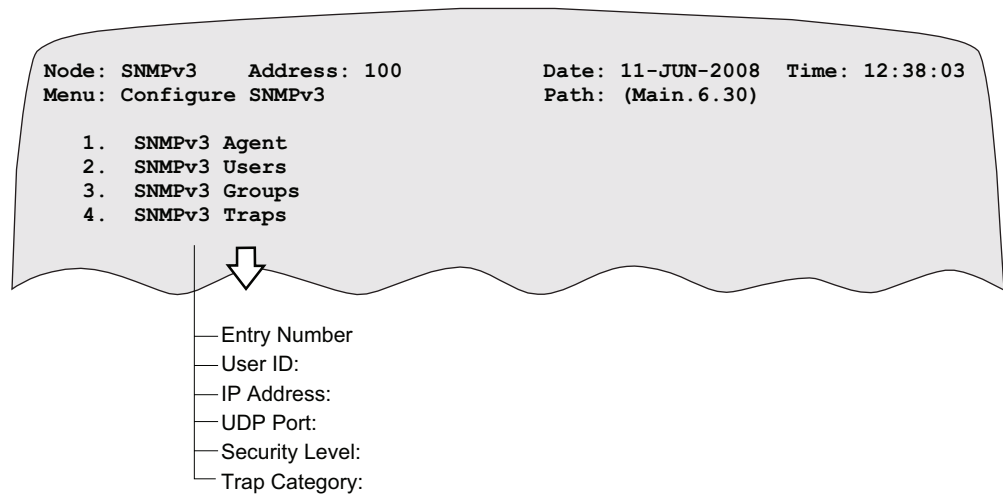
Range	NONE,READ-ONLY,READ-WRITE
Default	NONE
Description	The level of access allowed when a PDU arrives from a group member, and it has authorization enabled, but no privacy enabled. This could be none, read-only, or read-write.
Boot Type	SNMP Boot

**Access for Auth/Priv**

Range	NONE,READ-ONLY,READ-WRITE
Default	NONE
Description	The level of access allowed when a PDU arrives from a group member, and it has authorization and privacy enabled. This could be none, read-only, or read-write.
Boot Type	SNMP Boot

**Configure SNMP Traps Menu**

Figure 11 shows the SNMPv3 Traps Menu under configure SNMPV3.



**Figure 11. SNMPv3 Traps Menu**

**Configure SNMPv3 Traps Parameters**

Below are the configurable parameters available under the SNMPv3 Traps Menu.

**Entry Number**

Range	1-8
Default	1
Description	Entry number used to reference this table entry
Boot Type	SNMP Boot

**User ID**

Range	0-8
Default	0
Description	User id associated with Manager which will be receiving the configured traps. This id corresponds to a user which has been configured under the snmpv3 Users menu.
Boot Type	SNMP Boot

**IP Address**

Range	A valid IP address
Default	Blank

**IP Address** (continued)

Description	Input the IP address for the remote node. Valid entries are X.X.X.X where X is an integer between 0 and 255.
Boot Type	SNMP Boot

**UDP Port**

Range	0-65535
Default	0
Description	UDP port number on remote Manager which will be receiving traps.
Boot Type	SNMP Boot

**Security Level**

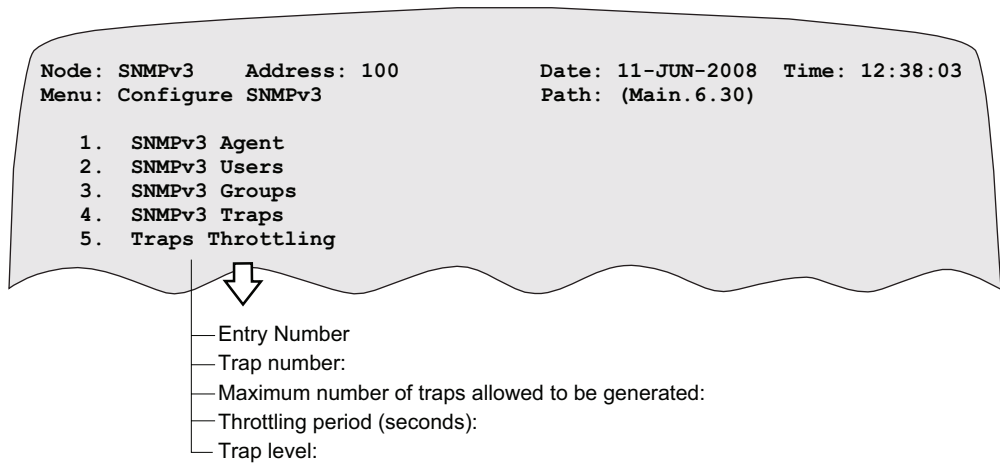
Range	NOAUTH-NOPRIV,AUTH-NOPRIV,AUTH-PRIV
Default	NOAUTH-NOPRIV
Description	The security level of traps as they are sent to a Manager. This could be no Authorization and no Privacy, or Authorization but no Privacy, or Authorization and Privacy.
Boot Type	SNMP Boot

**Trap Category**

Range	NONE,HIGH,MED,CONN,LOW,CODE,AGENT,DEBUG
Default	NONE
Description	<p>This parameter specifies the category of SNMP traps that this manager is allowed to receive.</p> <p>NONE - receive no traps  HIGH - receive high severity traps  MED - receive medium severity traps  LOW - receive low severity traps  CONN - receive connection traps  CODE - receive traps from Codex 6000 communication processors  AGENT - receive traps from SNMP Agent  DEBUG - receive traps generated for debugging Purposes</p> <p>Any combination of the above can be specified by summing (e.g. HIGH+CONN+ . . ).</p>
Boot Type	SNMP Boot

**SNMP Trap Throttling Menu**

Figure 12 shows the SNMPv3 Trap Throttling Menu under configure SNMPV3.



**Figure 12. SNMPv3 Trap Throttling Menu**

**SNMPv3 Trap Throttling Parameters**

Below are the configurable parameters available under the SNMPv3 Trap Throttling Menu.

**Entry Number**

Range	1-64
Default	1
Description	Entry number used to reference this table entry
Boot Type	SNMP Boot

**Trap number**

Range	1000-2147483647
Default	1000
Description	Trap number to be throttled. Refer to MIB file containing traps definitions
Boot Type	SNMP Boot

**Maximum number of traps allowed to be generated**

Range	0-65535
Default	5
Description	Maximum number of traps which are allowed to be generated in the throttling period. Excessive traps will be throttled in the specified period of time.

**Maximum number of traps allowed to be generated (continued)**

Boot Type	SNMP Boot
-----------	-----------

**Throttling period (seconds)**

Range	0-65535
Default	60
Description	Number of seconds for the throttling period. During that time, only the specified number of traps can be sent. Excessive traps are throttled. New traps can be sent when throttling period expires.
Boot Type	SNMP Boot

**Trap level**

Range	UNCHANGED,HIGH,MED,LOW
Default	UNCHANGED
Description	New severity level which should be used for this trap. The following values are allowed: <p style="text-align: center;">UNCHANGED HIGH MED LOW</p>
Boot Type	SNMP Boot

## SNMPv3 Configuration Examples

### SNMPv3 Configuration Example 1

#### Noauth/Nopriv

Shown below is the configuration of the SNMPv3 agent in its most simplest form. The bold represents the changes from a default configuration. As can be seen this shows only five parameters are required in this mode of operation (from default).

The Manager of choice should match these parameter values.

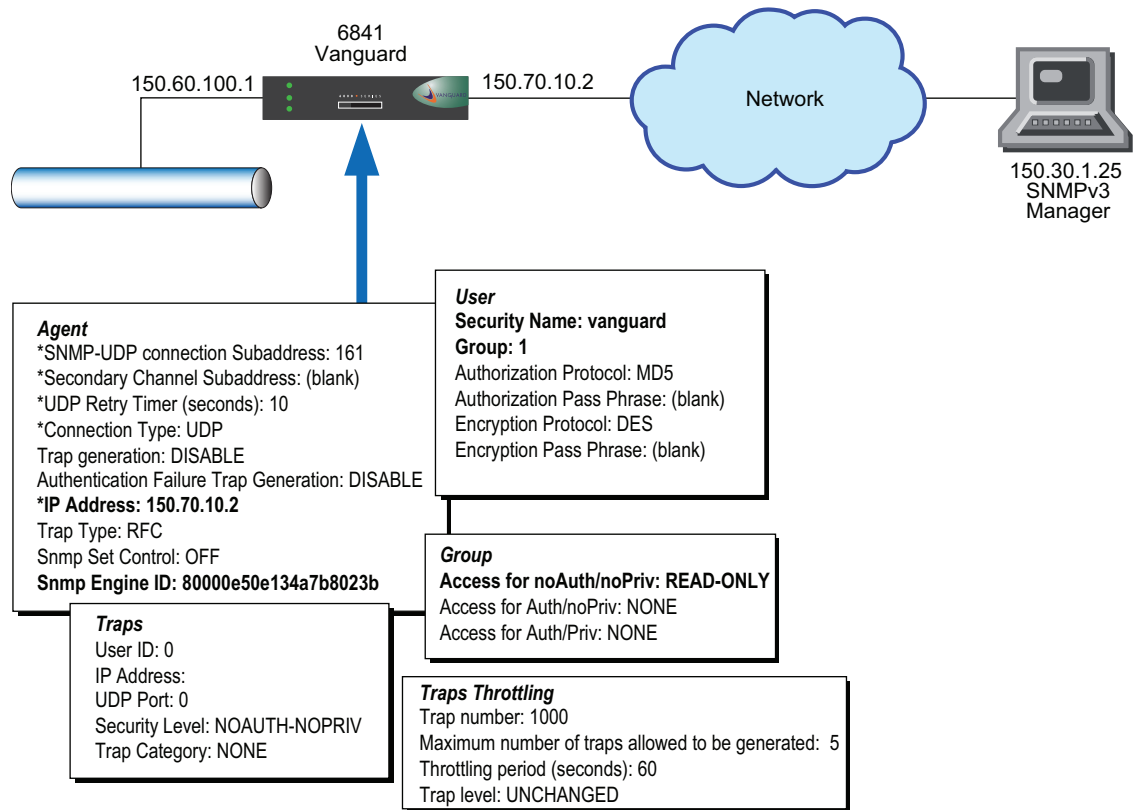


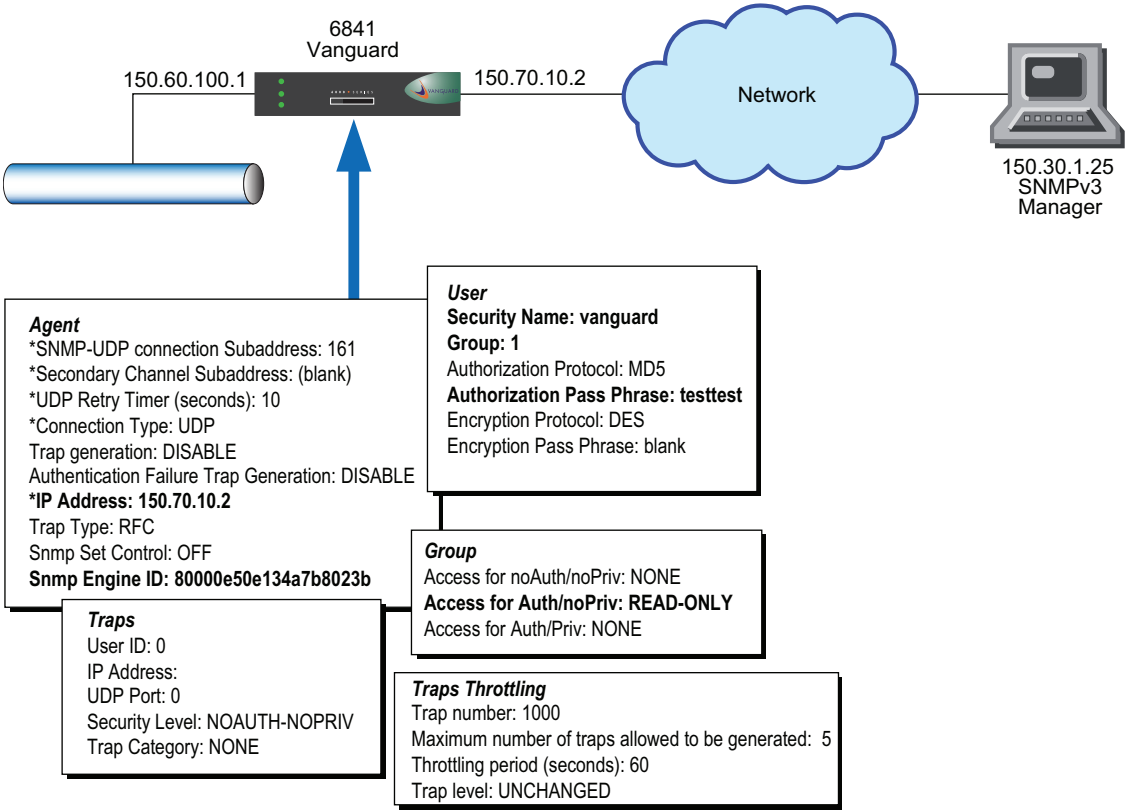
Figure 13. SNMPv3 Noauth/NoPriv Configuration Example

**SNMPv3 Configuration Example 2**

**Auth/NoPriv**

Shown below is the configuration of the SNMPv3 agent using Authorization only. The bold represents the changes from a default configuration. As can be seen this shows only six parameters are required in this mode of operation (from default).

The Manager of choice should match these parameter values.



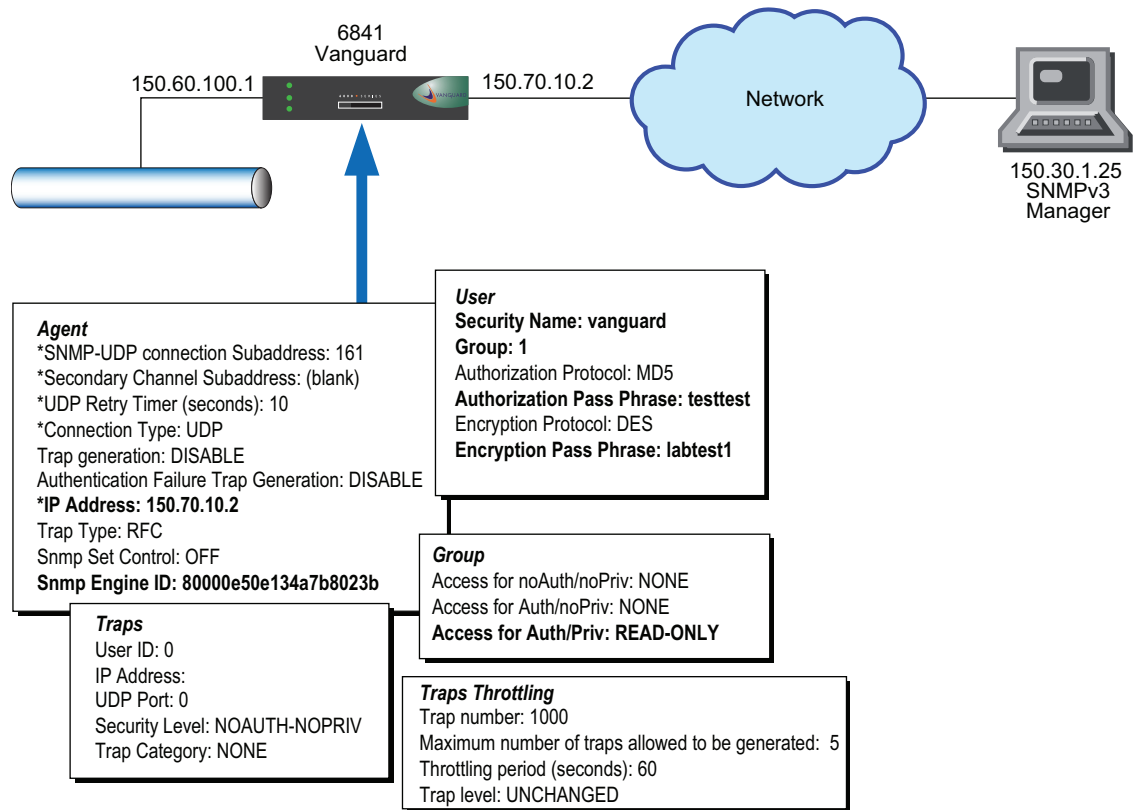
**Figure 14. Auth/NoPriv Configuration Example**

**SNMPv3 Configuration Example 3**

**Auth/Priv**

Shown below is the configuration of the SNMPv3 agent using both Authorization and Privacy. The bold represents the changes from a default configuration. As can be seen this shows only seven parameters are required in this mode of operation (from default).

The Manager of choice should match these parameter values.



**Figure 15. Auth/Priv Configuration Example**

## Viewing SNMP Statistics

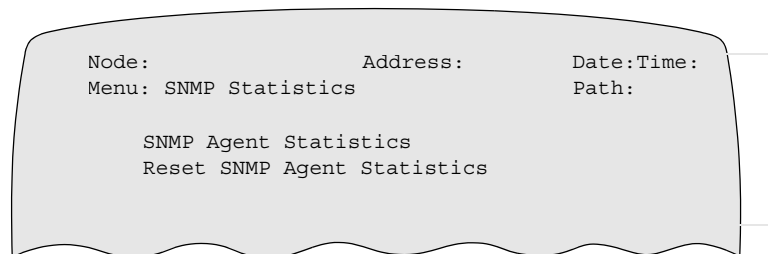
**Function** SNMP statistics provide detailed information about SNMP network connectivity. You can view and reset SNMP Agent statistics from the CTP for the Vanguard.

**View Statistics** Follow these steps to view the SNMP Statistics menu screen.

Step	Action	Result
1	From the CTP Main Menu, select Status/Statistics.	The Status/Statistics menu appears.
2	Select SNMP Statistics.	The SNMP Statistics menu screen appears as shown in Figure 16.
3	Select SNMP Agent Statistics.	Four screens appear sequentially as shown in Figures 17 through 20.

### What You See in This Menu

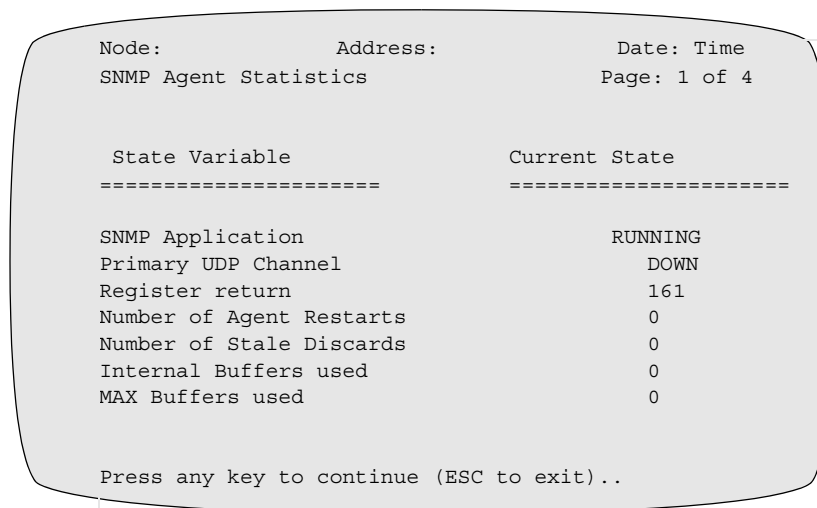
Figure 16 shows the SNMP Statistics menu screen.



**Figure 16. SNMP Statistics Menu Screen**

### What You See in the First Screen

Figure 17 shows an example of the first SNMP Agent Statistics screen.



**Figure 17. Example of SNMP Agent Statistics Screen, First Page**

---

**Screen Terms**

This table describes the statistics shown in Figure 17.

<b>Screen term</b>	<b>Describes</b>
SNMP Application:	Current state of the SNMP agent: <ul style="list-style-type: none"><li>• BOOT</li><li>• INITIALIZING</li><li>• RUNNING</li></ul>
Primary UDP Channel:	Current state of the UDP channel: <ul style="list-style-type: none"><li>• INITIALIZED/DOWN = channel has been initialized but is not active</li><li>• DOWN = channel is down</li><li>• REGISTERING = channel is setting up</li><li>• UP = channel is active</li><li>• CLEARING = channel is about to be disconnected</li></ul>
Register return:	This entry should match the SNMP-UDP channel Subaddress value.
Number of Agent Restarts:	Number of times SNMP agent has been rebooted through the Boot SNMP Agent command (found in the Boot menu).
Number of Stale discards:	The number of SNMP packets that were discarded or ignored because they could not be processed quickly enough.
Internal Buffers Used:	The number of internal buffers that the SMNP Agent is currently using.
MAX Buffers Used:	The Maximum number of buffers that the SNMP Agent has used at one time.

---

**What You See in the Second Screen**

Figure 18 shows an example of the second SNMP Agent Statistics screen. This screen lists the statistics values for Standard MIB statistics found in the RFC1213.

```
Node:                Address:                Date:                Time:
SNMP Agent Statistics                               Page: 2
of 4

SNMP Agent Statistics                               Statistic Value
=====
snmpInPkts                                           0
snmpOutPkts                                          0
snmpInBadVersions                                    0
snmpInBadCommunityNames                             0
snmpInBadCommunityUses                              0
snmpInASNParseErrs                                  0
snmpInBadTypes                                       0
snmpInTooBigs                                        0
snmpInNoSuchNames                                    0
snmpInBadValues                                      0

Press any key to continue (ESC to exit)...
```

**Figure 18. Example of SNMP Agent Statistics Screen, Second Page**

**What You See in the Third Screen**

Figure 19 shows an example of the third SNMP Agent Statistics screen, which lists the statistics values for Standard MIB statistics found in the RFC1213.

```
Node:                Address:            Date:              Time:
SNMP Agent Statistics                               Page:3
of 4

SNMP Agent Statistics                               Statistic Value
=====
snmpInReadOnlys                                     0
snmpInGenErrs                                       0
snmpInTotalReqVars                                  0
snmpInTotalSetVars                                  0
snmpInGetRequests                                   0
snmpInGetNexts                                      0
snmpInSetRequests                                   0
snmpInGetResponses                                  0
snmpInTraps                                         0
snmpOutTooBigs                                       0

Press any key to continue (ESC to exit ) ...
```

**Figure 19. Example of SNMP Agent Statistics Screen, Third Page**

**What You See in the Fourth Screen**

Figure 20 shows the fourth SNMP Agent Statistics screen, which lists the statistics values for standard MIB statistics found in the RFC1213.

```
Node:                Address:                Date:                Time:
SNMP Agent Statistics of 4                Page:4

SNMP Agent Statistics                Statistic Value
=====                =====

snmpOutNoSuchNames                0
snmpOutBadValues                0
snmpOutReadOnlys                0
snmpOutGenErrs                0
snmpOutGetRequests                0
snmpOutGetNexts                0
snmpOutSetRequests                0
snmpOutGetResponses                0
snmpOutTraps                0
snmpEnableAuthTraps                2

Press any key to continue (ESC to exit ) ...
```

**Figure 20. Example of SNMP Agent Statistics Screen, Fourth Page**

## Resetting SNMP Agent Statistics

### Introduction

You can reset values to the default state or to 0 using Reset SNMP Agent Statistics.

■ **Note**

Resetting SNMP statistics causes all MIB-II SNMP group statistics to reset.

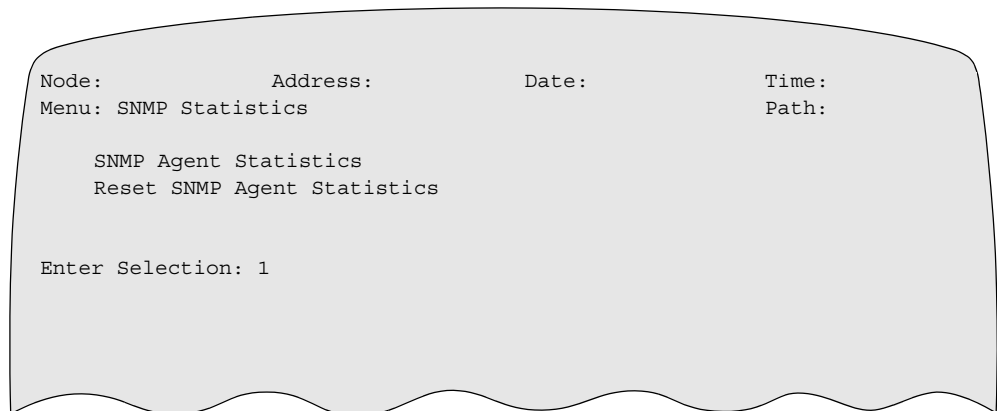
### How to Reset Statistics

Follow these steps to reset SNMP agent statistics.

<b>Step</b>	<b>Action</b>	<b>Result</b>
1	From the CTP Main Menu, select <b>Status/Statistics</b> .	The Status/Statistics menu appears.
2	Select <b>SNMP Statistics</b> .	The SNMP Statistics menu screen appears as shown in Figure 21.
3	Select <b>Reset SNMP Agent Statistics</b> .	<i>All MIB-II SNMP group statistics reset to the default state or to 0.</i>

### What You See in This Menu

Figure 21 shows the selection Reset SNMP Agent Statistics in the SNMP Statistics menu screen.



**Figure 21. SNMP Statistics Menu Screen**

## Trap Throttling

### Introduction

Vanguard Applications Ware consists of many modules that are often totally independent of each other. When a node enters a critical state, for example when a link goes down, many different modules start to report the same error. This often generates a flood of traps.

The generation of the multiple traps can rapidly congest the Network Management System (NMS) and, because each trap carries the same information, generating so many traps can hamper the investigation of potential problems. Receiving one or two traps should be sufficient to identify the node with the problem and the nature of the problem.

For this reason, the SNMP agent on any Vanguard node can throttle these repetitive traps. You can define the throttling parameters to filter out those traps that may flood the NMS.

#### ■ Note

64 different traps can be throttled on any one node.

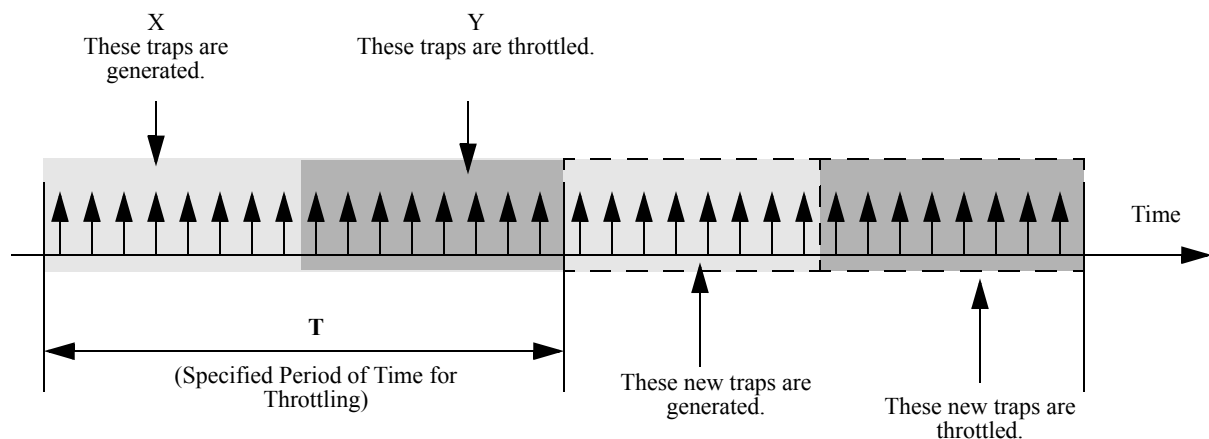
#### ■ Note

For additional information on traps, reports and fatal errors, please refer to the Vanguard *Basic Configuration Manual* (Part Number T0113).

### Throttling

Throttling is performed on a time basis; a node generates only a specified number of traps per specified period of time. Any repetitive traps that would be generated after the specified period of time expires are not generated.

As a Network Administrator, configure the node to generate the specified number of traps during the specified period of time. Figure 22 illustrates this concept, whereby **T** is the specified time period and **X** is the maximum number of traps that can be generated, and **Y** illustrates the traps that are throttled.

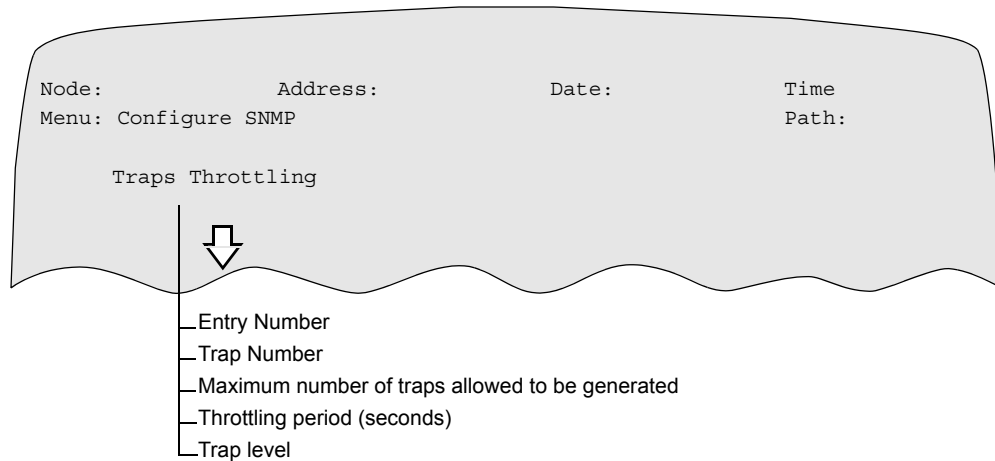


**Figure 22. Throttling Mechanism**

## Trap Throttling

To perform throttling, these parameters must be configured:

- Trap Number (a unique number for each event)
- Maximum number of traps allowed to be generated
- Throttling period



**Figure 23. Trap Throttling Menu Screen**

---

## Changing Priority

### Introduction

Previously, the assigned Priority (sometimes referred to as the Report Level) was fixed and could not be changed.

You can now use priority to control which traps are generated and which traps are suppressed. For example, you can configure a node to forward all MEDIUM priority reports as traps. The node, then, forwards all MEDIUM reports generated in the node as traps.

However, some situations may arise when you may want to change the priority of a particular report rather than to suppress all the reports of a particular priority. The node may often generate the same MEDIUM report. To suppress trap generation for the report, change its priority to LOW and configure the node to suppress all LOW priority reports. The node suppresses that report, while it continues to forward all other MEDIUM priority reports as traps.

### Changing Priority Configuration

Configuring throttling parameters (trap number, number of traps allowed to be sent and period of time) and defining new trap level, is performed using the CTP and SNMP. Complete this procedure to reconfigure the priority levels for a specific alarm(s):

#### ■ Note

Please refer to the table called `cdx6500SNMPTrapThrottleTable` found in the file `cdx_6500.mib`, located on the Vanguard CD-ROM that supports release 5.3M and later, for SNMP object definitions relating to Trap Throttling.

<b>Step</b>	<b>Action</b>	<b>Result</b>
<b>1</b>	Select <b>Configure</b> from the CTP Main menu.	The Configure menu appears.
<b>2</b>	Select <b>Configure SNMP</b> from the Configure menu.	The Configure SNMP menu appears.
<b>3</b>	Identify the alarm that you want to reconfigure by referencing the Trap number. You can find the required alarm in the <i>Vanguard Applications Ware Alarms and Reports Manual</i> (Part Number T0005) and record the corresponding Trap Number.	
<b>4</b>	Select <b>Traps Throttling</b> from the Configure SNMP menu.	You are prompted to start changing parameters.

### Configuration Parameters

These parameters must be set in order to configure traps throttling:

#### Entry Number

Range:	1 to 64
Default:	1
Description:	Specifies the entry number used to reference the table record.

#### Trap Number

Range:	1000 to 2147483647
Default:	1000
Description:	Specifies the trap number to be throttled. Refer to the <i>Vanguard Applications Ware Alarms and Reports Manual</i> (Part Number T0005) to identify the correct trap number.

#### Maximum number of traps allowed to be generated

Range:	0 to 65535
Default:	5
Description:	Specifies the maximum number of traps that can be generated during the throttling period. When this number of traps is exceeded, all excessive traps are throttled during the throttling period.

#### Throttling period (seconds)

Range:	0 to 65535
Default:	60
Description:	Specifies the number of seconds that to be assigned as the throttling period. During this time, only the number of traps specified as the “Maximum number of traps allowed to be generated” is sent. All others are throttled. Any new traps are sent once the Throttling period has expired.  <b>■ Note</b> Specifying a zero value for this parameter, traps are generated but not throttled.

**Trap level**

Range:	UNCHANGED, HIGH, MED, LOW
Default:	UNCHANGED
Description	<p>Specifies the priority level that should be used for the selected trap. If you select UNCHANGED and have entered non-zero values for the “Maximum number of traps allowed to be generated” and “Throttling period” parameters, throttling occurs as configured, but the trap level does not change.</p> <p>■ <b>Note</b> Refer to the <i>Vanguard Applications Ware Alarms and Reports Manual</i> (Part Number T0005) for additional explanations of these levels.</p>

**Alarms Throttling**


---

With Release 6.1 and greater Alarm Throttling menus are available through the CTP. For more information regarding Alarm Throttling, refer to the *Alarms and Reports Manual* (Part Number T0005).

---

## V.54 Loopback Test Using SNMP

---

### Introduction

These objects are defined to run the V.54 loopback test using SNMP:

- `cdx6500NMV54LoopbackDuration`
- `cdx6500NMV54LoopbackStatus`
- `cdx6500NMV54LoopbackTest`
- `cdx6500NMV54LoopbackTestType`
- `cdx6500NMV54LoopbackLastPortTested`
- `cdx6500NMV54LoopbackCurrentTestPort`
- `cdx6500NMV54LoopbackMessagesSent`
- `cdx6500NMV54LoopbackGoodMsgsReceived`
- `cdx6500NMV54LoopbackBadMsgsReceived`

#### ■Note

Refer to the *Vanguard Basic Configuration Manual* (Part Number T0113) for additional information on this test.

The SNMP agent allows the V.54 loopback test to run independent of the CTP. Therefore, one loopback test can be run using CTP while the other is being started using SNMP. The only restriction is that they can not be run on the same port.

---

### Running the Test

To start V54 test, the SNMP agent needs to know the following information:

- The type of the test (local loop, remote loop, and so forth.).  
Set the `cdx6500NMV54LoopbackTestType` object to the desired value. This contains definition of the object along with the allowed values.
- The port number on which the test is performed.  
Set the `cdx6500NMV54LoopbackCurrentTestPort` object to the port number.
- The duration of the test.  
Set the `cdx6500NMV54LoopbackDuration` object to the desired test duration. If you set this object to zero, the test runs until it is explicitly stopped.

To start the test, set the `cdx6500NMV54LoopbackTest` object to **testing**. If you want to stop the test at anytime, set this object to the **notTesting** value.

The SNMP agent allows only one test to be run at a time. When starting the test by setting value `testing` for `cdx6500NMV54LoopbackTest` object, the SNMP agent replies that the specified value has a bad type, meaning that the test is already running.

When the SNMP agent replies that the `cdx6500NMV54LoopbackTest` object has been set successfully, it means that V.54 agent tried to start the test. To check whether test has been started or to find the potential error, read the `cdx6500NMV54LoopbackStatus` object.

### ■ Note

The object *cdx\_6500.mib* defines a set of possible errors. These errors include a description explaining why the test could not be started.

When the *cdx6500NMV54LoopbackStatus* object has a value of **v54Running** it means that test is in progress although, if the value is **v54Stopped** this indicates that the test has completed.

---

### Test Results

The results of the V.54 loopback test can be found in three read-only counters:

- *cdx6500NMV54LoopbackMessagesSent* - the number of sent messages
- *cdx6500NMV54LoopbackGoodMsgsReceived* - the number of messages received without any error
- *cdx6500NMV54LoopbackBadMsgsReceived* - the number of messages containing an error

When the test is completed, the *cdx6500NMV54LoopbackCurrentTestPort* object is defaulted to zero. The next test cannot start without setting the new value for this object. The port number of the completed test can be found in *cdx6500NMV54LoopbackLastPortTested* object.

---

## SNMP Agent Table Worksheets

**Worksheet**

Use the following worksheets to create sample configurations for SNMP agents and communities.

Node Name \_\_\_\_\_ Node Number \_\_\_\_\_ Date \_\_\_\_\_

<i>Parameter</i>	<i>Operator Entries</i>					
Entry Number						
*SNMP-UDP Connection Subaddress						
*UDP Retry Timer						
*Trap Generation						
*Authentication Failure Trap Generation						

Node Name \_\_\_\_\_ Node Number \_\_\_\_\_ Date \_\_\_\_\_

<i>Parameter</i>	<i>Operator Entries</i>					
Entry Number						
*SNMP-UDP Connection Subaddress						
*UDP Retry Timer						
*Trap Generation						
*Authentication Failure Trap Generation						

# SNMP Communities Table Worksheet

**Worksheet**

Use the following worksheets to create sample configurations for SNMP agents and communities.

Node Name \_\_\_\_\_ Node Number \_\_\_\_\_ Date \_\_\_\_\_

<b>Parameter</b>	<b>Operator Entries</b>					
SNMP Community						
Access Privileges						
Trap Category						
SNMP Manager # _____						

Node Name \_\_\_\_\_ Node Number \_\_\_\_\_ Date \_\_\_\_\_

<b>Parameter</b>	<b>Operator Entries</b>					
SNMP Community						
Access Privileges						
Trap Category						
SNMP Manager # _____						

Node Name \_\_\_\_\_ Node Number \_\_\_\_\_ Date \_\_\_\_\_

<b>Parameter</b>	<b>Operator Entries</b>					
SNMP Community						
Access Privileges						
Trap Category						
SNMP Manager # _____						

**SNMP Communities Table Worksheet**

Node Name \_\_\_\_\_ Node Number \_\_\_\_\_ Date \_\_\_\_\_

<b>Parameter</b>	<b>Operator Entries</b>					
SNMP Community						
Access Privileges						
Trap Category						
SNMP Manager # _____						

---

**A**

Agent  
definition 2

**C**

Community Name  
access privileges 9  
and trap generation 5  
changing 19  
identifying existing names 19  
Configuration Examples 34  
Configuring 19  
guidelines 14  
SNMP agent record 14  
SNMP Community Record 19  
Configuring the SNMPv3 Agent 22

**G**

Get-Next-Request 2  
Get-Request 2

**M**

Management Information Base, see MIB  
MIB  
Device MIBs 4  
functional description 2  
getting copies 12  
Internet-standard hierarchy 3  
Management MIB 4  
Supported Read/Write 10  
VanguardMS supported 11  
MIB Objects  
access modes 9  
syntax 8

**N**

Network Management System  
defined 2

**O**

Object Identifiers  
for MIB 7  
functional description 3  
Object Names  
functional description 3

**P**

PDU  
list of 2  
PDUs, see Protocol Data Units  
Private Enterprise MIB Extensions 6  
Protocol Data Units

encoding used 3  
list of 2

**R**

Resetting SNMP Agent Statistics 42

**S**

SNMP  
Agents 4  
components 2  
connecting node to NMS 13  
display of hex or ASCII data 8  
functional description 1  
Set 10  
transport mapping 1  
SNMP agent record  
configuring 14  
functional description 14  
parameters 16  
SNMP Agent Statistics  
Resetting 42  
SNMP Community Record  
configuring 19  
functional description 19  
parameters 20  
SNMP Statistics  
Viewing 37  
SNMPv3 Agent  
Configuring 22  
Statistics  
screen terms 38  
SNMP 37  
SNMP agent 37  
Syntax  
counter 8  
network address 8  
timeticks 8

**T**

Trap  
filtering 5  
functional description 2  
levels 5  
throttling 43

**U**

User Datagram Protocol  
use in SNMP 1

**V**

Vanguard  
functional description of MIB 6  
implementation of SNMP 4  
Viewing SNMP Statistics 37

