Vanguard Managed Solutions

Vanguard Applications Ware
IP and LAN Feature Protocols

Traffic Monitor

Notice

575 West Street
Mansfield, Massachusetts 02048
(508) 261-4000

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).

Proprietary Material

Part No. T0100-15, Rev A
Publication Code: DS
First Printing: June 2003

Manual is current for 6.4 of Vanguard Applications Ware.

To comment on this manual, please send e-mail to LGEN031@vanguardms.com

Overview

Introduction

This manual describes the Vanguard Traffic Monitor feature available with Release 6.4 and greater software. Traffic Monitors have the ability to allocate packet collection counters for analyzing different types of applications based on various aspects. These counters provide the basis for real-time and historical performance monitoring by sampling data in regular intervals. Information can be displayed locally on CTP and CLI screens or remotely through the SNMP management protocol.

Note

The Traffic Monitor feature is supported on the Vanguard 34x, 6435, 6455 and 7300 Series.

In This Manual

Features

The major features of Vanguard Traffic Monitor are:

- Bandwidth and packet rate measurements are based on the following IP and link layer aspects:
  - Ethertype
  - IP Address
  - IP TOS Field
  - IP Protocol Type
  - TCP/UDP port number
- User configurable exception reporting based on selected protocol aspects
- On node storage of historical statistics for monitored protocol aspects
- SNMP support to facility integration into network management solutions

Upgrade License

Release 6.4 and greater includes a new License Upgrade called the QoS Application Performance Monitoring License Upgrade.

Performance Impact

The per packet classification and statistics collection places additional processing and memory demands on the system, which results in a reduction in the maximum system throughput. Traffic monitor features should only be enabled when in use to ensure maximum system performance.

Traffic Monitor

Introduction

In order for QoS tools (i.e. classification, conditioning, queuing and scheduling) to be useful, it's important to understand the characteristics of the traffic in the network and the needs of the users and applications that are generating the traffic. Even after traffic management mechanisms are deployed to enforce QoS policies, it is important to monitor the network traffic characteristics to identify changes as new users and applications are added to the network. The IP Traffic Monitoring features provide a practical and scalable means to collect and review information about traffic flowing through critical points in the network in order to support QoS policy establishment and maintenance.

The operational model for monitoring network traffic is illustrated in Figure 1. Traffic is classified and monitored at defined LAN/WAN ports and statistical information about the traffic is collected and stored in the Vanguard router where it can be accessed through SNMP by the appropriate management tools.

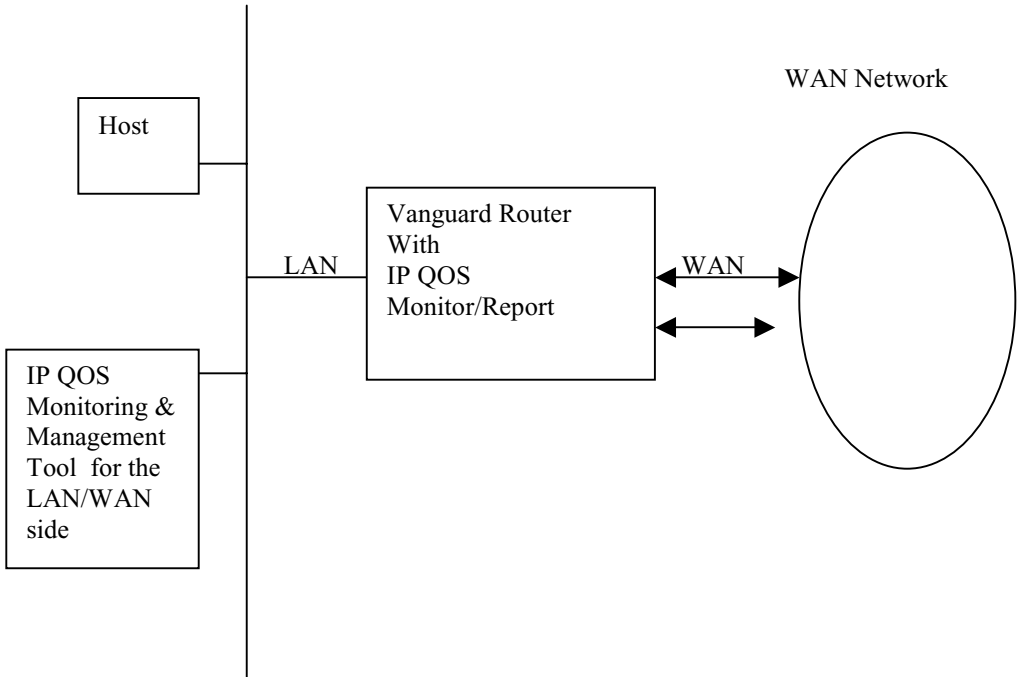

Figure 1. IP QoS Operating Diagram

IP QoS Metering

IP QoS Metering is a system for measuring, recording and displaying detailed information about data traffic passing through "Meter Points" defined in the router. The aspects of data traffic that can be monitored using the metering system provide the level of detail appropriate for use with the DiffServ based QoS capabilities of the Vanguard products.

Meter Points

Traffic is examined at specific points within the node at Meter Points, which are located as close to the physical link as possible in order to ensure that the information collected represents a realistic view of the traffic on the link.

Meters

Meters are very simple mechanisms that form the basis in the metering system. Each meter keeps track of the following statistics as packets pass it.

- Number of bytes
- Number of packets

Meters are typically used in sets to monitor specific aspects of the data traffic.

Aspects

Aspects represent a particular view of the traffic characteristics for a given meter point. For example, an aspect of an Ethernet port might be based on the ethertype of the Ethernet frames. In order to monitor this aspect of the traffic a number of meters are allocated, one for each ethertype that the user is interested in monitoring.
The Layer 2 aspects available for Ethernet ports are indicated below:

Layer 2 Aspect for Ethernet Ports

Aspect	*Description*
Frame Type	A set of meters indexed by the ethertype. L2 type identified using Ethertype for Ethernet II format frames and SAP/SNAP for 802.3 format frames.

The Layer 2 aspects available for Frame Relay ports are indicated below:

Layer 2 Aspect for Frame Relay Ports

Aspect	*Description*
Frame Type	A set of meters indexed by the L2 type based on the RFC1490 encapsulation type. NPLD for IP and SNAP for others.

The layer 3+ Aspects available for IP traffic on both Frame Relay and Ethernet ports are indicated in the table below:

Layer 3+ Aspect for Frame Relay Ports

Aspect	*Description*
TOS	A set of meters indexed in the 6 bit TOS field in the IP header.
IP Protocol	A set of meters indexed by the IP protocol field.
Destination Hosts	A set of meters indexed by the destination address in the IP header. Destination hosts monitor individual hosts or subnets.
Source Hosts	A set of meters indexed by the source address in the IP header. Source hosts can monitor individual hosts or subnets.
TCP Destination Ports	A set of meters indexed by individual TCP destination port numbers or a range of TCP destination port numbers.

Layer 3+ Aspect for Frame Relay Ports

TCP Source Ports	A set of meters indexed by individual TCP source port numbers or a range of TCP source port numbers.
UDP Destination Ports	A set of meters indexed by individual UDP destination port numbers or a range of UDP destination port numbers.
UDP Source Ports	A set of meters indexed by individual UDP source port numbers or a range of UDP source port numbers.

Aspect Monitor

Each aspect requires the user to configure the values or ranges to be monitored. Only those aspects that are configured for a meter point are monitored.

Traffic Classification

The traffic classification involves classifying and identifying traffic at different levels of the OSI 7-layer model. By “listening to the network” Vanguard devices can identify traffic types that are present in the network. Once the traffic is classified, the information is used for monitoring and reporting. In the Vanguard device, if the traffic monitoring tool is enabled, every packet captured on a metered LAN/WAN interface is classified based on the following aspects:

- Source and Destination IP Addresses
- IP TOS value - DSCP value
- Application name (UDP/TCP port numbers)
- IP Protocol Type

Note

The traffic classification used by the traffic monitor feature set is currently independent of the classifier(s) used in QoS_Kit.

Modes of Operation

The IP QoS Meter system supports two independent modes of operation that address different requirements in the QoS Service Process.

- **Monitor Mode** - Monitor mode is intended to be the normal long-term operating mode of the system. It is intended to monitor detailed characteristics for user-defined categories of traffic. Short and long-term information about traffic is collected and stored in the node. Exception conditions can be defined and alarms/traps generated when exception conditions occur. This facility is intended to be used as a primary component of the "Monitoring" phase of the QoS Service process.
- **Discovery Mode** - Discovery mode is run for a specific duration in order to gain an understanding of the traffic characteristics during that period. During the discovery period the node dynamically learns about the traffic and keeps track of bandwidth usage during that period. The facility is intended to assist in the "Evaluation" phase of the QoS Service process.

Exception Conditions

Exception conditions provide a mechanism for the user to specify alarms and traps that should be generated by the system when selected meters reach predefined values. The following items must be configured:

- Upper Threshold (On)
- Lower Threshold (Off)
- Alarm Priority (High, Medium, Low)

The alarm or trap indicates the exception ID and whether the meter has exceeded the upper threshold or gone below the lower threshold.

Traffic Monitor and Report

Vanguard devices use the protocol name, TOS and IP address information from traffic classification and identification to collect monitoring/reporting statistics. These statistics are used by the monitoring engine to produce reports that service providers can use to monitor applications.
In the Vanguard device, if the monitoring is enabled, the following statistics data is collected and stored in memory.

- Throughput (kbps): bytes classified under each discovered or monitored item
- Packet count-total: packets classified under each discovered or monitored item

Functional Overview

The IP QoS Monitor and Report consist of following features:

- Traffic Classification based on IP address, Protocol Name and TOS
- Traffic monitor and discovery mode
- Collect Statistical data for the Monitor and Report
- Support Monitor and Report Tool with SNMP

Figure 2 below, illustrates the relationship between the monitor and discovery processes. Packets enter the metering system in the monitor process and data is collected based on the monitor configuration (for example: monitor traffic from host x.x.x.x). If the packet is not counted in the monitor process (for example, packet is from host y.y.y.y), the packet is passed on to the discovery process. The discovery process dynamically builds a list of values to meter and maintains counts for items in the meter list. Once the discovery list if full any new items are counted as part of the "other" default entry.

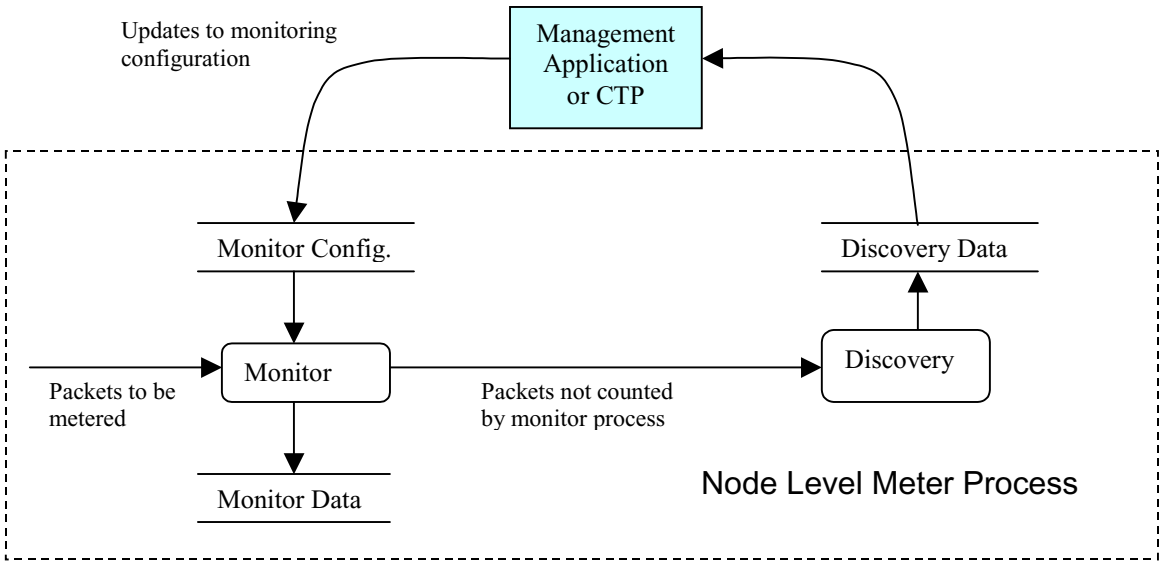

Figure 2. IP QoS Monitor/Report Functional Block

Discovery mode may or may not be enabled and active at the same time that monitoring is active. When discovery is active at the same time as monitoring the dynamically learned traffic detail applies to traffic outside the monitored set.

Traffic Capturing & Classification Function

The IP packets are captured at meter points can be classified based on:

- Source Address and Source Address Mask
- Destination Address and Destination Address Mask
- UDP/TCP Port Number
- TOS (Type of Service)

Traffic Capturing at the Meter Point

Traffic is examined at specific points within the node, which are located as close to the physical link as possible in order to ensure that the information collected represents a realistic view of the traffic on the link.

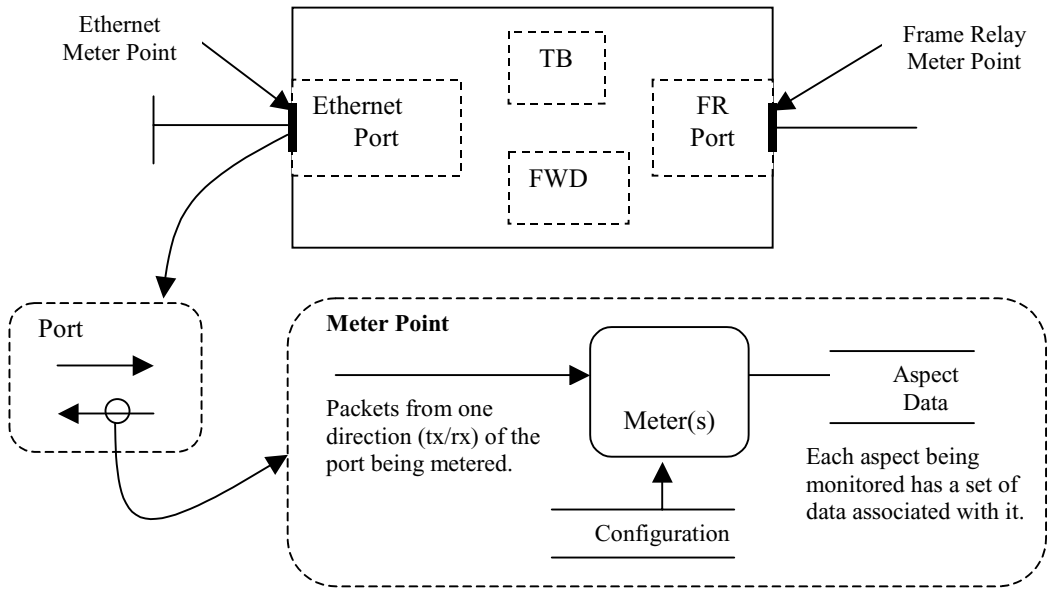

Figure 3. IP Packet Meter Point

Note

A single meter point examines both directions of traffic on a port.

The following link types support metering:

- Frame Relay Ports
- Ethernet Ports

Collecting and Storing Statistics

Layer two, Layer three and Layer four statistics are collected at each meter point. The layer three and four (IP) statistics are the same for all link types, however, the layer two statistics depend on the link type. Each meter point collects statistics for sixty seconds intervals. The most recent fifteen sixty-second intervals are retained in the node along with fifteen minute averages for the last twenty four hours.

Note

This applies to monitor mode only. Only the current value is maintained for discovery data. The “current” value is reset every sixty seconds after being saved as the most recent entry in the previous fifteen minute set. As each entry in the previous fifteen minute set is aged out, it is added to the accumulation for the current fifteen minute period.

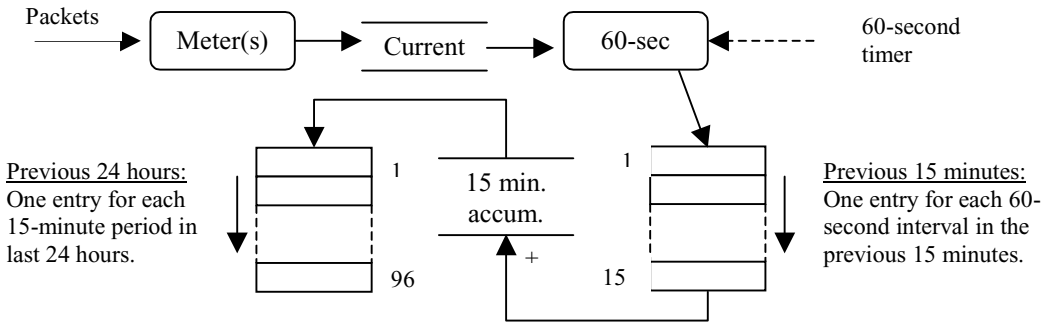

Figure 4. Collecting Statistics

Each meter point may be monitoring a number of aspects, each may have a number of meters associated with it. In Figure 5, the model for monitoring the "destination host address" is shown.

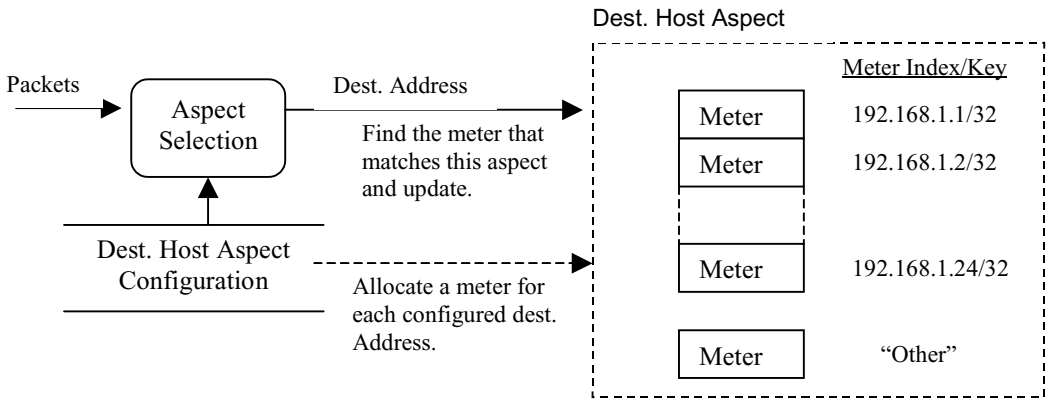

Figure 5. Storing Statistics

The "other" meter is provided by default for all aspects and is used to count those packets that do not match the monitored aspect values. This gives an aggregate measure of what is going on outside the monitored set.

Application Level Classification

The Vanguard device can capture inbound/outbound packets and classify them based on TCP/UDP source and destination port number.

Traffic Monitoring Function

Aspect specifications are used in monitor mode to constrain the processing and memory resources consumed by the traffic monitoring process. Users are required to specify the traffic characteristics that they are interested in monitoring.

IP Monitoring

The following table identifies the aspects of the IP level that can be monitored.

Aspects	*Description*
TOS	All TOS values are metered as part of the standard meter point. No configuration is required.
IP Protocol	All IP protocol values are metered as part of the standard meter point. No configuration is required.
Destination Hosts	Monitor bandwidth used by traffic to a host or subnet based on the destination address in the IP header. * **Host** - To monitor traffic destined for a specific host, configure the host address and a host mask (for example: 255.255.255.255). **Subnet** - To monitor traffic destined for a specific subnet, configure the address of the subnet with the corresponding subnet mask (for example: 255.255.255.0).
Source Hosts	Monitor bandwidth used by traffic from a host or subnet based on the source address in the IP header.* **Host** - To monitor traffic from a specific host, configure the host address and host mask (for example: 255.255.255.255). **Subnet** - To monitor traffic from a specific subnet, configure the address of the subnet with the corresponding subnet mask (for example 255.255.255.0).
TCP Ports	Monitor the bandwidth used by traffic to a specific TCP port number (source and destination). Specify a set of TCP ports and the associated display name (for example: 23, "telnet").
UDP Ports	Monitor the bandwidth used by traffic to a specific UDP port number (source and destination). Specify a set of destination UDP ports and the associated display name (for example: 69, "tftp").
* Does not include broadcast traffic sent to the host. Multicast addresses must be configured separately.	

Traffic Discovery Function

Discovery mode is controlled per meter point and is intended to operate over a limited period of time. When discovery is started, a meter point begins with a blank list of types and builds a list of types as packets/frames arrive. The new types are added to the list until the list limit is reached. For learned types the statistics are updated for each new packet or that type that arrives. When packets arrive that are not in the list and the list has reached it's limit, the statistics for those packets are included in the “other” traffic category which is the present in all protocol type lists. Resetting discovery mode statistics or learned types requires restarting the entire discovery process (for example, stop discovery and then re-start).

IP Discovery

IP discovery includes the following:

- Destination IP Address
- Source IP Address
- TCP Port Number
- UDP Port Number

Note

TOS and Protocol values are not independently supported in discovery mode because their value space is fully covered by monitor mode.

Statistics for Monitor/Report

Real Time Statistic Collection for the Traffic

Every inbound and outbound IP packet is captured and classified in real time based on the Ethernet/WAN Port. All collected data is stored within the node and is available via SNMP. The real time collection and structured data consists of following items:

- Time Stamp: captured date and time
- Source IP Address
- Destination IP Address
- TCP/UDP port number
- TOS value
- Ethernet Type
- Application Name (Telnet, SNMP, HTTP, FTP, SNTP, etc.)
- Throughput
- Packet count

IP Traffic Statistics

The Traffic Monitor feature generates throughput, packet count (total) statistical data based on Ethernet/WAN port during traffic capturing and classification. It collects statistical (STAT) data once a minute. The most recent 15 minute intervals are accumulated in the device along with the 15 minute average for the last 24 hours. This statistical data is illustrated in following table:

STAT Data	*Description*
Throughput (kbps)	Bytes classified under each monitored or discovered item.
Packet Count Total	Packets classified under each monitored or discovered item.

Note

The statistic (STAT) data is stored in the node and can be retrieved periodically by the SNMP query.

Configuration

Configure Traffic Monitor Menu

The following menu is displayed when the “Configure Traffic Monitor” menu entry is selected in Configure menu.

Main Menu->Configure->Configure Traffic Monitor

```
Node: V340      Address: (blank)          Date: 26-JAN-2004  Time: 12:17:35
Menu: Configure Traffic Monitor           Path: (Main.6.14)

 1. Configure Meter Point Table
 2. Configure Exception Table
 3. Configure Application Monitor Table
 4. Configure Source IP Monitor Table
 5. Configure Destination IP Monitor Table
 6. Configure Tos Value Monitor Table
 7. Configure Protocol Type Monitor Table
 8. Configure Ethernet Type Monitor Table
```

Figure 6. Configure Traffic Monitor Menu

Note

The location of "Configure Traffic Monitor" menu entry in the Configure menu is dependent on the features included in the node.

Configure Meter Point Table

Selecting the “Configure Meter Point Table” entry from the “Configure Traffic Monitor” menu allows the user to configure meter point configuration records. Each record defines one meter point. The entry number of the meter point configuration record uniquely identifies the meter point. Figure 7 shows an example meter point record configuration screen.

```
#Enter Selection: 1

      Traffic Monitor Meter Point

Entry Number: 1/
[1] Meter Port Number: 5/
[1] Traffic Monitor Enable/Disable: Enable/
[1] Traffic Discovery Enable/Disable: Enable/
[1] Traffic Bound: BOTHBOUND/
[1] Maximum Discovery Table: 64/
```

Figure 7. Traffic Monitor Meter Point Table

A maximum of 15 meter points (entry numbers 1 to 16) can be defined. The individual parameters are defined in the following sections.

Meter Port Number

Range:	Physical Port Range
Default:	1
Description:	This parameter specifies the LAN and FRI port for the traffic capture.
Boot Type:	Boot Meter Point Table

Traffic Monitor Enable/Disable

Range:	Enable, Disable
Default:	Disable
Description:	Traffic Monitor select enable or disable.
Boot Type:	Boot Meter Point Table

Traffic Discovery Enable/Disable

Range:	Enable, Disable
Default:	Disable
Description:	Traffic Discovery enable/disable.
Boot Type:	Boot Meter Point Table

Traffic Bound

Range:	BOTHBOUND, INBOUND, OUTBOUND
Default:	BOTHBOUND
Description:	Traffic Bound both/inbound/outbound.
Boot Type:	Boot Meter Point Table

Maximum Discovery Table

Range:	0 to 64
Default:	64
Description:	Maximum entry number for the discovery.
Boot Type:	Boot Meter Point Table

Configure Exception Table

Selecting the “Configure Exception Table” entry from the “Configure Traffic Monitor” menu allows the user to configure exception configuration records. Each record specifies an exception definition that can be applied to any one of the monitored aspect values. The entry number of the exception configuration record uniquely identifies the exception definition. Figure 8 shows an example exception record configuration screen.

```
#Enter Selection: 2

      Traffic Monitor Exception Configuration

Entry Number: 1/
[1] Upper Value: 0/
[1] Lower Value: 0/
[1] Direction: INBOUND/
[1] Alarm Priority: HIGH/
[1] Stat Unit: Bitrate/
```

Figure 8. Traffic Monitor Exception Configuration

A maximum of 254 records (entry numbers 1 to 255) can be defined. The individual parameters are defined in the following sections:

Upper Value

Range:	0 to 65535
Default:	0
Description:	Statistics Upper threshold value.
Boot Type:	Exception Table Boot.

Lower Value

Range:	0 to 65535
Default:	0
Description:	Statistics Lower threshold value.
Boot Type:	Exception Table Boot.

Direction

Range:	BOTHBOUND, INBOUND, OUTBOUND
Default:	BOTHBOUND
Description:	Traffic direction for the exception case.
Boot Type:	Exception Table Boot.

Alarm Priority

Range:	HIGH, MED, LOW
Default:	HIGH
Description:	Alarm Priority for the exception case.
Boot Type:	Exception Table Boot.

Stat Unit

Range:	Bitrate, Packets
Default:	Bitrate
Description:	Statistics Unit for the exception case.
Boot Type:	Exception Table Boot.

Configure Application Monitor Table

Selecting the “Configure Application Monitor Table” entry from the “Configure Traffic Monitor” menu allows the user to configure application monitor configuration records. Each record specifies an aspect value to be monitored. The entry number of the application monitor configuration record uniquely identifies the definition. Figure 9 shows an example application monitor record configuration screen.

```
#Enter Selection: 3

      Traffic Monitor Application Configuration

Entry Number: 1/
[1] Application Name: TELNET/
[1] Type: TCP/
[1] First Port Number: 23/
[1] Last Port Number: 23/
[1] Meter Point Entry List: ALL/
[1] Exception Entry Number: 0/
```

Figure 9. Traffic Monitor Application Configuration

A maximum of 63 records (entry numbers 1 to 64) can be defined. The individual parameters are defined in the following sections.

Application Name

Range:	0 to 16 (alphanumeric characters)
Default:	Telnet
Description:	This parameter specifies the Application Protocol name (for example, SNMP, TELNET, TFTP, etc.). Use the space bar to blank the field.
Boot Type:	Application Monitor Table Boot.

Type

Range:	TCP, UDP
Default:	TCP
Description:	This parameter specifies the protocol type number.
Boot Type:	Application Monitor Table Boot.

First Port Number

Range:	0 to 64555
Default:	23
Description:	This parameter specifies the TCP/UDP first port number.
Boot Type:	Application Monitor Table Boot.

Last Port Number

Range:	0 to 64555
Default:	23
Description:	This parameter specifies the TCP/UDP last port number.
Boot Type:	Application Monitor Table Boot.

Meter Point Entry List

Range:	1 to 16, ALL
Default:	ALL
Description:	This parameter specifies an entry number of a meter point which a packet is captured. A maximum of 16 ranges are permitted to be configured in this list (for example: 1, 2, 5). • ALL : This option is a wildcard used to match all meter ports.
Boot Type:	Application Monitor Table Boot.

Exception Entry Number

Range:	0 to 255
Default:	0
Description:	This parameter specifies the exception table entry number.
Boot Type:	Application Monitor Table Boot.

Configure Source IP Monitor Table

Selecting the “Configure Source IP Monitor Table” entry from the “Configure Traffic Monitor” menu allows the user to configure source IP address monitor configuration records. Each record specifies an aspect value to be monitored. The entry number of the source IP address monitor configuration record uniquely identifies the definition. Figure 10 shows an example source IP address monitor record configuration screen.

```
#Enter Selection: 4

     Traffic Monitor Source IP address Configuration

Entry Number: 1/
[1] Host Name: www.vanguardms.com/
[1] Source IP Address: 0.0.0.0/
[1] Source IP Address Mask: 255.255.255.255/
[1] Meter Point Entry List: ALL/
[1] Exception Entry Number: 0/
```

Figure 10. Traffic Monitor Source IP Address Configuration

A maximum of 63 records (entry numbers 1 to 64) can be defined. The individual parameters are defined in the following sections.

Host Name

Range:	0 to 36 Alphanumeric characters
Default:	www.vanguardms.com
Description:	This parameter specifies the symbolic user name of IP address. Use the space bar to blank the field.
Boot Type:	Source IP Monitor Table Boot.

Source IP Address

Range:	A valid IP address in dotted notation
Default:	0.0.0.0
Description:	This parameter specifies the address for comparing with source IP address of the incoming packet. 0.0.0.0 indicates a packet with any address.
Boot Type:	Source IP Monitor Table Boot.

Source IP Address Mask

Range:	A valid IP address in dotted notation
Default:	255.255.255.255
Description:	This parameter specifies the Address Mask for the Source IP Address. The mask along with the configured Source IP Address specifies a range of IP addresses to be compared with the Source IP Address of the incoming packet. For example, an address 130.25.2.10 with a mask of 255.255.255.240 is equivalent to an address range from 130.25.2.0 to 130.25.2.15. An address 130.25.2.10 with a mask of 0.255.255.0 is equivalent to all the addresses falling in *.25.2.*, where the wild card * is 0 to 255. An address 130.25.2.10 with a mask of 255.255.255.0 specifies the whole sub-net 130.25.2.*. A mask of 255.255.255.255 specifies only the configured address.
Boot Type:	Source IP Monitor Table Boot.

Meter Point Entry List

Range:	1 to 16, ALL
Default:	ALL
Description:	This parameter specifies an entry number of a meter point which a packet is captured. A maximum of 16 ranges are permitted to be configured in this list (for example: 1, 2, 5). • ALL: This option is a wildcard used to match all meter ports.
Boot Type:	Source IP Monitor Table Boot

Exception Entry Number

Range:	0 to 255
Default:	0
Description:	This parameter specifies the exception table entry number. 0 indicates that there is no exception defined for this value.
Boot Type:	Source IP Monitor Table Boot.

Configure Destination IP Monitor Table

Selecting the "Configure Destination IP Monitor Table" entry from the "Configure Traffic Monitor" menu allows the user to configure destination IP address monitor configuration records. Each record specifies an aspect value to be monitored. The entry number of the destination IP address monitor configuration record uniquely identifies the definition. Figure 11 shows an example of a destination IP address monitor record configuration screen.

```
#Enter Selection: 5
Traffic Monitor Destination IP address Configuration

Entry Number: 1/
[1] Host Name: www.vanguardms.com/
[1] Destination IP Address: 0.0.0.0/
[1] Destination IP Address Mask: 255.255.255.255/
[1] Meter Port Entry List: 1,5/
[1] Exception Entry Number: 2/
```

Figure 11. Traffic Monitor Destination IP Address Configuration

A maximum of 63 records (entry numbers 1 to 64) can be defined. The individual parameters are defined in the following sections.

Host Name

Range:	0 to 36 Alphanumeric characters
Default:	www.vanguardms.com
Description:	This parameter specifies the string that is used to represent the IP Address in displays and reports. Use the space bar to blank the fields.
Boot Type:	Destination IP Monitor Table Boot.

Destination IP Address

Range:	A valid IP address in dotted notation.
Default:	0.0.0.0
Description:	This parameter specifies the address for comparing with the destination IP address of the incoming packet. • 0.0.0.0 indicates “packet with any address”.
Boot Type:	Destination IP Monitor Table Boot.

Destination IP Address Mask

Range:	A valid IP address in dotted notation.
Default:	255.255.255.255
Description:	This parameter specifies the Address Mask for the Destination IP Address. The mask along with the configured Source IP Address specifies a range of IP addresses to be compared with the Source IP Address of the incoming packet. For example, an address 130.25.2.10 with a mask of 255.255.255.240 is equivalent to an address range from 130.25.2.0 to 130.25.2.15. An address 130.25.2.10 with a mask of 0.255.255.0 is equivalent to all the addresses falling in *.25.2.*, where the wild card * is 0 to 255. An address 130.25.2.10 with a mask of 255.255.255.0 specifies the whole sub-net 130.25.2.*. A mask of 255.255.255.255 specifies only the configured address.
Boot Type:	Destination IP Monitor Table Boot.

Meter Point Entry List

Range:	1 to 16, ALL
Default:	ALL
Description:	This parameter specifies an entry number of a meter point which a packet is captured. A maximum of 16 ranges are permitted to be configured in this list (for example: 1, 2, 5) • ALL: This option is a wildcard used to match all meter ports.
Boot Type:	Destination IP Monitor Table Boot.

Exception Entry Number

Range:	0 to 255
Default:	0
Description:	This parameter specifies the exception table entry number.
Boot Type:	Destination IP Monitor Table Boot.

Configure TOS Value Monitor Table

Selecting the “Configure TOS Value Monitor Table” entry from the “Configure Traffic Monitor” menu allows the user to configure TOS Value monitor configuration records. Each record record uniquely identifies the definition. An example TOS value monitor record configuration screen is provided (see Figure 12) that specifies an aspect value to be monitored. Also shown is the entry number of the TOS value monitor configuration.

```
#Enter Selection: 6

      Traffic Monitor Tos Value Configuration

Entry Number: 1/
[1] TOS Value: 0/
[1] Meter Point Entry List: ALL/
[1] Exception Entry Number: 0/
```

Figure 12. Traffic Monitor TOS Value Configuration

A maximum of 63 records (entry numbers 1 to 64) can be defined. The individual parameters are defined in the following sections.

TOS Value

Range:	0 to 63
Default:	0
Description:	This parameter specifies the TOS value.
Boot Type:	TOS Value Table Boot

Meter Point Entry List

Range:	1 to 16, ALL
Default:	ALL
Description:	This parameter specifies an entry number of a meter point which a packet is captured. A maximum of 16 ranges are permitted to be configured in this list (for example: 1, 2, 5). • ALL: This option is a wildcard used to match all meter ports.
Boot Type:	TOS Value Table Boot

Exception Entry Number

Range:	0 to 255
Default:	0
Description:	This parameter specifies the exception table entry number.
Boot Type:	TOS Value Table Boot

Configure Protocol Type Monitor Table

Selecting the “Configure Protocol Type Monitor Table” entry from the “Configure Traffic Monitor” menu allows the user to Configure Protocol Type monitor configuration records. Each record record uniquely identifies the definition. An example IP Protocol Type monitor record configuration screen is provided (see Figure 12) that specifies an aspect value to be monitored. Also shown is the entry number of the IP Protocol Type monitor configuration.

```
#Enter Selection: 7

      Traffic Monitor Protocol Type Configuration

Entry Number: 1/
[1] Protocol Type Keyword: ICMP/
[1] Protocol Number: 1/
[1] Meter Point Entry List: ALL/
[1] Exception Entry Number: 0/
```

Figure 13. Traffic Monitor Protocol Type Configuration

A maximum of 255 records (entry numbers 1 to 256) can be defined. The individual parameters are defined in the following sections.

Protocol Type Keyword

Range:	0 to 10 Alphanumeric characters
Default:	ICMP
Description:	This parameter specifies the Internet Protocol Type Keyword name (for example: ICMP, OSPF, BGP, IGGP, etc.). Use the space bar to blank the field.
Boot Type:	IP Protocol Type Table Boot

Protocol Number

Range:	0 to 64555
Default:	1
Description:	This parameter specifies the Internet Protocol number.
Boot Type:	IP Protocol Type Table Boot

Meter Point Entry List

Range:	1 to 16, ALL
Default:	ALL
Description:	This parameter specifies an entry number of a meter point which a packet is captured. A maximum of 16 ranges are permitted to be configured in this list (for example: 1, 2, 5). • ALL: This option is a wildcard used to match all meter ports.
Boot Type:	IP Protocol Type Table Boot

Exception Entry Number

Range:	0 to 255
Default:	0
Description:	This parameter specifies the exception table entry number.
Boot Type:	IP Protocol Type Table Boot

Configure Ethernet Type Monitor Table

Selecting the “Configure Ethernet Type Monitor Table” entry from the “Configure Traffic Monitor” menu allows the user to configure Ethernet Type monitor configuration records. Each record specifies an aspect value to be monitored. The entry number of the Ethernet Type monitor configuration record uniquely identifies the definition. An example Ethernet Type monitor record configuration screen is provided below.

```
#Enter Selection: 8

      Traffic Monitor Ethernet Type Configuration

Entry Number: 1/
[1] Ethernet Type Name: IP/
[1] Ethernet Type: 0800/
[1] Meter Point Entry List: ALL/
[1] Exception Entry Number: 0/
```

Figure 14. Traffic Monitor Ethertype Configuration

A maximum of 63 records (entry numbers 1 to 64) can be defined. The individual parameters are defined in the following sections.

Ethernet Type Name

Range:	0 to 36 Alphanumeric characters
Default:	IP
Description:	This parameter specifies the Ethernet Type name (for example: ARP, APPLE, IPX, IBM, etc.).
Boot Type:	Ethernet Type Monitor Table Boot.

Ethernet Type

Range:	0000-FFFF (Hexidecimal)
Default:	0800
Description:	This parameter specifies the Ethernet type Hex value.
Boot Type:	Ethernet Type Monitor Table Boot.

Meter Point Entry List

Range:	1 to 16, ALL
Default:	ALL
Description:	This parameter specifies an entry number of a meter point which a packet is captured. A maximum of 16 ranges are permitted to be configured in this list (for example: 1, 2, 5). • ALL: This option is a wildcard used to match all meter ports
Boot Type:	Ethernet Type Monitor Table Boot.

Exception Entry Number

Range:	0 to 255
Default:	0
Description:	This parameter specifies the exception table entry number.
Boot Type:	Ethernet Type Monitor Table Boot.

Boot Types

Introduction

This section discusses the new boot types added to support the traffic monitor feature and the impact of the various boot types on the traffic monitor features.

Boot Menu

The “Boot Traffic Monitor” menu entry has been added to the boot menu. When this entry is selected the following new menu is displayed.

```
Node: Nodename  Address: (blank)        Date:  2-FEB-2004  Time: 17:03:16
Menu: Boot Traffic Monitor              Path: (Main.7.10)

  1.  Boot Meter Point Table
  2.  Boot Except Table
  3.  Boot Application Monitor Table
  4.  Boot Source IP Monitor Table
  5.  Boot Destination IP Monitor Table
  6.  Boot Tos Value Table
  7.  Boot Protocol Type Table
  8.  Boot Ethernet Type Table


#Enter Selection:
```

Figure 15. Boot Traffic Monitor

Boot	Effect
Boot Meter Point Table	• Reset current and historical statistics for all aspects • Load updated configurations records
Boot Except Table	• Load updated configurations records
Boot Application Monitor Table	• Reset current and historical statistics for application aspect • Load updated application monitor records
Boot Source IP Monitor Table	• Reset current and historical statistics for Source IP aspect • Load updated Source monitor records
Boot Destination IP Monitor Table	• Reset current and historical statistics for Destination IP aspect • Load updated Destination IP monitor records
Boot TOS Value Table	• Reset current and historical statistics for Type of Service (ToS) value aspect • Load updated ToS value monitor records

Boot	Effect
Boot Protocol Type Table	• Reset current and historical statistics for Protocol Type aspect • Load updated Protocol Type monitor records
Boot Ethernet Type Monitor Table	• Reset current and historical statistics for Ethernet Type aspect • Load updated Ethernet Type monitor records.

List and Examine

Configuration records can be displayed through the standard List and Examine Menus.

Statistics

Traffic Monitor Statistics

The "Traffic Monitor Statistics" menu entry has been added to the statistics menu. When this entry is selected the following new menu is displayed:
Main Menu->Status/Statistics->Traffic Monitor Statistics

```
Node: Nodename  Address: (blank)            Date: 19-DEC-2003  Time: 13:48:50
Menu: Traffic Monitor Statistics            Path: (Main.5.24)

  1.  Monitor Statistics
  2.  Discovery Statistics
```

Figure 16. Traffic Monitor Statistics

```
Node: Nodename  Address: (blank)          Date:  2-FEB-2004  Time: 17:22:14
Menu: Monitor Statistics                  Path: (Main.5.15.1)

  1.  Application
  2.  Source IP
  3.  Destination IP
  4.  TOS
  5.  Protocol Type
  6.  Ether Type

#Enter Selection:
```

Figure 17. Monitor Statistics

Monitor Statistics Screen Format

The monitor statistics screen displays the statistics for the configured monitor aspect values.

```
Traffic Monitor is Disabled at Meter Port=1
------------------------------------------------------------------------
   <Aspect Name>     In/Out(bps)  In/Out(bytes)  In/Out(Pkt Num)
------------------------------------------------------------------------
       FTP DATA        0/    0        0/    0          0/    0
    FTP CONTROL        0/    0        0/    0          0/    0
         TELNET        0/    0        0/    0          0/    0
           SMTP        0/    0        0/    0          0/    0
           TFTP        0/    0        0/    0          0/    0
           HTTP        0/    0        0/    0          0/    0
           X400        0/    0        0/    0          0/    0
           POP3        0/    0        0/    0          0/    0
           SNTP        0/    0        0/    0          0/    0
           SNMP        0/    0        0/    0          0/    0
         RLOGIN        0/    0        0/    0          0/    0

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

Figure 18. Monitor Statistics

Discovery Statistics

Figure 19 shows the Discovery Statistics:

```
Node: Nodename  Address: (blank)          Date:  2-FEB-2004  Time: 17:22:38
Menu: Discovery Statistics               Path: (Main.5.15.2)

  1.  Application
  2.  Source IP
  3.  Destination IP
  4.  Ether Type

#Enter Selection:
```

Figure 19. Discovery Statistics Menu

```
Traffic Discovery is Disabled at Meter Port=1
-------------------------------------------------------------------
 <Aspect Name> In/Out(bps)  In/Out(bytes)  In/Out(Pkt Num)
-------------------------------------------------------------------
```

Figure 20. Discovery Statistics Format

Screen Terms

Statistic	Description
Meter Port	The port number to which the statistics apply.
Aspect Name	The following labels are used to indicate the aspect being displayed. • TOS Value • SrcIp Address • DstIP Address • Protocol Type • Ethernet Type

Index