Administrator Guide

CA Multi-Port Monitor

Version 10.2

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: What is Multi-Port Monitor?

CA Application Delivery Analysis Multi-Port Monitor is a powerful appliance that captures session-level packet data from a monitored data center. The appliance captures the data for reporting in CA Application Delivery Analysis and CA Application Performance Management (CA APM).

- Data from the TCP packet headers help CA Application Delivery Analysis monitor end-to-end performance to measure application response time.
- Data from full HTTP packets help CA APM map transactions in your environment to monitor the end-user experience and measure service-level agreements.

By passively monitoring large volumes of data center traffic from multiple ports, Multi-Port Monitor helps keep a continuous record of end-to-end system performance.

Packet headers from all traffic passing through the monitored mirrored ports are recorded and stored on Multi-Port Monitor for a short time. Data from 1-minute reporting intervals is kept for a few days and provided for analysis. Metrics are forwarded to CA Application Delivery Analysis for reporting or to CA Transaction Impact Manager (CA TIM), for reporting in CA APM.

Charts and tables in a Multi-Port Monitor analysis show per-host activity and performance data. An analysis offers multiple views of sessions data, volume statistics, and response times. An analysis also offers work flows for troubleshooting, several options for exporting data, and filtering options to help IT staff diagnose and respond to issues.

Multi-Port Monitor offers features to monitor its functionality.

- Hardware-based filtering and packet-capturing options per logical port.
- Hardware filters to calibrate performance and capture only the data of interest.
- Multiple data feeds administered from one web page.
- SNMP traps send an automatic notification about errors that can affect data monitoring or capture.

Multi-Port Monitor includes the following components:

Appliance

Hardware and software that monitor traffic that flows into and out of a switch. Performs the following functions:

- Captures packets and writes them to storage.
- Collects traffic statistics and analyzes packets for performance information.
- Stores statistical data about the network, server, and application performance in a high-performance database.
- Sends statistical data to CA TIM or CA Application Delivery Analysis for reporting and analysis.

Web interface

An administrative interface, accessible from a browser, that lets you:

- View appliance statistics, including drive, CPU, and capture card status.
- Configure system settings, such as port definitions, filtering options, and secure user accounts.
- View, filter, and sort performance data that is based on captured packets and presented in formatted charts or tables.
- Review locally stored session-level data on the Analysis tab.

Chapter 2: How to Log In to the Web Interface

Log in to the web interface to perform administrative tasks, such as monitoring Multi-Port Monitor system health.

Follow these steps:

1. Access the web interface in a web browser. Use the following syntax in the browser Address field:

   `http://<hostname or IP address>/`

   The Multi-Port Monitor Login page opens.

2. Log in using your assigned case-sensitive user name and password. The following are the default values.

   - User name: admin
   - Password: admin

   The web interface opens.

More information

Change the Password of the Administrator Account (see page 12)

Chapter 3: Recommended Configuration

Multi-Port Monitor is designed to run with minimal configuration. However, the administrator can organize, secure, and customize the system after installing the hardware and the Multi-Port Monitor software.

Note: Installation tasks are discussed in the *CA Application Delivery Analysis Multi-Port Monitor Installation Guide*.

This section contains the following topics:

Configure a Trusted Internet Site

To improve web interface performance, add the host name of the appliance to the list of trusted internet sites. Microsoft Internet Explorer uses high security settings that restrict navigation to trusted sites.

In Internet Explorer, you can add the host name to the list of Trusted Sites by clicking Tools, Internet Options, Security.

Change the Password of the Administrator Account

Multi-Port Monitor ships with predefined user accounts that provide different product privileges. The default Administrator account provides access to all configuration options. Change the password for this account in the following situations:

- Multi-Port Monitor is scheduled to be a monitoring device for CA Application Delivery Analysis, but CA Application Delivery Analysis is not yet deployed.

  Note: After CA Application Delivery Analysis is deployed, Multi-Port Monitor retrieves all user and role information, including passwords, from CA Application Delivery Analysis.

- Multi-Port Monitor is deployed only with CA TIM in a CA APM environment.

Follow these steps:

1. Click Administration, Users in the web interface.

   The User Accounts page opens.

2. Click the Edit link for the admin account.

   The Edit User page opens.

3. (*Optional*) Edit the default text in the Description field to mention that the default password has been changed. Although optional, this step is a best practice.

4. Delete the encrypted text and type the new password in the Password and Confirm Password fields.

5. Select the Enabled check box. This setting prevents you from accidentally disabling the account under which you are logged in to the web interface.

6. Click Save.

   The new password is saved.

More information:

What are Users and Roles? (see page 29)

Verify Packet Flow Through Ports

Verify that packets flow through the ports to determine that installation of the hardware and software was successful.

Follow these steps:

1. Click System Status in the web interface.
2. Review the Capture Card Physical Port Status section for the following information:
   - Which ports are connected on the adapter.
   - The number of packets that are received through each port.

   Configuration is successful if the ports are active.

Verify VLAN Identifiers

When CA Application Delivery Analysis assigns tagged VLAN traffic on a logical port to a domain, we recommend that you verify the traffic which is mirrored to the logical port is tagged properly. Make sure:

- VLAN traffic is tagged in both directions.

  To properly compute 1-minute metrics, the logical port must receive tagged VLAN traffic between both the server and the client. The Analysis page does not report 1-minute metrics for sessions that are only tagged in a single direction.

  If only one direction has VLAN tags:

  - Under TCP conversations, sessions are listed with no metrics except one packet in either the To or From direction.
  - On the Analysis page, the traffic is reported as two separate, one-way sessions.
- VLAN traffic is tagged with a single VLAN identifier.

  Multi-Port Monitor identifies VLAN traffic by the first VLAN identifier in the packet header. If your traffic is tagged with more than one VLAN identifier, and the order of the VLAN identifiers varies, Multi-Port Monitor cannot properly monitor the traffic.

Configure Logical Ports

The Multi-Port Monitor appliance has two, four, or eight physical ports through which it receives data from switches in your network. When connected to a mirrored port, a physical port is assigned a logical port definition that corresponds to its ID number on the Multi-Port Monitor adapter.

Associate a name with a logical port to make it easier to identify the monitor feed in CA Application Delivery Analysis for the TIM. You can change the default logical port definitions.

CA CEM TIM does not support VLAN-based monitor feeds. Do not assign VLAN traffic on the logical port for the TIM to domains.

Logical port settings also let you limit the amount of data that is captured and monitored from each mirror session. Port filters determine the segments of the network or hosts that are monitored and the types of data to include or exclude from capture files.

CA Transaction Impact Monitor (CA TIM) monitors mirrored ports from one logical port, despite the availability of multiple logical ports on the Multi-Port Monitor appliance. To map multiple physical ports to one logical port, mirror the web traffic from the WAN to the logical port. This traffic is processed for CA TIM and CA CA Application Delivery Analysis. Use the other logical ports for other port mirroring, ideally from the access-layer switches closest to the servers. The non-TIM logical ports are processed for CA Application Delivery Analysis only.

Follow these steps:

1. Click Administration, Logical Ports in the web interface. The Logical Ports page opens.
2. Provide a new name for the port in the Name field. The name helps to identify the source of the traffic you want to monitor, such as the name or location of a core switch.
3. Select Enabled to enable the port for monitoring.
4. (*Optional*) Select 'Save Packets To Disk' to save captured data packets on the hard disk drive of the appliance.

   Note: When this option is disabled, packets are affected in the following ways:

   - Packet capture files are not saved.
   - Packet capture files are not available for packet capture investigations that are launched from CA Application Delivery Analysis.
   - Packet capture files are not available for the Export to PCAP feature.

5. Select 'TIM' to identify the port you are configuring as a CA TIM port. This check box is available only when CA TIM is installed on the Multi-Port Monitor appliance. You can also use this option to disable or enable packets to the TIM.

   Note: When this option is disabled, packets are affected in the following ways:

   - Packets are not sent to the TIM.
   - The logical port filter settings for the TIM are preserved.

6. Click Filters to enable a hardware filter for the port you are configuring. For more information, see Using Hardware Filters to Manage Data (see page 16).

   Web traffic that CA TIM monitors must have full packets.

7. Select a check box to assign (map) a physical port to the logical port. The number of available ports depends on the capture card configuration you purchased. You can map two or more physical ports to one logical port. This configuration provides more accurate monitoring in environments with asymmetrical routing, and lets you monitor primary and failover circuits.

   Logical port numbering begins at 0. The capture layer maps physical ports to logical ports. The mapping process is transparent to CA TIM.

8. Click Save.
9. Repeat steps 2 through 8 for each port you want to configure.
10. Restart (see page 47) the nqcapd process if you changed any parameter other than the Name field.
11. (*Optional*) Review the status of the logical ports in the Capture Card Logical Port Status table on the System Status page.

More information:

Capture Card Logical Port Status (see page 40)
What is Packet Slicing? (see page 16)
Regular Expression Syntax (see page 67)

Using Hardware Filters to Manage Data

Hardware filters can further refine the data that is processed from your switches and thus optimize Multi-Port Monitor performance. For example:

- If data volume is heavy on your network, you can apply filtering or packet slicing to selected logical port definitions.
- You can refine the capture of data by selecting specific IP addresses or subnets.

Filtering options include prioritization and packet inclusion or exclusion per-protocol, per-VLAN, per-subnet or IP address, and per-port. The packet-slicing feature lets you limit the portion or size of the packets that are written to disk.

Multi-Port Monitor filtering and packet-slicing options are applied on a per-port basis, as part of logical port definition. You can set the filter priority to determine the order in which filters are applied.

Hardware filters are distinct from the analysis filters you can apply to captured data.

- Hardware filters affect the *capture* of data.
- Analysis filters affect the *display* of data.

Traffic is captured when a packet matches the criteria of an enabled filter. Filters with overlapping instructions are applied in order according to their Priority settings. The capture card provides a limited number of hardware filtering resources. Use these filters to refine the limitations on mirrored traffic.

Tip: You can use hardware filters to refine the captured data. However, do not use hardware filters in place of properly configured mirror ports, which filter the data before it is captured.

More information:

Port Mirroring (see page 62)
Configure Logical Ports (see page 14)

What is Packet Slicing?

Multi-Port Monitor filters include a packet-slicing option that lets you selectively discard parts of a frame as it is captured.

Packet slicing is typically deployed when data volumes are high and the data of interest is in the packet headers. The packet payload is not typically needed for CA Application Delivery Analysis monitoring. Packet slicing reduces Multi-Port Monitor load and uses fewer resources for storing capture files.

The "All Traffic — headers only" filter specifies that all types of packets are captured and sliced to retain only their headers. The filter slices a packet to the size of the frame through the header, plus one byte of payload. Unless you add a filter or edit this filter, packet slicing is applied to all new logical port definitions on new installations. This filter maximizes Multi-Port Monitor performance while still capturing all data needed for monitoring with CA Application Delivery Analysis.

The network adapter that is installed on the Multi-Port Monitor appliance offers options for slicing packets, including fixed-length truncation and dynamic, per-protocol truncation. The capture card performs two types of slicing:

Fixed slicing

The frame size is truncated to a maximum specified length that you can set in bytes.

Dynamic slicing

The frame size is truncated to a maximum length after the header is included, for example, the full TCP header plus 8 bytes of payload. The card considers encapsulations or TCP options when calculating the place where payload data is discarded.

What are the Default Hardware Filters?

Hardware filters specify the protocols, servers, and ports that are monitored by a logical port. The capture card applies more than one hardware filter based on the priority you specify. For more granular captures, you can filter particular IP addresses or TCP ports.

When multiple hardware filters are created on a logical port, they are treated as an OR. Traffic is captured if it matches the criteria specified by any hardware filter. The filter Priority indicates the order in which the filters are applied. So, if there is overlapping criteria in the filters, the priority can be used to determine other options such as slicing.

To maximize the available system resources, we recommend filtering to the traffic of interest. Create a hardware filter or use the hardware filters provided with the CA Multi-Port Monitor:

All Traffic — headers only

Captures header information plus one payload byte for all protocols. This filter is Enabled by default. Use this filter with:

- CA Multi-Port Monitor. Includes volume metrics for non-TCP traffic
- CA Application Delivery Analysis. Packet capture investigations include headers only

HTTP — full packets

Captures HTTP packets with full payloads on Port 80 and Port 443. This filter is Disabled by default. Use this filter with:

- CA TIM
- CA Application Delivery Analysis. Packet capture investigations for Web applications include full packets

TCP — headers only

Captures header information plus one payload byte for TCP protocol; packets from all other protocols are discarded. This filter is Disabled by default. Use this filter with:

- CA Multi-Port Monitor. Does not include volume metrics for non-TCP traffic
- CA Application Delivery Analysis. Packet capture investigations include headers only

Configure a Hardware Filter

You can create, enable, disable, and modify predefined filters and the filters that you created. For example, if you want to temporarily disable a filter while preserving its filter settings, disable the filter.

When configuring a hardware filter, the criteria listed in a single field, such as the IP Address, is treated as an OR. For example, if you specify a list of IP addresses, packets will match the filter if the packets source or destination addresses matches any IP address in the list.

If multiple fields are used, then the criteria for each field is treated as an AND. So, for example, if you specify both a list of IP addresses and a port number, then the packets would match the filter if the source or destination address matches any IP address in the list AND the source or destination port matched the port specified.

If you click on the "Show Details" link of the hardware filter, you will see the logic used when combining the different fields. The syntax follows what is required by Napatech to specify the hardware filters; the keywords such as mIPSrcAddr, mIPDestAddr, mTCPSrcPort, mTCPDestPort are macros that indicate the field of the packet.

If you want to create more sophisticated filters, you can use the Advanced Hardware Filter page to build up the expression.

Follow these steps:

1. Click Administration, Logical Ports in the web interface. The Logical Ports page opens.
2. Click the Filters link in the Edit Filters column for the logical port that you want to filter. The Logical Ports: Hardware Filters page opens.
3. *To create a filter, click New*. The Logical Ports: New Hardware Filter page opens.
    a. Complete the following fields:
        - **Filter Enabled**. Select this option to apply the filter. Packets that pass the filter are analyzed based on the options below:

          Send Packets to ADA. Filtered packets are analyzed for network-level metrics and displayed in the Analysis tab of the Multi-Port Monitor web interface and sent to the Application Delivery Analysis console based on the console's configuration. This option is always selected and cannot be turned off.

          Send Packets to TIM. Filtered packets are analyzed for application-level metrics and events by the CA APM Transaction Impact Manager (TIM) on the Multi-Port Monitor. The TIM must be installed to display this option.

          Filter Name. The name of the filter you are creating or editing. The filter name is shown on the Hardware Filters page for the logical port to which it is applied.

- **Filter Priority**. Priority determines which filters take precedence when filter criteria overlap. That precedence is undefined when two or more overlapping filters have the same priority. Values range from 0 (highest priority) to 62 (lowest priority). The default priority is 10.

  Filter priority settings can be used with packet slicing. For example, you want to keep more bytes of each HTTP packet. You specify a filter for TCP and Port 80, with slicing set to 'TCP headers + 50 bytes' and Priority set to 1. You then specify another filter for TCP, with slicing set to 'TCP headers + 1 byte' and Priority set to 10. In this scenario, more payload bytes are kept for HTTP traffic than for other TCP traffic.

- **Packet Slicing Mode**. Options for capturing only selected parts of each packet. The hardware filters let you capture packets for protocols other than TCP/IP. However, Multi-Port Monitor collects performance metrics only for TCP traffic. Volume metrics are collected for all traffic types.

  Capture full packet: All information is captured from each packet that passes the filter.

  Capture fixed size: Some bytes are captured from every packet. In the Packet Slicing Size field, supply the number of bytes to capture.

  Capture headers plus size: All Layer 2, Layer 3, and Layer 4 headers are captured, plus the fixed number of payload bytes from the 'Packet Slicing Size' field. Layer 2 headers include Ether II, LLC, SNAP, and Raw headers, and VLAN, ISL, and MPLS tags. Layer 3 headers include IPv4 (including IPv4 options) and IPX headers. Layer 4 headers include TCP, UDP, and ICMP headers.

- **Include only Protocols**. Limits the protocols to capture and process. Only the selected protocols are included in monitoring. If no check boxes are selected, all protocols are included. Transport Control Protocol (TCP) is the main protocol that CA Application Delivery Analysis monitors. User Datagram Protocol (UDP) is used for transport of the data that real-time or streaming applications send. Internet Control Message Protocol (ICMP) is used for error messaging among servers and for CA Application Delivery Analysis traceroute investigations.

- **VLANs**. The identifiers of the virtual local area networks (VLANs) to monitor or exclude from monitoring. List the identifiers of VLANs whose traffic passes through the indicated logical port. Separate multiple VLANs with commas and no spaces. Select Exclude to discard traffic from the VLANs you listed.

- **Subnets**. The subnets to monitor or exclude from monitoring. Supply a valid IPv4 address and subnet mask. Select Exclude to discard traffic from the subnets you listed.

  Use the following format for IPv4 addresses: x.x.x.x/*n*, where x.x.x.x is the IPv4 subnet address in dotted notation and *n* is the number of bits to use for the mask.

- **IP Addresses**. The IPv4 addresses, or range of addresses, of individual hosts to monitor or exclude from monitoring. Separate multiple addresses with commas and no spaces. Separate ranges with a hyphen and no spaces. Select Exclude to discard traffic from the addresses you listed.

  Use dotted notation for IPv4 addresses. For example, 10.9.7.7,10.9.8.5-10.9.8.7

- **Ports**. The TCP ports or port ranges to monitor or exclude from monitoring. Separate multiple port numbers with commas and no spaces. For a range of ports, use the following format: 2483-2484. Select Exclude to discard traffic from the ports you listed.

b. (*Optional*) Click Advanced to use regular expressions to create more precise filters (see page 21).

c. Click Save. The new filter appears on the Logical Ports: Edit Hardware Filter Page.

4. *To modify or enable a filter*, click Edit. The Logical Ports: Edit Hardware Filter page opens.

   a. Complete the fields as described in step 3a.

   b. (*Optional*) Click 'Show Details' to view your selections as a regular expression.

   c. Click Save. The revised filter appears on the Logical Ports: Hardware Filters page.

5. Restart (see page 47) the nqcapd process to apply your changes.

Use Regular Expressions for Precise Filtering

Hardware filters can include regular expressions that precisely control the data that is captured or discarded. You can apply regular expressions when you create a filter.

Follow these steps:

1. Create a hardware filter.
2. Click Advanced on the Logical Ports: New Hardware Filter page. The Logical Ports: New Advanced Hardware Filter page opens.
3. Complete the following fields:

   - **Filter Enabled**. Applies the filter on the logical port whose name is indicated. If selected, the filter is applied after you restart the nqcapd process.

   - **Filter Name**. The name of the filter you are creating or editing. The filter name is shown on the Hardware Filters page for the logical port to which it is applied.

- **Filter Priority**. Priority determines which filters take precedence when filter criteria overlap. That precedence is undefined when two or more overlapping filters have the same priority. Values range from 0 (highest priority) to 62 (lowest priority). The default priority is 10.

  Filter priority settings can be used with packet slicing. For example, you want to keep more bytes of each HTTP packet. You specify a filter for TCP and Port 80, with slicing set to 'TCP headers + 50 bytes' and Priority set to 1. You then specify another filter for TCP, with slicing set to 'TCP headers + 1 byte' and Priority set to 10. In this scenario, more payload bytes are kept for HTTP traffic than for other TCP traffic.

- **Packet Slicing Mode**. Options for capturing only selected parts of each packet. The hardware filters let you capture packets for protocols other than TCP/IP. However, Multi-Port Monitor collects performance metrics only for TCP traffic. Volume metrics are collected for all traffic types.

  - Capture full packet: All information is captured from each packet that passes the filter.
  - Capture fixed size: Some bytes are captured from every packet. In the Packet Slicing Size field, supply the number of bytes to capture.
  - Capture headers plus size: All Layer 2, Layer 3, and Layer 4 headers are captured, plus the fixed number of payload bytes from the Packet Slicing Size field. Layer 2 headers include Ether II, LLC, SNAP, and Raw headers, and VLAN, ISL, and MPLS tags. Layer 3 headers include IPv4 (including IPv4 options) and IPX headers. Layer 4 headers include TCP, UDP, and ICMP headers.

4. In the Field lists and the blank field, build your expression. All packets that *match* the filter syntax are captured. Wildcards are not accepted.

   a. From the first list, select the field from the packet header on which you want to filter. By default, the filter *includes* traffic. You select items that correspond to that data from the traffic at the logical port where the filter is applied. To create a filter that *excludes* traffic, specify all traffic *except* for the traffic you want to exclude.

      - **VLAN ID**: The identifier of the virtual LAN (VLAN) whose data you want to include. Specify the VLAN IDs to include as a comma-separated list in the empty field provided. For example, to include traffic from VLANs 165 and 140, enter 165,140. If you did not add filtering to this logical port, the packets with either of these VLAN identifiers is captured. You can also specify a range of VLANs, such as 140-165. Such a filter is inclusive.

- **Encapsulation**: The encapsulation that is applied to a packet. Supply a value for the type of encapsulation to include from capture files. The following values are valid:

  VLAN: A category that includes all packets with a VLAN header in the filter operation.

  MPLS: The Multiprotocol Label Switching network architecture. MPLS affixes a header to each packet containing labels to control packet routing, including quality of service and TTL information.

  ISL: A proprietary Cisco VLAN encapsulation method for high-performance links.

- **Layer 3 Protocol**: The Layer 3 protocol to include in the filter operation. If you select this option, then specify one protocol, or a comma-separated list of protocols. Valid values are IP and IPv4.

- **Layer 4 Protocol**: The Layer 4 protocol to include in the filter operation. Specify one protocol or a comma-separated list of protocols. Valid values are TCP, UDP, and ICMP.

- **IPv4 Source Subnet**, **IPv4 Destination Subnet**: The IP address of the subnet to include in the filter operation. Select IPv4 Source Subnet or IPv4 Destination Subnet, or click the AND or OR button to add them both to the regular expression. The filter is applied to the Source or Destination field in the packet header. Provide an IP address and the number of bits in the subnet mask. Use the following syntax: 123.45.67.0/24.

- **IPv4 Source IP Address**, **IPv4 Destination IP Address**: The full IPv4 address of the host to include in the filter operation. The filter is applied to the Source or Destination field in the packet header. You can enter one IPv4 address, a comma-separated list, or a range. Use standard syntax, such as 123.45.67.89, or 123.45.67.8,123.45.67.15, or 123.45.67.8-123.45.67.15.

- **TCP Source Port**, **TCP Destination Port**: A single port number, a comma-separated list of port numbers, or a hyphenated range of port numbers to include in the filter operation. The filter is applied to the Source or Destination port fields in the packet header.

b. Select a condition from the second list: Equals (==) or Not Equals (!=).

c. In the blank field, type the value that is associated with your selection in step a.

d. (*Optional*) To add more conditions to the filter, click one of the Boolean operator buttons, AND or OR, and then repeat steps a through d.

   The filter syntax appears in the Conditions field.

5. Click Save. The filter appears on the Logical Ports: Hardware Filters page.

6. Restart (see page 47) the nqcapd process if you enabled a filter.

Set Global Preferences

You can configure global settings that affect the way data is automatically collected, stored, and forwarded, such as the following settings:

- The number of hours to retain packet capture files.
- The frequency of automatic database maintenance.
- Whether packet deduplication is enabled.

In most cases, the default settings are appropriate. However, you can change the settings to ensure the optimal functioning of your system.

Follow these steps:

1. Click Administration, Application Settings in the web interface. The Application Settings page opens.
2. Complete the following fields:
   - **Perform automatic file maintenance every**. The number of minutes between automatic file maintenance operations. If necessary, the oldest raw packet capture files are deleted during maintenance. This setting determines the frequency of capture file deletion. The default is 5. If you change this setting, restart the nqmaintd process. The threshold for removing raw packets also affects the frequency of file deletion.
   - **When disk space usage is normal, keep raw packet capture files for**. The length of time raw packet capture files are stored before being automatically deleted. These files are continually generated during ordinary monitoring. The default is 6. If you change this setting, restart the nqmaintd process.
   - **Automatically remove raw packet capture files older than one hour when disk utilization reaches**. The maximum percentage of disk space that can be in use before raw packet capture files older than one hour are automatically purged. The automatic file maintenance interval also affects the frequency of file deletion. The default is 80 percent. This threshold does not apply to packet capture investigation files. If you change this setting, restart the nqmaintd process.
   - **Keep Application Delivery Analysis packet capture investigation files for**. The number of days that packet capture investigation files are stored before being automatically deleted. These files are generated in response to a packet capture investigation request from CA Application Delivery Analysis. Packet capture investigation files are stored separately from raw capture files. This threshold does not apply to raw packet capture files. The default is 90. If you change this setting, restart the nqmaintd process.

- **Keep one-minute session metrics for.** The number of days that metric data taken from captured packets are kept in the Multi-Port Monitor database. The default is 7. An internal maximum threshold is applied to this database. Data from fewer than the selected number of days is kept when the number of rows in the database exceeds 12 billion rows. If the threshold is exceeded, the oldest data is discarded first.
- **Perform packet deduplication**. When enabled, Multi-Port Monitor attempts to filter out duplicate packets that can be received from mirrored ports. By default, deduplication is enabled. The System Status page tracks the number of packets that the capture card discarded. If you change this setting, restart the nqcapd process.
- **Encrypt raw packet capture files on disk**. When enabled, raw packet capture files are saved in encrypted format on the Multi-Port Monitor hard disk. By default, these files contain only the header information of all traffic captured. But they can contain payload data when packet slicing options are changed to retain more of the packet. Packet capture investigation files, which are filtered to contain information from a single server, are not encrypted. Encryption is processor-intensive. Enabling this option can degrade the ability of the monitoring device to save packet capture files. A unique key for the encryption is created when you first start Multi-Port Monitor. The key is not changed thereafter. If you change this setting, restart the nqcapd process.

3. Click Save. The Application Settings page is refreshed with your changes.
4. Restart (see page 47) the nqmaintd process or the nqcapd process if necessary.

More information:

Packet Deduplication (see page 63)
Capture Card Physical Port Statistics (see page 41)
Stop or Restart a Process (see page 47)
What is Packet Slicing? (see page 16)
Purge Data from the Database (see page 50)

Create SNMP Traps

The SNMP alerting feature adds a layer of error reporting to the CA Application Delivery Analysis incidents feature. With SNMP alerting, Multi-Port Monitor performs some self-monitoring tasks and sends trap notifications to alert you to conditions that can affect performance.

The nqsnmptrap_[Date].log files identify the conditions that triggered SNMP traps. For more information, see Review System Logs (see page 47).

SNMP traps are sent automatically to a third-party monitoring application when an error condition is detected. You can modify SNMP trap settings to change the reason that traps are sent. Traps are defined in the Management Information Base (MIB) and are sent as SNMP v2 notifications.

Multi-Port Monitor includes a MIB file that contains unique OIDs: CA-MULTI-PORT-MONITOR-MIB. You can review the contents of the MIB file at Administration, SNMP Traps in the web interface.

Prerequisites:

- Configure a trap receiver to communicate with Multi-Port Monitor.
- Import CA-MULTI-PORT-MONITOR-MIB into the trap receiver. The process of importing a MIB file is specific to the trap receiver.

Follow these steps:

1. Click Administration, SNMP Traps in the web interface.

   The SNMP Traps page opens.

2. Type the IP address or host name of the computer where the SNMP trap receiver is installed.

3. Click Save.

   By default, all traps shown in the table are enabled, with a severity level of Warning. This setting means that Info traps are not sent by default. However, traps are sent in response to conditions that meet either the Warning criteria or the Error criteria.

More information:

Review System Logs (see page 47)

SNMP Trap Severity Levels

Multi-Port Monitor SNMP traps are associated with key processes that detect error conditions that affect performance. Error conditions that correspond to the following severities trigger each trap:

- Info (least severe condition)
- Warning (medium-severity condition)
- Error (highest-severity condition)

You can select the minimum severity of traps that you want Multi-Port Monitor to send. Traps are then sent for any condition that meets or exceeds the criteria for the minimum severity. By default, all traps are enabled for a Warning or Error severity, but not for the Info severity.

The following SNMP traps are available:

mtpProcessTrap

This trap is sent when a Multi-Port Monitor process fails or is restarted. The trap text supplies the name of the process that was restarted. The trap is sent by default for the following conditions:

- Warning is sent when the watchdog process restarts another process.
- Error is sent when the watchdog process restarts the same process the maximum number of times.

mtpCaptureTrap

This trap is sent in response to an error or warning message from the network adapter (the capture card). Where applicable, the trap text supplies information to identify the affected adapter.

- Warning is sent when a physical port is no longer connected.
- Error is sent when the nqcapd process encounters a problem while capturing packets.

mtpDiskUsageTrap

This trap is sent when a disk usage threshold is exceeded for a file system.

- Warning is sent when disk usage reaches 80 percent.
- Error is sent when disk usage reaches 95 percent.

Tips:

- The mtpDiskUsageTrap monitors the /nqtmp/headers file system, a RAM disk file system. The /nqtmp/headers file system exceeds a threshold when the nqmetricd process is not sufficiently processing header files. Possible reasons include:
  - The nqmetricd process cannot query the CA Application Delivery Analysis management console for configuration information. Review the nqMetricReader.log file for indications of a SQL error.
  - The Multi-Port Monitor appliance can have resource issues that affect the nqmetricd process. Restart the appliance. If the problem persists or occurs again, contact CA Technical Support.
- The mtpDiskUsageTrap also monitors the /nqtmp/tim file system, a RAM disk file system. The /nqtmp/tim file system exceeds a threshold when the TIM process is not sufficiently processing packet files.

mtpRAIDTrap

This trap is sent in response to a RAID array or disk drive failure.

- Info is sent when a RAID array that was rebuilding returns to an Optimal state.
- Warning is sent when a disk RAID array is degraded because a disk drive is rebuilding.
- Error is sent when either a disk RAID array failure or a degraded disk RAID array due to a disk drive failure is detected.

Note: This trap is available only if the Adaptec Storage Manager (arcconf) utility is installed. For more information, see the *CA ADA Multi-Port Monitor Installation Guide*.

More information:

Process Information (see page 38)
Log In to the Appliance (see page 52)
Review System Logs (see page 47)

Change Trap Behavior

You can change the severity for each type of trap. For mtpDiskUsageTrap, you can also change the usage thresholds. Each type of trap includes several severity parameters. You can select a minimum severity level that can trigger the trap notification. Severity levels range from Info, the least severe, to Error, the most severe.

Follow these steps:

1. Click Administration, SNMP Traps in the web interface.

   The SNMP Traps page displays the IP address or host name of the configured trap receiver and table describing the SNMP traps.

2. Click Edit for the trap you want to disable or change.

   The Edit SNMP Trap Settings page opens.

3. Select the severity level of the trap in the Setting field.

4. Change the value in the "Send Warning trap when disk utilization reaches" field. The default is 80.

   Note: This field applies to mtpDiskUsageTrap.

5. Change the value in the "Send Error trap when disk utilization reaches" field. The default is 95.

   Note: This field applies to mtpDiskUsageTrap.

6. Click Save.

   The SNMP Traps page opens. Your changes to the trap settings appear in the table.

What are Users and Roles?

Before you configure Multi-Port Monitor as a monitoring device for CA Application Delivery Analysis, two default user accounts can be used: admin and user.

After you configure Multi-Port Monitor as a monitoring device, Multi-Port Monitor obtains information about users and roles from CA Application Delivery Analysis. The CA Application Delivery Analysis administrator creates and manages secure user accounts that are valid for CA Application Delivery Analysis and Multi-Port Monitor. These accounts allow operators to access the System Status page, Analysis page, System Setup page, or Administration page. In addition, these accounts are synchronized and displayed on the User Accounts page in the web interface.

Important: Multi-Port Monitor does not obtain information about users and roles from CA TIM or CA APM. Only the default user accounts are applicable when CA TIM is installed on the appliance *and* the appliance is not a monitoring device for CA Application Delivery Analysis.

Multi-Port Monitor security is fully compatible with CA Application Delivery Analysis and is based on login access privileges.

- Users with the CA Application Delivery Analysis User privilege, and at least one role right, can view the data on the System Status tab. A user with User product privilege but no role rights will be denied access to the System Status page.
- Users with the CA Application Delivery Analysis Administrator privilege can access the Multi-Port Monitor Administration tab.

The rights that are associated with user account roles further determine access.

- Users with the CA Application Delivery Analysis Engineering role can view the Analysis page.
- Users with the CA Application Delivery Analysis Investigations role can view the Analysis page and can use the Export to PCAP feature.

The CA Application Delivery Analysis administrator can create more user accounts to track Multi-Port Monitor status and configure data monitoring. For better security, change the default password of the administrator and user accounts.

More information:

Change the Password of the Administrator Account (see page 12)

User Account Information

Multi-Port Monitor provides default user accounts with different product permissions and different roles. The product permissions of the default accounts allow for two different levels of access to the web interface.

User permission level

View-only access to the System Status and Analysis pages.

Administrator permission level

Access to all product features.

The role that is assigned to each user account determines the web pages and product features that the user can access.

When Multi-Port Monitor is a monitoring device for CA Application Delivery Analysis, the administrator can create and modify accounts in the management console or in CA Performance Center. These accounts are synchronized and displayed on the Multi-Port Monitor web interface. You can view details about user accounts at Administration, Users.

Name

The user name and login ID for this account. Identifies the user account. Identifies the product permission level for the default accounts.

Role

Determines the level of access to product features for the user.

Privilege

The level of access to the product configuration, either Administrator or User. Only a user with the Administrator permissions can change the product configuration, such as setting capture filters or changing database retention settings.

Status

The status of the user account, either Enabled or Disabled.

Time Zone

The local time zone of the operator most likely to be using the user account.

Change the Properties of a User Account

User accounts establish the credentials of people who are authorized to operate Multi-Port Monitor and perform certain tasks. Information about the default user accounts (admin and user) can be viewed on the User Accounts page of the web interface.

Before you add Multi-Port Monitor as a monitoring device for CA Application Delivery Analysis, you can use the web interface to modify the default user accounts. For example, you can change an account password, update the associated time zone, or assign another role.

Note: The settings for these accounts are updated with the settings from CA Application Delivery Analysis after you add Multi-Port Monitor as a monitoring device and synchronize. After you add Multi-Port Monitor as a monitoring device, use the CA Application Delivery Analysis management console or CA Performance Center to create and change user accounts.

Follow these steps:

1. Click Administration, Users in the web interface.

   The User Accounts page displays the predefined user accounts and the custom accounts you created.

2. Click the Edit link for the account that you want to edit.

   The Edit User page opens.

3. Complete the following fields:
   - **Description**. Describe the account or a recent change. For example, you can state that the password has been changed. This optional step is a best practice.
   - **Password**, **Confirm Password**. Delete the encrypted text in each field and enter a new password in each field.
   - **Product Privilege**. Select a permission level that determines whether the user can perform administrative tasks.
   - **Role**. Select a role to determine the permissions that the user has for viewing report data and access product features.
   - **Time Zone**. Select the local time zone of the operator most likely to use this user account.
   - **Enabled**. Select this check box to prevent accidental disabling of the account under which you are logged in to the web interface. To disable the admin account, create another user with the Administrator product permission and log in as that user. You can then disable the admin account.
4. Click Save.

Role Information

Roles control access to product menus and data sources. Assign roles to restrict user access to product functionality. For example, limit user access to the System Status page of the Multi-Port Monitor. When a role restricts the user's access, the user cannot view the restricted parts of the product.

The role that is associated with a user account determines the following restrictions:

- The menus and report pages a user can access.
- The ability of the user to customize data and to drill down for more information.

In CA Application Delivery Analysis, each role has an Area Access parameter that determines page-level access to CA Application Delivery Analysis reports and other features, such as on-demand investigations. The same roles also operate within CA Performance Center after the CA Application Delivery Analysis data source is registered.

The privileges that the role controls do not extend to administration. Administrative permissions are assigned to the user when the user account is created.

The Multi-Port Monitor Roles page is a read-only list of predefined role names and descriptions.

IT Manager

This Administrator role for Multi-Port Monitor and CA Application Delivery Analysis provides access to the following CA Application Delivery Analysis reports:

- Investigations
- Engineering
- Operations
- Incidents
- Management

IT Engineer

This role:

- Consists of user permissions that are geared toward the troubleshooting of reported issues and provides access to the following CA Application Delivery Analysis reports:
  - Investigations
  - Engineering
  - Operations
  - Incidents
  - Management
- Gives Drill into Data Sources role right. This role right enables the user to drill into a data source, including the CA Application Delivery Analysis management console, from Performance Center, and from the CA Application Delivery Analysis management console to the Multi-Port Monitor.

  Important! The Multi-Port Monitor does not enforce permission sets from CA Performance Center. For example, if a particular group of servers is assigned to a user, the Multi-Port Monitor displays performance data for all servers in the domain.

IT Operator

This role:

- Consists of user permissions that are geared toward the troubleshooting of reported issues and provides access to the following CA Application Delivery Analysis reports:
  - Engineering
  - Operations
  - Incidents
  - Management
- Does not give Drill into Data Sources role right, however, this role does not prevent a user from logging into the CA Application Delivery Analysis management console and from the management console, drilling into the Multi-Port Monitor.

  Important! The Multi-Port Monitor does not enforce permission sets from CA Performance Center. For example, if a particular group of servers is assigned to a user, the Multi-Port Monitor displays performance data for all servers in the domain.

Product Privilege

Product privilege is an aspect of a user account that grants or restricts access to administrative features.

Each level of product privilege corresponds to a predefined role. The CA Application Delivery Analysis administrator can assign different roles and privileges to user accounts and can customize roles to grant access to different product areas.

The Power User product privilege does not exist in Multi-Port Monitor. However, a Power User with access to the CA Application Delivery Analysis Engineering product area can access all Multi-Port Monitor features except features on the Administration page.

CA Performance Center supports the product privileges used in CA Application Delivery Analysis and Multi-Port Monitor, but the privileges operate on a different level. Product privileges can let one user account have different levels of access to different CA data source products. For example, a person can be a user of CA Application Delivery Analysis, with the ability to view selected items in CA Performance Center. This same person can also be an administrator for a specific instance of CA Application Delivery Analysis when navigated to from a CA Performance Center view.

All Multi-Port Monitor operators have access to the System Status page. However, the User privilege requires at least one role right to be given in order to access the System Status page.

The Administrator product permission is required for an operator to access the Administration page. However, the role for the user account determines access to the Analysis area. And the ability to export an analysis to PCAP format is further restricted to a second area access parameter.

Access to the Analysis page in Multi-Port Monitor is associated with access to the CA Application Delivery Analysis Engineering tab. The Area Access parameter of the user account role determines this access. But even this access is not sufficient to allow the user to export PCAP files, which requires access to the Investigations area.

In CA Performance Center, the product permission setting overlaps with the role settings at the data source level. A user must have access rights and at least User product permissions for a data source to perform the following tasks:

- View reports.
- Drill into views.
- Navigate to that data source from CA Performance Center.

Permissions and role-determined access rights that apply in CA Performance Center are preserved within the Multi-Port Monitor web interface.

The following list summarizes the types of product privileges available in CA Application Delivery Analysis and Multi-Port Monitor and explains their default areas of access:

Administrator level

This level is typically associated with the role of IT Manager and provides access to the following features:

- Analysis page
- System Status page
- Administration page
- Export Analysis to PCAP feature

Power User or Investigator level

No predefined Power User account is available in Multi-Port Monitor. This level is the default for the role of Network Engineer and provides access to the following features:

- Analysis page
- System Status page
- Export Analysis to PCAP feature

User level

This level is the default for the role of IT Operator and provides access to the following features:

- Analysis page
- System Status page

The default IT Operator role does not allow the associated user to export data to the PCAP format, which can contain sensitive data. To grant the necessary area access to a user with this role, the CA Application Delivery Analysis administrator can add the Investigations area to the IT Operator role.

Chapter 4: System Health and Maintenance

Multi-Port Monitor monitors itself to keep the system performing at peak levels. In addition, the administrator can perform the following tasks:

- View system status.
- Customize system maintenance options.
- Stop or restart processes.
- Apply software upgrades to the appliance.
- View system logs for troubleshooting purposes.

This section contains the following topics:

System Status

The System Status page displays the status of all active Multi-Port Monitor processes, including the following metrics:

- Capture card and disk performance
- File system status
- Memory and CPU usage

Both users and administrators have access to the System Status page.

System Information

The System Information section provides details about the Multi-Port Monitor appliance.

Hostname (IP Address)

The DNS host name and IPv4 address of the appliance.

CA Application Delivery Analysis Manager

The IPv4 address of the CA Application Delivery Analysis management console and a link to the CA Application Delivery Analysis login page.

This information is available only if the appliance is configured as a monitoring device for CA Application Delivery Analysis.

Multi-Port Monitor Version

The version and build numbers of the software.

Process Information

Multi-Port Monitor consists of multiple processes, or daemons, that capture packets, calculate metrics, inspect packets, and perform automatic system maintenance. The Process Information section provides frequently updated status information for the following processes:

nqcapd

The packet-capture daemon. Its log file name is nqnapacapd.log.

Tip: To reset port statistics, restart the nqcapd process.

nqmetricd

The metric-computation engine is roughly equivalent to the Metric Compute Module on the CA Application Delivery Analysis single-port monitor. Its log file name is nqMetricReader.log.

nqinspectoragentd

The inspector daemon is roughly equivalent to the SA Monitor service on a single-port monitor. Its log file name is nqInspectorAgentd.log.

nqwatchdog

The watchdog process monitors the status of other processes and restarts them if necessary. Its log file name is nqwatchdog.log.

nqmaintd

The system-maintenance daemon. Its log file name is nqmaintd.log.

sadatatransfermanager

The Data Transfer Manager process receives and transfers data from a Cisco Wide-Area Application Services deployment. This process has a status of Stopped when Multi-Port Monitor is not configured as a CA Application Delivery Analysis monitoring device. After you configure the monitoring device, this process is always running, even if it is not used. The log file name is saDataTransferManager.log.

Tip: You can also see the status of these processes on the Process Status page at Administration, Processes.

More information:

Stop or Restart a Process (see page 47)

Database Status

The Database Status section identifies the status of the high-performance database on the Multi-Port Monitor appliance. This section shows the name of the local database and one of the following status levels:

- UP
- DOWN
- SHUTTING DOWN
- INITIALIZING

A time stamp indicates when the status was updated.

More information:

Database Status and Usage (see page 49)

Capture Card Physical Port Status

The Capture Card Physical Port Status section provides information about the traffic flowing through each port and describes each link. Most values are dynamically updated and the browser is refreshed every 5 seconds.

Physical Port

The physical port on the Multi-Port Monitor appliance.

Type

The type of cable that is used for the connection.

Link State

Whether the link to this port is connected or not connected.

Link Quality

The quality of this connection, which is based on information from the network adapter. Indicates whether the link is down.

Link Speed

The normal speed of this link.

More information:

Capture Card Clock Differs from System Clock (see page 58)

Capture Card Logical Port Status

The Capture Card Logical Port Status section provides the status of each logical port and the number of processed and dropped packets. You can assign multiple physical ports, or data feeds, to one logical port definition for reasons such as:

- Organizing your reporting around primary and failover circuits.
- Monitoring more accurately in asymmetrical routing environments.

Logical Port

The logical port, as defined on the Logical Ports page. Each physical port on the capture card is associated with a logical port definition. This association helps you identify data feeds and lets you aggregate sources of data so that they are monitored together. Logical port definitions include a port number, a name, and hardware filter settings that let you determine the traffic that is captured.

Logical Name

The logical port name. If you do not assign a name to the port, default values are used: Port 0, Port 1, and so on.

State

The status of the link to this port: Enabled or Disabled.

Status

The current port status: Running, Stopped, or Error. If the status is Error, position the mouse pointer over the error icon to display the reason for the error.

Packets Processed

Indicates the total number of packets that are delivered by the capture card after the hardware filters have been applied. This statistic is reset when the nqcapd process is started or restarted.

Drops

The number of packets incoming from this logical port that the capture card dropped and did not process. The number of drops provides an indication of capture card load. Under normal performance conditions, the number of drops is zero.

More information:

Configure Logical Ports (see page 14)

Capture Card Physical Port Statistics

The Capture Card Physical Port Statistics section provides information about the amount of data flowing through each physical port on the Multi-Port Monitor appliance. The statistics are calculated before any hardware filters are applied, therefore, the statistics indicate the actual line rate coming in from the switch.

This section also identifies the number of current errors. This information lets you verify mirror port configuration to ensure that the mirrored session is not overloaded.

These statistics are reset to zero when the nqcapd process is started or restarted.

Physical Port

The physical port through which data flows to Multi-Port Monitor. Either All (a total from all channels) or the identifier of a physical port. The number of physical ports depends on the type of capture card in use.

Logical Name

The name of the logical port that is associated with this physical port.

Packets Received

The number of discrete packets that were received after statistics were reset.

Bytes Received

The number of bytes that were received after statistics were reset.

CRC/Align Errors

The number of frames with cyclical redundancy check (CRC) errors or alignment errors.

Discarded Duplicates

The number of packets that the capture card discarded, according to its deduplication logic, because they were duplicates of packets already received. You can enable or disable automatic deduplication on the Application Settings page.

This value is an indication of whether the mirror port is appropriately configured. If a large percentage of captured traffic consists of duplicate packets, verify the port mirroring configuration.

Receive Rate

The number of packets that were received per second through this channel.

More information:

Set Global Preferences (see page 24)
Stop or Restart a Process (see page 47)

RAID Status Information

The RAID section provides information about disk performance from the RAID arrays on the Multi-Port Monitor appliance.

Note: RAID information is available only if the Adaptec Storage Manager (arcconf) utility is installed. For more information, see the *CA ADA Multi-Port Monitor Installation Guide*.

Array

The identifier of the RAID array. Indicates whether the information applies to the System array or the Data array.

Status

The status of the array:

- Optimal: Performing at the highest level
- Degraded: Not performing at the highest level
- Failed: Not running; showing an error condition. The error type and the ID and serial number of the affected drive are indicated.
- Rebuilding: Coming back online. After the RAID controller detects a drive that is rebuilding, the status changes to Optimal. Meanwhile, the array is still running in Degraded state. All metrics are still collected.

Note: Metric processing is not interrupted when the data array shows a Failed status for a drive, but packet capture investigations cannot be performed. You can change out a failed drive without interrupting metric processing.

Type

The type of RAID array.

- CA6000 Multi-Port Monitor RAID arrays are configured as RAID 5.
- CA6300 RAID arrays:
  - System Array: RAID 1
  - Data Array: RAID 6

Number of Drives

The number of disk drives that the array controls.

Failed Drives

An indication of failed drives, drives that indicate an error, or drives that are rebuilding. Includes drive numbers, ID numbers, and serial numbers. The System Array drives have ID numbers of 1 through 4. Data Array drives have ID numbers of 5 through 16.

File Systems

The File Systems section provides usage statistics for the file systems on the Multi-Port Monitor appliance.

File System

The name of the file system whose statistics are shown.

Size

The total capacity, as a number of bytes, of this file system.

Used

The number of bytes in this file system that are in use.

Avail

The number of bytes in this file system that are free and available for use.

Use%

The percentage of file system capacity that is in use.

Mounted

The mount point of the file system in the operating system directory.

Memory

The Memory section provides information about memory size, used and free bytes, and buffering statistics.

Linux may show high memory utilization when there is still ample memory available for processes to use. The reason is that the operating system uses available memory for disk caching (Cached) but will relinquish this memory to processes when needed. This is standard behavior of the Linux operating system and is done to improve performance.

When interpreting the Memory information, consider the following:

- If the Memory Free column is low but the Cached number is high and Swap Used is low or zero, then the Multi-Port Monitor is operating normally.
- If the Memory Free column is low and Cached is low and Swap Used is high (indicating that the Multi-Port Monitor is swapping), then this could indicate that some processes are using a significant amount of memory and may be impacting performance.

The Multi-Port Monitor appliance runs on 64-bit CentOS Linux. The memory information is obtained using the Linux 'free –o' command. The following columns are displayed:

Total

Indicates the total number of bytes of physical memory or swap space.

Used

Indicates the number of bytes of physical memory or swap space that are in use. Note that for physical memory, this number includes the number of bytes cached.

Free

Indicates the number of bytes of physical memory or swap space that are free.

Buffers

Indicates the number of bytes of physical memory used by kernel buffers.

Cached

Indicates the number of bytes of physical memory used by kernel for disk caching.

See the following articles for more information about Linux memory management:

- http://www.linuxhowtos.org/System/Linux%20Memory%20Management.htm
- http://www.itworld.com/it-managementstrategy/280695/making-sense-memory-usage-linux
- http://www.linuxintheshell.org/2012/06/05/episode-008-free-understanding-linux-memory-usage/

CPU

The CPU section provides information about CPU usage and performance statistics, which illustrate Multi-Port Monitor performance and load.

CPU

Identifies the CPU on the appliance to which the statistics correspond. One of the following values:

- All: Statistics that are averaged for all processors.
- 0 through 15: The CPU identifier, 0 through 15. The Multi-Port Monitor platform has a dual quad core CPU with hyper-threading that appears as 16 CPUs.

User

The percentage of CPU time of processes executing at the user level.

Nice

The percentage of CPU time of processes executing at the user level with nice priority. The kernel determines priority.

System

The percentage of CPU usage attributable to the kernel itself.

IO Wait

The percentage of time that the CPU was idle, but the system had an outstanding disk I/O request.

IRQ

The percentage of CPU time spent processing interrupt requests.

Soft

The percentage of CPU time spent in soft interrupt state.

Steal

The percentage of CPU time that a virtual CPU is waiting for a real CPU while the hypervisor services another virtual processor.

Idle

The percentage of time that the CPU was idle, and the system did not have an outstanding disk I/O request.

Interrupts/Sec

The total number of interrupts that the CPU received per second.

Maintenance Tasks

Some system maintenance is performed automatically. Other tasks are performed manually, such as restarting a daemon or process.

The need to log in to the Multi-Port Monitor appliance is minimal, even for maintenance of the database. You can use the web interface to perform the following tasks:

- Upgrade software.
- Stop and start processes.
- Open system logs and save them to a file.
- Generate support files.
- Purge data from the database.

Upgrade Software

Administrators can upgrade the Multi-Port Monitor software, the operating system, and the CA TIM software when new releases or patches are available. Product upgrade files are delivered from CA Technical Support.

You upgrade Multi-Port Monitor software, including the prerequisites file, Multi-Port Monitor software, and operating system from the Administration, Upgrade page in the web interface. Use the System Setup, Install Software page to upgrade the CA TIM software.

Upgrading the Multi-Port Monitor software and the operating system

The *CA ADA Multi-Port Monitor Upgrade Guide* contains complete instructions for upgrading Multi-Port Monitor and for upgrading the CentOS operating system (when applicable).

Upgrading the CA TIM software

The procedure for upgrading CA TIM is the same as the procedure for installing CA TIM. For more information, see Install the TIM Software.

In general, the upgrade process is as follows:

1. Browse to the location where you saved the upgrade files.
2. Select it and click Open.
3. Click Upgrade to start the process.

   Messages indicate the progress of the patch or upgrade. Do not navigate away from the page until the message indicating completion appears.

Stop or Restart a Process

Stop or restart the Multi-Port Monitor processes when certain error conditions occur, or when you change a systemwide setting.

Note: You can restart the nqmaintd process through the web interface. However, you cannot stop or start the process through the web interface. If the nqmaintd process is stopped, log in to the appliance directly to start it.

Follow these steps:

1. Click Administration, Processes in the web interface.

   The Process Status page opens. The Process column lists the names of the processes.

2. Click a link to start, stop, or restart a process in the Start/Stop column.

Tip: To reset port statistics, restart the nqcapd process.

More information:

Process Information (see page 38)

Review System Logs

You can view the last 200 lines of logged activity in a log file for a Multi-Port Monitor process. In addition to logs for the Multi-Port Monitor processes, you can view the recent entries in the following logs:

SAService.log

Contains entries for communications from CA Application Delivery Analysis to Multi-Port Monitor, including heartbeats and feed status updates.

Also contains requests for the network health information that appears on the Defect Details page in the APM console.

SAInvestigations.log

Contains entries that record packet capture investigation requests from CA Application Delivery Analysis.

nqsnmptrap.log

Contains entries for every condition that triggered an SNMP trap.

Follow these steps:

1. Click Administration, System Logs in the web interface.

   The System Logs page opens.

2. Select a log file from the Log File field.

   The System Logs page refreshes to show the size of the log you selected. For example:

   ```
   The file nqInspectorAgentd_20110228.log is 300160 bytes in size.
   ```

3. Click View.

   The System Logs page refreshes to show up to the last 200 lines of the log you selected.

More information:

Process Information (see page 38)

Generate a Support File

You can generate a Support file that contains troubleshooting information that is useful for CA Technical Support personnel. The Support file compiles all recent logs from all processes and saves the data in compressed tar format (.tgz).

Follow these steps:

1. Click Administration, System Logs in the web interface.

   The System Logs page opens.

2. (*Optional*) Select 'Include metrics database diagnostics' to include information from a diagnostics utility on the Multi-Port Monitor metrics database.

   Note: Generating the Support file can take longer when you select this option. Select this option only when CA Technical Support personnel instruct you to do so.

3. Click Generate.

   The System Logs page displays the name of the new Support log file.

4. Select the log file from the 'Select the support file for download' field.

5. Click Download.

   The File Download dialog opens.

6. Click Save and navigate to the location in which you want to save the file.

Database Status and Usage

The statistics on the Database Status page describe database status and usage. Use this information as a guide when selecting purge (File Retention) settings on the Application Settings page. The information in the Database Usage section is especially useful for determining when to purge older database entries containing metrics from 1-minute intervals.

The Database Status page provides the following information:

Database

The name of the local databases on the Multi-Port Monitor appliance.

Status

Status of a database: UP, DOWN, SHUTTING DOWN, or INITIALIZING.

Start/Stop

Links that let you start or stop a database. Stop a database before you shut down or restart the appliance.

Date of oldest data

The oldest time stamp of the data in a database.

Date of newest data

The most recent time stamp of the data in a database.

Rows in database

The total number of rows in the database that are in use. The maximum number of rows is 12 billion. If the maximum threshold is exceeded, the nightly maintenance routine prunes it to less than 12 billion.

Rows for past day

The number of database rows in use during the past 24 hours.

Rows for past 7 days

The number of database rows in use during the past week.

Tips:

- The Database Usage section provides a range of dates to show when the oldest and most recent data was inserted, and several database row counts. This information helps you gauge how quickly data is accumulating. Based on this information, you can adjust the number of days that information is kept in the database.
- To reduce the number of rows added to the database, adjust the filters that are applied to each logical port. For example, instead of using the default filter that captures all protocol traffic, you can capture only TCP packets.

- The status of the database is automatically updated every 60 seconds. The row counts are updated only when you navigate to the Database Status page or when you refresh the browser.
- Users who do not have the Administrator product permission can review the database status on the System Status page. All Multi-Port Monitor users can access the System Status page.

More information:

Set Global Preferences (see page 24)
Command Line Syntax (see page 65)
System Status (see page 37)
Using Hardware Filters to Manage Data (see page 16)

Purge Data from the Database

During normal operation, Multi-Port Monitor performs routine maintenance on the database and file systems. Routine maintenance includes purging data and files of various types. Typically, raw packet capture files are retained for six hours before being purged. Files containing performance metrics from 1-minute intervals are retained for one week before being purged.

You can manually purge the Multi-Port Monitor database for several reasons:

- The Database Status page reveals a problem.
- Statistics on the System Status page indicate that file systems are nearly full.
- You receive an mpcDiskUsage SNMP trap indicating that disk usage exceeds a threshold.

Important: Purged data is permanently removed from the database. You cannot recover purged data.

Follow these steps:

1. Click Administration, Purge Data in the web interface.

   The Purge Data page opens.

2. Select "Purge all data and metric database tables" to remove all data and database tables.

   This option stops the processes that collect data. No new data is collected until you restart the processes.

   When you select this option, all other options on the page are unavailable.

3. Select at least one of the following options to remove only selected data. Processes continue to run and new data is still collected.
   - **Purge one-minute session metrics**. Removes the 1-minute session metrics from the metrics database.
   - **Purge raw capture files**. Removes packet capture files. These files are continually generated during ordinary monitoring and are used to derive performance statistics. The default is 6.
   - **Purge packet capture investigations**. Removes files from packet capture investigations. Investigation files are stored separately from raw capture files. The default is 90.
   - **Purge log files**. Removes the log files that Multi-Port Monitor creates.
4. Select the time frame for removing the data that you selected in step 3.
   - **Purge across all dates**. Removes data of the selected type, regardless of the time frame.
   - **Purge prior to this date**. Removes the data that was collected before the date you specify.

     Note: Data is stored in Coordinated Universal Time (UTC). This option removes data that was collected before midnight UTC. When you view data using the local time, it may seem as though some data still exists for the previous day.
5. Click OK.
6. Restart the processes that were stopped if you purged all data as described in step 2.

More information:

Set Global Preferences (see page 24)
Database Status (see page 39)
System Status (see page 37)
Create SNMP Traps (see page 25)

Log In to the Appliance

Typically, it is not necessary to log in to the Multi-Port Monitor appliance after you install the hardware and software. Most administrative tasks can be performed from the web interface. However, you access the appliance directly for the following tasks:

Start the maintenance daemon (nqmaintd) if it is stopped

The daemon is required to start or restart other processes. The daemon cannot be started or stopped from the web interface.

Shut down or restart the appliance

A shutdown or reboot is not required, even for an upgrade. However, to take the computer offline, use the login procedure and commands to shut it down correctly.

Shutting down the appliance during a load or merge operation can corrupt the local database. Stop the database before you shut down the appliance.

Use the attached keyboard and monitor to log in to the appliance directly. You can also log in from a remote system using a secure shell (SSH) client such as PuTTY, which runs on Microsoft Windows.

Follow these steps:

1. Press Alt+F2 on the initial screen.

   The Linux login screen opens.

2. Log in with the following credentials:

   - User name: netqos
   - Password: The password that you created when you installed the Multi-Port Monitor software.

   The Linux command-line interface opens.

3. Run the necessary command.

More information:

Database Status (see page 39)
Command Line Syntax (see page 65)

System Setup

The System Setup page identifies components that are installed on the Multi-Port Monitor appliance. Often, the name of the component is a hyperlink to more information.

Machine Settings

The build number and a link to the Machine Settings page. Use the Machine Settings page to review your network setup, set the time zone, and shut down or restart the appliance.

Multi-Port Monitor

The build number and a link to the Administration page. Use the Administration page to configure data monitoring, system settings, and authentication, and perform maintenance.

Multi-Port Monitor Prerequisites

The build number of the most recently downloaded prerequisites package.

System Health

The build number and a link to the Appliance Health page on the Customer Experience Manager (CEM) console. Use the Appliance Health page to review information about disk and memory usage, logged-in users, and running processes. This item is available only when CA TIM is installed on the appliance.

Third-party

The version and build numbers of the CA TIM third-party applications that are installed on the appliance. This item is available only when CA TIM is installed on the appliance.

TIM

The build number and a link to the TIM Setup page on the CEM console. Use the TIM Setup page to stop and start CA TIM, to view status and statistics, and to configure Watchdog settings. This item is available only when CA TIM is installed on the appliance.

More information:

Machine Settings (see page 54)

Machine Settings

The Machine Settings page provides links to the following pages:

- Network Setup (see page 54)
- Set Time Zone (see page 55)
- System Shutdown/Restart (see page 56)

Network Setup

The Network Setup page identifies the network configuration that was created when you installed the Multi-Port Monitor software and you enabled network access. For more information, see the *CA ADA Multi-Port Monitor Installation Guide* that was shipped with your appliance.

You can use the fields on this page to change the network configuration.

Select which interface to configure

The selection in this field determines the contents of the other fields on this page. Select an interface and click Set before changing the information in the remaining fields. The page refreshes and indicates whether the interface has IPv4 addresses.

Automatically obtain IP address settings with DHCP

Select this option to use DHCP (Dynamic Host Configuration Protocol) to obtain the IP address of the management NIC. You can provide the DHCP host name of the management NIC.

Manual IP Address Settings

Select this option to type the IP Address, Subnet Mask, and Default Gateway Address of the management NIC.

Note: The IP address of the management NIC must match the IP address that is assigned to Multi-Port Monitor in the CA Application Delivery Analysis management console.

Manual DNS Settings

Type the IP address of the local DNS server in the "DNS server 1" field.

(*Optional*) Type the IP addresses of secondary DNS servers in the "DNS server 2" and "DNS server 3" fields.

Submit

Click to preserve your changes to network settings.

Choose the Time Zone

You can change the time zone of the Multi-Port Monitor appliance.

Follow these steps:

1. Click System Setup, Machine Settings in the web interface.

   The Machine Settings page opens.

2. Click Set Time Zone.

   The Set Time Zone page opens.

3. Select the time zone of the appliance.

4. Click Set Time Zone at the confirmation prompt.

   A confirmation message appears.

Shut Down or Restart the Appliance

Applies to CA6000 and CA6300 appliances

Always shut down the Vertica metrics database before shutting down or restarting the appliance. When shutting down or restarting the appliance from:

The Multi-Port Monitor web interface

1. Shut down the Vertica metrics database:
   a. Click Administration to open the Administration page.
   b. Click Database Status to open the Database Status page.
   c. Click Stop to stop the Metrics database.
2. Shut down or restart the appliance:
   a. Click System Setup to open the System Setup page.
   b. Click Machine Settings to open the Machine Settings page.
   c. Click System Shutdown/Restart.
   d. Click an option:
      - **Shut down the computer**. Select this option to turn off the appliance. You must have physical access to the appliance to turn it back on.
      - **Restart the computer**. Select this option to turn off the appliance and then restart it. The Vertica metrics database start automatically when you restart the appliance.

The command line

Run the following commands:

1. Stop the Vertica metrics database.
   `sudo /opt/NetQoS/scripts/doVerticaCmd.sh --shutdown`
2. Shut down or restart the appliance.

   To shut down the appliance:
   `sudo /sbin/shutdown -h now`

   To restart the appliance:
   `sudo /sbin/shutdown –r now`

More information:

Log In to the Appliance (see page 52)

Chapter 5: Troubleshooting

This section contains the following topics:

IPv6 Traffic Not Captured Correctly

Symptom:

The following errors occur when I attempt to capture IPv6 traffic:

- Traffic that is sliced to "Headers Only" includes the IPv6 header but no TCP header.
- Filters based on Layer 4 header information (such as TCP port number) do not capture IPv6 traffic.

Solution:

You may need to update the FPGA (firmware) on the Napatech card. The following table identifies the FPGA versions necessary for capturing IPv6 traffic:

Napatech Card Model	FPGA Version
NT4E (4x1Gb)	200-9015-**42**-08
NTPORT4 (4x1Gb expansion card)	200-9019-**42**-05
NT20E (2x10Gb)	200-9014-**42**-07

The portion of the FPGA version number in bold text is the determining factor. FPGAs with a number lower than 42 do not fully support decoding of the IPv6 packet header.

Use one of the following methods to verify the version of the FPGA:

- Click About in the Multi-Port Monitor web interface. The About page identifies the version number of the active Napatech FPGA.
- Run the following command from the Linux command line.
  ```
  sudo  /opt/napatech/bin/AdapterInfo
  ```
  The output includes a line indicating the active FPGA image.

The Napatech FPGA is not updated when you upgrade the Multi-Port Monitor software. Contact CA Technical Support for instructions and the FPGA images.

Capture Card Clock Differs from System Clock

Symptom:

I see the following message on the System Status page, in the Capture Card Physical Port Status section:

"Capture card clock differs from system clock by *N* seconds."

Solution:

The capture card has an independent clock that stamps the time of incoming packets. In normal operation, this clock is synchronized with the Multi-Port Monitor system clock. The error message appears when there is a discrepancy between the Multi-Port Monitor system clock and the clock on the capture card. The discrepancy can occur when, for example, someone manually changes the time of the system clock.

Synchronize the clocks using the following methods:

- **Immediately synchronize the clocks**. Run the following command from the Linux command-line interface on the appliance. This command stops the nqcapd and nqmetricd processes, which disrupts monitoring. The processes are restarted after the clocks are synchronized.

  ```
  sudo /opt/NetQoS/scripts/syncNapatechClock --force
  ```

- **Maintain synchronization**. Run the Network Time Protocol (NTP) to maintain synchronization between the clocks. You can configure NTP with the Network Settings Utility on the appliance. To open the utility, run the following command from the Linux command-line interface:

  ```
  sudo /opt/NetQoS/tui/tui-setup.php
  ```

  In the utility, type the host name or IP address of your NTP server in the NTP Server field. The default is pool.ntp.org.

Time Range Exceeds Raw Packet Retention Time

Symptom:

I received the following warning message when attempting to export data to PCAP format:

```
Time range exceeds raw packet capture retention time.
```

Solution:

The Applications Settings (see page 24) page in the web interface includes a File Retention setting that affects the Export to PCAP feature. The error occurs when the data you want to export is from a time frame that is less than the "Keep raw packet capture files for" setting.

Use the System Status page to assess the disk usage for data in the File Systems section. If you have sufficient free space, increase the value of the "Keep raw packet capture files for" setting. Future PCAP exports will include data from farther in the past.

Appendix A: Best Practices for Deployment

This section contains the following topics:

Appliance Placement

The Multi-Port Monitor appliance requires connectivity to a SPAN or mirror port on each network switch that handles the traffic you want to monitor. Connectivity typically occurs at the access layer.

The appliance must be able to *see* as much of the relevant network traffic as possible. Consider the following questions:

- Which applications do you want to monitor?
- Which servers host these applications?
- To which switches are these servers connected?
- From which subnets do users access the monitored applications?

If your network or traffic volume is exceptionally large, you can purchase an additional appliance to balance the processing load.

Port Mirroring

On a network switch, the *port mirroring* function sends copies of network packets from one port to another switch or port for analysis. Port mirroring is a safe, effective way to mirror traffic to CA Application Delivery Analysis monitoring devices. Some switches do not provide a diverse range of TCP packet-mirroring capabilities. Where traffic cannot be mirrored optimally, use alternatives such as fiber taps.

Note: The port mirroring function on Cisco switches is named Switched Port Analyzer (SPAN).

Mirror the switch ports, where traffic travels to and from the monitored servers, to the ports where Multi-Port Monitor is connected. When mirror ports are configured correctly, CA Application Delivery Analysis monitors the flow of application among clients and servers without the use of desktop or server agents.

For more information, see the *CA Best Practices for Data Acquisition Guide*.

Port Requirements

The Multi-Port Monitor appliance requires several ports to be open to support the following communication paths:

- Between CA Application Delivery Analysis and the appliance.
- Between Enterprise Manager and the appliance, when CA TIM is installed.
- To allow access to the web interface for Multi-Port Monitor administration.

Port	Direction	Description
80	Inbound from CA Application Delivery Analysis and Enterprise Manager	■ HTTP for web interface access ■ Enterprise Manager communications with CA TIM
80	Outbound to CA Application Delivery Analysis	Multi-Port Monitor web service requests for configuration data
161	Inbound	SNMP MIB queries
162	Outbound	SNMP traps
7878	Inbound	TCP flows containing packet digests from WAE devices. **Note**: Needed only if a WAE device is a monitor feed.

Port	Direction	Description
8080	Inbound from CA Application Delivery Analysis and Enterprise Manager	■ CA Application Delivery Analysis web service requests for data ■ Enterprise Manager requests for the network health data that appears on the Defect Details page in the CA APM console.
9995	Inbound	UDP flows containing packet digests from the CA GigaStor Connector. **Note**: Needed only if NI GigaStor is a monitor feed.

Packet Deduplication

The term *packet duplication* refers to reporting on the same traffic multiple times as it passes through interfaces on a switch. Several port mirroring configurations can result in duplication because traffic from all ports is forwarded to Multi-Port Monitor.

The presence of duplicate packets can skew the metrics that are collected. Packet loss statistics are affected because duplicate packets are viewed as retransmissions.

As a best practice, configure mirror ports to minimize or eliminate duplicate packets. Multi-Port Monitor provides a packet deduplication setting that applies to the capture card and is enabled by default. This setting discards packets that seem to be duplicates of packets that were already processed.

During initial port mirroring configuration, you can temporarily disable the global setting for packet deduplication. Disabling the setting lets you see duplicate packets, which can help you eliminate duplication from mirrored sessions.

Deduplication logic applies to all packets received on a given logical port. Therefore, a duplicate packet from the same VLAN is not discarded when it is received on a different logical port. If you combine two physical ports into one logical port definition, a duplicate is discarded in the following situations:

- If it arrives on one physical port soon after the original packet arrived on another physical port.
- If it arrives on a second switch.

Both packets are retained if the two physical ports are not combined into a logical port.

Appendix B: Command Line Syntax

The default user name and password for the Multi-Port Monitor appliance provide superuser access. You can perform the following operations at the Linux command-line interface using the “sudo” prefix that identifies a superuser command.

sudo /sbin/service nqmaintd status

Verifies the status of the maintenance daemon (nqmaintd).

sudo /sbin/service nqmaintd restart

Restarts the maintenance daemon. Use only if the status message indicates that the process is running.

sudo /sbin/service nqmaintd start

Starts the maintenance daemon. Use only if the status message indicates that the process is stopped.

sudo /opt/NetQoS/scripts/stopprocs.sh

Stops all daemons (processes).

sudo /opt/NetQoS/scripts/startprocs.sh

Starts all daemons (processes).

sudo /sbin/shutdown -h now

Stops the appliance immediately. Stop the Multi-Port Monitor database before you stop the appliance.

sudo reboot

Stops and restarts the appliance immediately. Stop the Multi-Port Monitor database before you stop the appliance.

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --shutdown

Stops the Vertica metrics database. You can also stop the database from the web interface.

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --start

Starts the Vertica metrics database.

sudo /opt/NetQoS/scripts/doVerticaCmd.sh --status

Verifies the status of the Vertica metrics database. You can also verify the status from the web interface.

sudo /opt/NetQoS/tui/tui-setup.php

Invokes the Network Settings Utility on the appliance.

sudo /opt/NetQoS/scripts/syncNapatechClock --force

Immediately synchronizes the clock on the Multi-Port Monitor capture card with the system clock. This command temporarily stops the nqcapd and nqmetricd processes, which disrupts monitoring. Both processes are restarted after the clocks are synchronized.

More information:

Log In to the Appliance (see page 52)
Database Status (see page 39)
Database Status and Usage (see page 49)
Capture Card Clock Differs from System Clock (see page 58)

Appendix C: Regular Expression Syntax

For advanced filters, the syntax that is written to the Conditions field automatically conforms to vendor specifications for capture card compatibility. Review the generated expressions, especially the placement of the parentheses that group the expressions, to verify that they are evaluated in the correct order. For example, the following grouping:

```
(A OR B) AND C
```

has a different result than this grouping:

```
A OR (B AND C)
```

You can edit the syntax in the Conditions field.

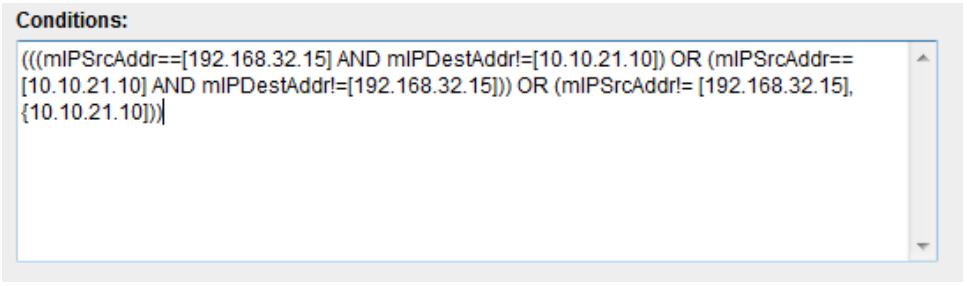
Multi-Port Monitor filtering includes packets that match the criteria. Take special care when creating filters that *exclude* packets from specific hosts or subnets. Discuss any questions about expression syntax with CA Technical Support.

Example

You want to ignore a conversation between Host A (192.168.32.15) and Host B (10.10.21.10). The conversation represents an automatic backup process that runs once per week and skews the baseline each time. You want to report on "all other traffic." You also want to retain all packets from traffic that travels to hosts other than the excluded pair. So you create a filter that retains the following packets:

- All packets where Host A is the source but where the destination does NOT EQUAL Host B, OR,
- All packets where Host B is the source but where the destination does NOT EQUAL Host A, OR,
- All packets with source addresses that do NOT EQUAL the IP address of Host A and Host B (all other traffic).

In the Conditions field, the proper syntax looks like the following example:



If written in English, the expression you create reads something like the following example:

```
(IP Source Address EQUALS 192.168.32.15 AND IP Destination Address does NOT EQUAL 10.10.21.10) OR (IP Source Address EQUALS 10.10.21.10 AND IP Destination Address does NOT EQUAL 192.168.32.15) OR (IP Source Address does NOT EQUAL 192.168.32.15, 10.10.21.10)
```

When creating an advanced filter with regular expressions, select "Equals" to insert "==." Select "Not Equals" to insert "!=."

More information:

Use Regular Expressions for Precise Filtering (see page 21)

Index

P

R

S

T

U

V

W