Integration with CA Transaction Impact Monitor

CA Application Delivery Analysis Multi-Port Monitor

Version 10.1

ca technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

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: Support for CA TIM

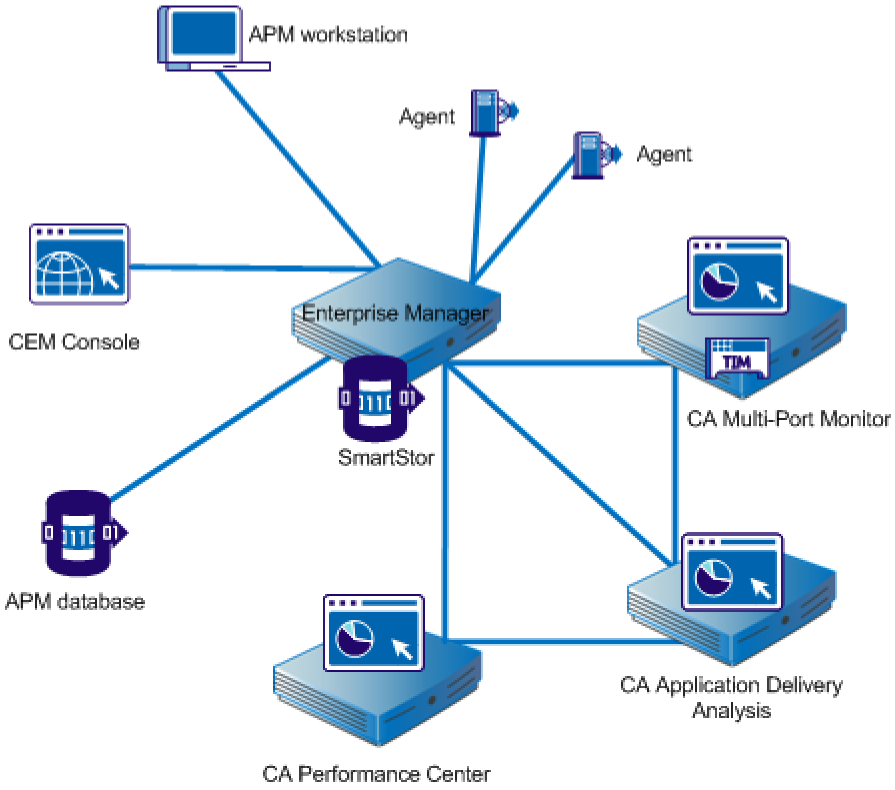
Multi-Port Monitor captures HTTP packets for CA Transaction Impact Manager (TIM).

- CA TIM passively monitors traffic from mirrored ports.
- CA TIM records HTTP and HTTPS packets to identify user logins and related transactions for the following products:
  - CA Customer Experience Manager (CA CEM)
  - CA Application Performance Management (CA APM)
- CA TIM performs Secure Sockets Layer (SSL) decoding.

When CA TIM is installed on the Multi-Port Monitor appliance, the resulting *converged appliance* provides visibility into the application and network-level data of application usage per user. As a standalone appliance, CA TIM monitors HTTP transactions in real time and generates defects when it detects anomalies. Multi-Port Monitor provides session-level data at 1-minute intervals. With the converged appliance, this finer granularity of data can be used to investigate the defects that CA TIM detects. Use the CA APM console to drill down from defects to related data in the Multi-Port Monitor web interface.

The web interface lets you perform administrative and maintenance tasks for CA TIM.

The following diagram shows the components in a network in which Multi-Port Monitor, CA APM, and CA Application Delivery Analysis are installed.



As shown in the diagram, Multi-Port Monitor can support CA TIM and CA Application Delivery Analysis simultaneously. In this scenario, packets for CA TIM and CA Application Delivery Analysis are processed in parallel. Separate RAM disks help buffer packets for both applications.

- For CA Application Delivery Analysis, Multi-Port Monitor provides all packets with headers only.
- For CA TIM, Multi-Port Monitor provides filtered HTTP packets with a full payload.

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.
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 CA GigaStor is a monitor feed.

Chapter 2: Install CA TIM on the Multi-Port Monitor Appliance

The Multi-Port Monitor appliance includes a CD with the CA Transaction Impact Manager (CA TIM) software. Or, you can download the CA TIM software from CA Technical Support.

Note: If you use Multi-Port Monitor only with CA Application Delivery Analysis, you do not need to install the CA TIM software.

You use the Multi-Port Monitor web interface to install the following files:

- Third-party image: third-party-update-xxxxxxxxxx.image
- TIM image: tim-complete-xxxxxxxxxxxxx.image

Follow these steps:

1. Download the setup files to a workstation that has web-browser access to the Multi-Port Monitor appliance.
2. Log in to the Multi-Port Monitor web interface as a user with Administrative privileges.

   The web interface opens.
3. Click System Setup, Install Software in the web interface.

   The Install Software page opens.
4. Click Browse and navigate to the location where you downloaded the setup files.
5. Select the third-party-update-xxxxxxxxxx.image file.
6. Click Open.

   The name of the file appears on the Install Software page.
7. Click Upload and Install.
8. Read and accept the License Agreement.

   The software installation log opens. If the log contains errors in red text, contact CA Technical Support.
9. Click Browse on the Install Software page and navigate to the location where you downloaded the setup files.
10. Select the tim-complete-xxxxxxxxxxxxx.image file, and then repeat Steps 6 through 8.

11. Click System Setup in the web interface.

    When installation is successful, the names of the files you installed appear on the System Setup page.

12. Identify the logical port to use for monitoring with CA TIM. For more information, see Configure Logical Ports (see page 13).

13. Enable the "HTTP - full packets" hardware filter to capture full packets:

    a. Click Administration, Logical Ports in the web interface.

    b. Click the Filters link for the logical port that is associated with CA TIM monitoring.

       The Logical Ports: Hardware Filters page opens.

    c. Click the Edit link for the "HTTP - full packets" filter.

       The Logical Ports: Edit Hardware Filter page opens.

    d. Select the Filter Enabled check box.

    e. Restart the nqcapd process.

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.

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.

   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 12) 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.

Configure a Hardware Filter

You can create, enable, disable, and modify predefined filters and the filters you create.

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 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**. 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), IPv6, 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.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.

- **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, or a valid IPv6 address and prefix bits. Do not combine IPv4 and IPv6 addresses in the list. 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.

  Use the following format for IPv6 addresses: x:x:x:x:x/*n* where x:x:x:x:x is the colon-separated IPv6 subnet address and *n* is the number of prefix bits. You can use standard abbreviated IPv6 addresses. For example, 2001:ba0:1a0::/48

  Tip: To filter for IPv4 *and* IPv6 subnets, create one hardware filter for the IPv4 subnets and another hardware filter for the IPv6 subnets.

- **IP Addresses**. The IPv4 or IPv6 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. Do not combine single addresses and ranges in the list. Do not combine IPv4 and IPv6 addresses in the same list or range of addresses. Select Exclude to discard traffic from the addresses you listed.

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

  Use colon-separated IPv6 addresses. You can use standard abbreviated IPv6 addresses. For example, 2001:f0d0:1002:51::4

  Tip: To filter for IPv4 *and* IPv6 addresses, create one hardware filter for the IPv4 addresses and another hardware filter for the IPv6 addresses.

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.

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

5. Restart (see page 12) the nqcapd process if you enabled a filter.

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 (see page 14).
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 12) the nqcapd process if you enabled a filter.

Chapter 3: Upgrade CA TIM on the Multi-Port Monitor Appliance

Administrators can upgrade the CA TIM software when new releases are available. Product upgrade files are delivered from CA Technical Support.

You use the Multi-Port Monitor web interface to install the following files:

- Third-party image: third-party-update-xxxxxxxxxx.image
- TIM image: tim-complete-xxxxxxxxxxxxx.image

Follow these steps:

1. Download the setup files to a workstation that has web-browser access to the Multi-Port Monitor appliance.
2. Log in to the Multi-Port Monitor web interface as a user with Administrative privileges.

   The web interface opens.
3. Click Administration, Upgrade page in the web interface.

   The Upgrade Software page opens.
4. Click Browse and navigate to the location where you downloaded the setup files.
5. Select the third-party-update-xxxxxxxxxx.image file.
6. Click Open.

   The name of the file appears on the Upgrade Software page.
7. Click Upload and Install.
8. Read and accept the License Agreement.

   The software installation log opens. If the log contains errors in red text, contact CA Technical Support.
9. Click Browse on the Upgrade Software page and navigate to the location where you downloaded the setup files.
10. Select the tim-complete-xxxxxxxxxxxxx.image file, and then repeat Steps 6 through 8.
11. Click System Setup in the web interface.

    When upgrade is successful, the names of the files you installed appear on the System Setup page.

Chapter 4: Troubleshooting

This section contains the following topics:

CA TIM is Not Configured to Use Napatech

Symptom:

I see the following message in the CA TIM error log:

```
Napatech software is installed but TIM is not configured to use Napatech.
```

Solution:

This message appears when CA TIM is installed on the Multi-Port Monitor appliance. Because Multi-Port Monitor is configured to manage the Napatech card, you can safely ignore this message.

CA TIM Stops Working

Symptom:

The TIM installed on the Multi-Port Monitor has stopped functioning properly. For example, it has stopped recording and generating statistics. Additionally, I see "skip old packets" messages in the TIM log.

Solution:

When Tim is installed on Multi-Port Monitor, the Napatech card on Multi-Port Monitor marks the packet arrival time using the time on that card. If the system time on the Multi-Port Monitor and the Napatech card time are different, then TIM can stop functioning properly.

Two possible use cases exist. Determine which use case applies to your situation.

1. TIM processing can sometimes lag behind the packet files from the Multi-Port Monitor. For example, if TIM is stopped and restarted or the Multi-Port Monitor is generating packet files faster than TIM can consume. Confirm TIM lag time by performing the following tasks:

    a. Confirm that the Napatech card time synchronizes with your system time on Multi-Port Monitor.

    b. Look at the Multi-Port Monitor System Status page and verifying that it does not display a warning message.

    If you have confirmed these two scenarios, then nothing is wrong with TIM. TIM does not process packet files that are older than 15 minutes (this default value can be changed). After it skips these old packet files, TIM resumes normal processing. TIM simply needs time to catch up with the Multi-Port Monitor generated files.

2. Compare the Napatech card time to that of your system time on Multi-Port Monitor. Use the following command from the terminal to see the Napatech card time:

    ```
    /opt/napatech/bin/TimeConfig  -cmd time_get
    ```

    Use the following command from the terminal to see the system time on Multi-Port Monitor:

    ```
    date
    ```

    If the two times are different and the Multi-Port Monitor System Status page displays a warning message, then look at the times on the Napatech card and Network Time Protocol (NTP) server.

    Select the time zone at the following website to get NTP time:

    http://www.time.gov/

    Consider the following scenarios and determine which one applies to your situation.

    Scenario 1

    <u>Conditions</u>

    - The Napatech card time is **vastly** different from the NTP time (more than 15 minutes).
    - The system time on Multi-Port Monitor is slightly different from the NTP time (less than 5 seconds).

Actions

- Synchronize the NapaTech time to the system clock by running the following command:

  ```
  /opt/NetQoS/scripts/syncNapatechClock
  ```

- If the Napatech time is different from the system time on Multi-Port Monitor by **less** than 5 minutes, then the Napatech driver OS synchronization gradually adjusts the Napatech clock. If the Napatech time is different from the system time on Multi-Port Monitor by **more** than 5 minutes, then the Napatech time synchronizes with the system time on the Multi-Port Monitor immediately.

Scenario 2

Conditions

- The Napatech card time is slightly different from the NTP time.
- The system time on Multi-Port Monitor and CEM console time is vastly different from the NTP time.

Actions

- Adjust the CEM console time to synchronize with the NTP time.
- Wait and verify that the system time on Multi-Port Monitor is set and is also synchronized with the NTP time.
- Confirm that the ntpd process on Multi-Port Monitor is running. If it is not running, start it.

  The ntpd process can stop automatically when the system time on the Multi-Port Monitor is different from the NTP time by more than 1000 seconds.

Scenario 3

Conditions

- The Napatech card time is **vastly** different from the NTP time.
- The system time on the Multi-Port Monitor and CEM console time are also **vastly** different from the NTP time.

Actions

- Adjust the CEM console time to synchronize with the NTP time.
- Wait and verify that the system time on Multi-Port Monitor is set and is also synchronized with the NTP time.
- Confirm that the ntpd process on Multi-Port Monitor is running. If it is not running, start it.
- Synchronize the Napatech time to the system clock by running the following command:

  ```
  /opt/NetQoS/scripts/syncNapatechClock
  ```

Index