Integration with CA Application Delivery Analysis

CA Application Delivery Analysis Multi-Port Monitor

Version 10.1

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 Application Delivery Analysis 7

Packet-Capture Investigations 8
Architecture for CA Application Delivery Analysis Support 9
Comparison with the CA Application Delivery Analysis Standard Monitor 10
Network Address Translation (NAT) 12
Overview of CA Application Delivery Analysis Data 13
Port Requirements 14

Chapter 2: Multi-Port Monitor as a Monitoring Device 17

Add the Monitoring Device 18
Verify Logical Port Status 20
Review TCP Session Information 20

Chapter 3: Incidents for Monitoring Devices 23

Enable Monitoring Device Incidents 24
Respond to an Inactive Monitoring Device Incident 25

Chapter 4: Support for Special Initialization (.ini) Files 27

Eliminate Duplicate Packets 28
Filter Out Keep-Alive Messages 29

Chapter 5: Monitoring in a WAN-Optimized Environment 31

CA Application Delivery Analysis Support for Cisco WAAS 31
How Multi-Port Monitor Integrates with a WAN Optimization Device 32
The CA Application Delivery Analysis Optimization Report 33
Sharing Data from WAN Optimization Devices 34

Index 35

Chapter 1: Support for CA Application Delivery Analysis

The Multi-Port Monitor appliance aggregates and exports IPv4-based TCP metrics to CA Application Delivery Analysis. The appliance collects more data, faster, than multiple Standard Monitors. The appliance is an alternative for enterprises that require high-volume monitoring with more flexibility and less overhead.

When monitoring IPv4-based traffic, the appliance stores packets to let you perform enhanced packet-capture investigations in CA Application Delivery Analysis. With a Standard Monitor, these investigations capture only the packets that are sent after the investigation is initiated. By contrast, the capture files that are stored on the appliance let you perform a forensic analysis of a performance issue.

When monitoring IPv4-based traffic with Multi-Port Monitor and the CA Application Delivery Analysis management console, you can perform the tasks below:

- Process a network throughput rate equivalent to multiple single-port monitors.
- View data at 1-minute granularity, and select from multiple chart types.
- Generate packet-capture investigation files at the time the incident occurred, and store those files for up to 90 days.
- Perform rapid, accurate detection of networks, servers, and applications.
- Track TCP sessions on multiple switches, and drill down into detailed metrics from a high-level CA Application Delivery Analysis summary report.
- Leverage multiple filtering and sorting capabilities to analyze the available data and rapidly isolate problem hosts.
- Create and save analyses, which are troubleshooting work flows that combine frequently used filtering and reporting options.
- Export packet-capture files in PCAP format and send them to IT Engineering staff for further analysis.

- Monitor a Cisco Wide-Area Application Services (WAAS) environment without installing a separate Aggregator appliance.
- Calculate response time metrics from the packet digest files that CA GigaStor provides.

This section contains the following topics:

Packet-Capture Investigations (see page 8)
Architecture for CA Application Delivery Analysis Support (see page 9)
Comparison with the CA Application Delivery Analysis Standard Monitor (see page 10)
Network Address Translation (NAT) (see page 12)
Overview of CA Application Delivery Analysis Data (see page 13)
Port Requirements (see page 14)

Packet-Capture Investigations

CA Application Delivery Analysis automatically runs packet-capture investigations in response to a network or server performance incident. These investigations increase the granularity of performance metric analysis by automatically recording packet-level data that can then be further analyzed.

When a packet capture investigation is performed with the CA Application Delivery Analysis Standard Monitor, the captured data does not always include the traffic of interest. A packet-capture investigation that Multi-Port Monitor performs is far more comprehensive. The short-term packet storage capabilities of the appliance let packet-capture investigations provide details of the traffic at the time the incident occurred.

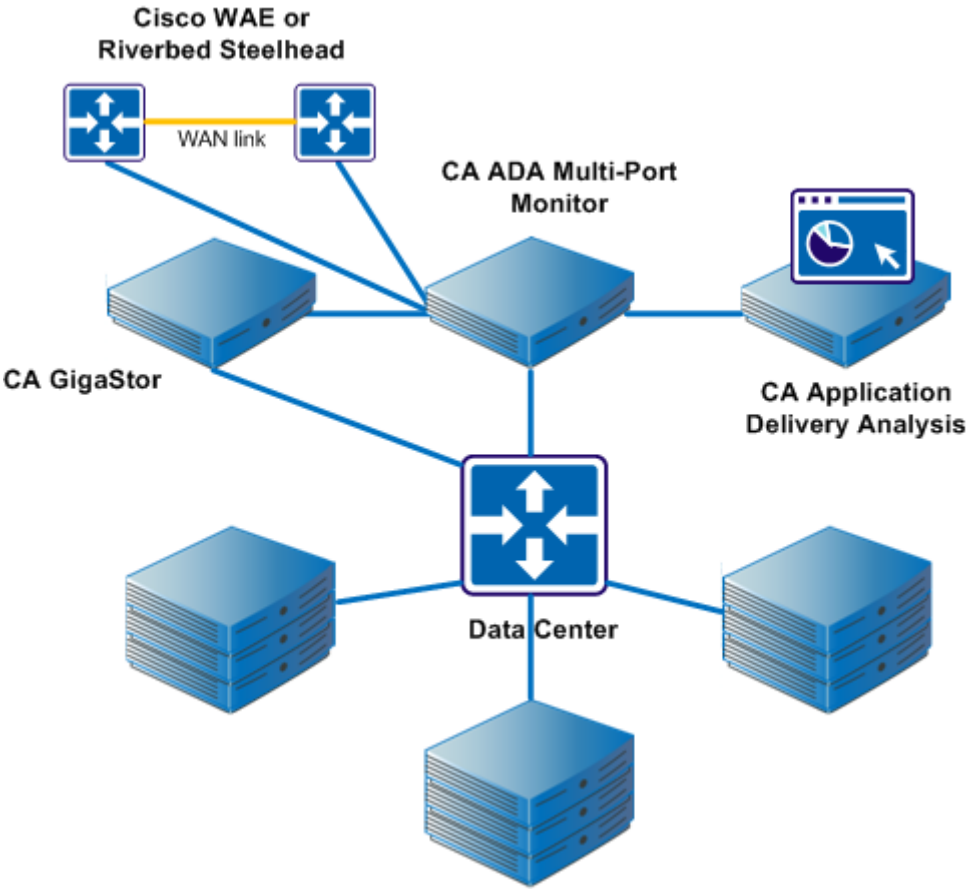
Options for capture and monitoring let you inspect the packet headers or the entire packet. By default, the appliance stores packet-capture investigation files for 90 days. To access them, log in to the CA Application Delivery Analysis management console and navigate to the Packet Capture Investigations report. Click the Incidents tab to see a link to the Investigations Report page.

When CA GigaStor is assigned to CA Application Delivery Analysis as a monitoring device, it sends the packet digests to CA Application Delivery Analysis for aggregation. CA Application Delivery Analysis packet-capture investigations are based only on the packets that are stored on CA GigaStor.

Architecture for CA Application Delivery Analysis Support

The following illustration depicts Multi-Port Monitor architecture and configuration to support CA Application Delivery Analysis. Multi-Port Monitor works within a typical CA Application Delivery Analysis distributed configuration, with network connectivity to the CA Application Delivery Analysis management console.

Depending on the configuration you purchased, one appliance can be connected to mirror ports on as many as eight separate switches. The appliance sends data from the monitored switches to the management console, where it is included in all CA Application Delivery Analysis reports.



Comparison with the CA Application Delivery Analysis Standard Monitor

The Multi-Port Monitor appliance and the CA Standard Monitor both aggregate and export IPv4-based TCP metrics to CA Application Delivery Analysis. The following table summarizes the most significant differences between the CA Application Delivery Analysis single-port monitor and Multi-Port Monitor when monitoring IPv4-based TCP traffic:

Feature	Standard Monitor	Multi-Port Monitor
Monitors multiple mirrored switch ports		Yes
Offers availability monitoring of servers, applications, and networks	Yes	Yes
Offers self-monitoring and alerting	Yes	Yes. The CA Application Delivery Analysis Inactive Monitoring Device incident is supported. SNMP traps provide additional alerting.
Monitors URLs	Yes	No
Supports investigations from the CA Application Delivery Analysis management console	Yes	Yes. Enhanced packet-capture investigations are supported.
Collects all CA Application Delivery Analysis metrics	Yes	Yes
Supports automatic configuration of servers, applications, and networks	Yes	Yes
Ignores duplicate packets (from a mirrored VLAN, for example)	Yes, after extra configuration.	Yes, automatically.
Provides performance data at 1-minute granularity	No	Yes
Filters and displays captured data for the specified host, server, or application	No	Yes

Feature	Standard Monitor	Multi-Port Monitor
Receives packet digest data from a Cisco WAE device	Yes	Yes
Receives packet digest data from CA GigaStor	Yes	Yes
Supports CA Application Delivery Analysis on a 64-bit operating system	Yes	Yes. CA Application Delivery Analysis *must* be running on a 64-bit operating system to be compatible with Multi-Port Monitor.

Network Address Translation (NAT)

The Multi-Port Monitor requires some additional configuration to work properly in an environment where network address translation (NAT) is enabled between the Multi-Port Monitor and the ADA Manager. Be sure to:

1. Use the setNatInfo command-line utility to update the Multi-Port Monitor with the translated IP addresses.
2. Specify the translated IP address of the Multi-Port Monitor when adding the monitoring device to CA Application Delivery Analysis.

By default, the Multi-Port Monitor and the ADA Manager use their management IP address to communicate with each other.

To view the IP addresses that the Multi-Port Monitor and the ADA Manager currently use to communicate with each other, click the System Status page. The System Information section displays the management IP addresses, and if specified, the translated IP addresses.

Use the command-line utility, /opt/NetQoS/scripts/setNATInfo.php, to specify the translated IP addresses. The usage is as follows:

/opt/NetQoS/scripts/setNATInfo.php [--console d.d.d.d] [--probe d.d.d.d]

Where:

--console

Is the translated IP address of the ADA Manager. The Multi-Port Monitor accesses the ADA Manager through this address.

--probe

Is the translated IP address of the Multi-Port Monitor. The ADA Manager accesses the Multi-Port Monitor through this address.

Use the command-line utility to perform the following tasks:

View a usage statement

Run the utility with no parameters: /opt/NetQoS/scripts/setNATInfo.php

Specify the translated IP address of the ADA Manager

Run the utility with the following parameter: /opt/NetQoS/scripts/setNATInfo.php --console d.d.d.d

Specify the translated IP address of the Multi-Port Monitor

Run the utility with the following parameter: /opt/NetQoS/scripts/setNATInfo.php --probe d.d.d.d

Specify the translated IP address of the ADA Manager and the Multi-Port Monitor

Run the utility with the following parameters: /opt/NetQoS/scripts/setNATInfo.php --console d.d.d.d --probe d.d.d.d

Reset (clear) the NAT information in the database

Run the utility with the NULL keyword: /opt/NetQoS/scripts/setNATInfo.php --console NULL --probe NULL

Overview of CA Application Delivery Analysis Data

The CA Application Delivery Analysis product documentation provides information for interpreting report data and for diagnosing issues that stem from a monitored network, server, or application.

The metric that serves as a starting point for any troubleshooting activity is transaction time, another term for response time. A transaction consists of the following components:

- One request and one server response
- One period of data transfer
- One or more acknowledgments
- Observed latency from retransmitted packets

CA Application Delivery Analysis data identifies performance from the network perspective. Corresponding data in an analysis highlights activity and performance data with multiple views of TCP sessions, volume statistics, and response times. As you investigate a performance issue, consider the transaction time and related metrics such as throughput.

Note: Session-level performance data is available only for the IPv4-based port mirror data that is received on the Multi-Port Monitor logical ports. Session level data is not available for the packet digest data from CA GigaStor or from WAE devices.

The process is as follows:

- Click Session Analysis in an CA Application Delivery Analysis report.
- CA Application Delivery Analysis passes information to Multi-Port Monitor to identify the context and time frame of the data for the selected network, server, or application.
- In a separate browser window, the Multi-Port Monitor web interface opens to the Analysis page. Data is filtered to display relevant performance data for the selected context. The graphs in an analysis look different from the graphs displayed in CA Application Delivery Analysis because Multi-Port Monitor data is available in 1-minute increments. The smallest CA Application Delivery Analysis reporting interval is 5 minutes.

Averaging of metrics is also different because of the different reporting interval lengths. Your configuration determines whether data displayed in the analysis appears in the management console. For example, data from networks that are not defined in CA Application Delivery Analysis is available only in the analysis.

- You can apply more filters, select different chart formats, change the time frame, and save custom analyses.

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: Multi-Port Monitor as a Monitoring Device

The Multi-Port Monitor appliance is a monitoring device for CA Application Delivery Analysis.

In environments where network address translation (NAT) is enabled between the Multi-Port Monitor and the ADA Manager, be sure to:

1. Use the setNatInfo command-line utility to update the Multi-Port Monitor with the translated IP addresses.
2. Specify the translated IP address of the Multi-Port Monitor when adding the monitoring device to CA Application Delivery Analysis.

Tip: Take the following optional steps before configuring the appliance as a monitoring device.

- Configure hardware filters to control the data that is sent to CA Application Delivery Analysis.
- Assign meaningful labels to each logical port to make it easier to identify each data source.

This section contains the following topics:

Add the Monitoring Device (see page 18)
Verify Logical Port Status (see page 20)
Review TCP Session Information (see page 20)

More information:

Network Address Translation (NAT) (see page 12)

Add the Monitoring Device

Add a Multi-Port Monitor as a monitoring device for CA Application Delivery Analysis.

In environments where network address translation (NAT) is enabled between the Multi-Port Monitor and the ADA Manager, be sure to:

1. Use the setNatInfo command-line utility to update the Multi-Port Monitor with the translated IP addresses.
2. Specify the translated IP address of the Multi-Port Monitor when adding the monitoring device to CA Application Delivery Analysis.

By default, the Multi-Port Monitor and the ADA Manager use their management IP address to communicate with each other.

Follow these steps:

1. Disable the popup blocking feature in your web browser. CA Application Delivery Analysis uses popups when it adds the monitoring device.
2. Log in to the CA Application Delivery Analysis management console as a user with Administrative privileges.
3. Click Administration, Data Monitoring, Monitoring Devices.

   The ADA Monitoring Device List opens.
4. Click Add ADA Monitor.

   The Standard Monitor Properties page opens.
5. Complete the following fields:
   - **Server Name**. Type the server name for the appliance. If you do not know the server name, type an IP address in the Management Address field and click DNS. CA Application Delivery Analysis attempts to resolve the IP address.
   - **Management Address**. Type the IP address of the Multi-Port Monitor management NIC. If you do not know the IP address, type the DNS name in the Server Name field and click IP. CA Application Delivery Analysis attempts to resolve the DNS name.
   - **Incident Response**. Select a response for monitoring device incidents
   - **Availability Monitoring**. (*Optional*) Select Enabled to let CA Application Delivery Analysis monitor the availability of the appliance every 5 minutes.
   - **Is Multi-Port Monitor**. Select this option to add a CA Multi-Port Monitor. This option is displayed when the management console cannot contact the monitoring device by host name or IP address.

Note: The following fields do not apply to Multi-Port Monitor:

- Enable Multiple Monitor NICs
- Monitor Address
- Disable Packet Monitoring

6. Click OK.

   The ADA Monitoring Device List refreshes to show that the appliance is available.

7. (Optional) If domains are implemented in CA Performance Center, assign the correct domain to each monitor feed. By default, all monitor feeds are assigned to the Default Domain.

   a. Click to edit the CA Multi-Port Monitor monitoring device.

   b. In the Multi-Port Monitor Properties, the list of monitor feeds corresponds to the logical ports on the CA Multi-Port Monitor. Manage each monitor feed, including:

   - The domain where you want to report:
     - VLAN-tagged traffic. Click Assign VLANs to assign particular VLAN traffic to a domain, and to designate a domain for unassigned VLAN traffic.
     - Untagged traffic. Click the edit icon () to specify the domain for untagged traffic on the monitor feed.

     If you are not using domains to separate duplicate IP traffic, this is not applicable.

   - The monitor feed for redundant data monitoring, for example, when the same traffic fails over to a different network.

     To pair a secondary monitor feed, click the edit icon () and then click the Secondary Feed column. Avoid data duplication by only assigning a secondary monitor feed that sees the same traffic that the monitor feed sees.

   - The active sessions information.

     To view active sessions information, click Active Sessions. Active sessions information helps you understand whether the monitor feed is monitoring active TCP sessions.

8. Click the blue gear menu () and click Synchronize Monitor Devices.

   CA Application Delivery Analysis sends monitoring instructions to the appliance.

9. Configure the networks, servers, and applications that you want to monitor. The *CA Application Delivery Analysis Administrator Guide* contains complete instructions.

10. Navigate to the ADA Monitoring Device List and synchronize again.
11. Review the ADA Monitoring Device List to confirm that the appliance sends data to CA Application Delivery Analysis

Note: The Last Monitored and Status fields are updated after you configure at least one valid server subnet and one network. It can take up to 10 minutes before the appliance sends data to CA Application Delivery Analysis.

Verify Logical Port Status

Verify logical port status for Multi-Port Monitor from CA Application Delivery Analysis. A logical port is a source of TCP response-time data. You can view the status of logical ports, which are identified as monitor feeds in the CA Application Delivery Analysis management console.

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

Follow these steps:

1. Click Administration, Data Monitoring, Monitoring Devices in the CA Application Delivery Analysis management console.

   The device name of the appliance appears in the ADA Monitoring Device List.

2. Click the Edit icon in the Options column ().

   The Multi-Port Monitor Properties page opens. The Monitor Feeds table provides status information for each logical port.

3. Click Help for a description of the information in the table.

Review TCP Session Information

Review TCP session information for Multi-Port Monitor in CA Application Delivery Analysis. For each logical port on the Multi-Port Monitor, CA Application Delivery Analysis reports the number of active IPv4-based TCP sessions, with a server name, address, VLAN identifier, and port number to identify the traffic. A logical port is identified as a monitor feed in the CA Application Delivery Analysis management console. If a monitor feed separates tagged VLAN traffic into domains, CA Application Delivery Analysis reports all of the sessions in the monitor feed.

Follow these steps:

1. Click Administration, Data Monitoring, Monitoring Devices in the CA Application Delivery Analysis management console.

   The device name of the appliance appears in the ADA Monitoring Device List.

2. Click the Edit icon in the Options column ().

   The Multi-Port Monitor Properties page opens.

3. Click Active Sessions in the third Show Me list.

   The Active Sessions page opens.

4. Select a monitor feed to view its session information.

   The Active Sessions page provides information about monitored servers and their corresponding feeds. The Active Sessions data is helpful for verifying the setup of the appliance and mirror ports, and for troubleshooting network or server issues.

5. Click Help for information about the fields on the Active Sessions page.

Chapter 3: Incidents for Monitoring Devices

In the CA Application Delivery Analysis management console, the Administrator can specify whether to create a monitoring device incident when Multi-Port Monitor or a monitoring feed becomes inactive.

An Inactive Monitor incident is raised when CA Application Delivery Analysis stops receiving data from a single-port monitor, a Multi-Port Monitor, or a monitoring feed. All monitoring device incidents have an Excessive severity. CA Application Delivery Analysis does not create Degraded monitoring device incidents.

Multi-Port Monitor also sends SNMP traps in response to issues associated with the following events:

- Critical process status
- Packet capture functionality
- Disk usage levels
- RAID array and disk drive failures

A monitoring device is considered to be inactive when CA Application Delivery Analysis stops receiving performance data from that device. For example:

- The network is down. No data is generated.
- The monitoring device is down. Data is present on the mirror port, but the monitoring device is not active.
- A feed that is assigned to the monitoring device is inactive. For example, a WAN optimization device is unavailable.
- The mirror port connection is lost. Data is generated, but the port is not active.

The incident can be created even when some logical ports still send data to CA Application Delivery Analysis. For example, monitor feeds that are assigned to Multi-Port Monitor stop sending packet digests, but other ports remain active. Therefore, the incident does not necessarily indicate complete inactivity for Multi-Port Monitor.

This section contains the following topics:

Enable Monitoring Device Incidents (see page 24)
Respond to an Inactive Monitoring Device Incident (see page 25)

Enable Monitoring Device Incidents

A default Monitoring Device incident response is assigned to each monitoring device. The default response is not associated with an action. You associate an incident response with an action on the Multi-Port Monitor Properties page in CA Application Delivery Analysis. The typical CA Application Delivery Analysis work flow is as follows:

- Create a Monitoring Device incident response.
- Add an action to the response, such as an email notification.
- Select the new incident response in the device properties.

The “Availability Monitoring” setting on the Multi-Port Monitor Properties page determines whether CA Application Delivery Analysis raises Inactive Monitoring Device incidents for Multi-Port Monitor. The setting is enabled by default on all new monitoring devices. To prevent CA Application Delivery Analysis from creating Inactive Monitoring Device incidents, disable availability monitoring on the device.

The CA Application Delivery Analysis online help contains guidance for creating incident responses. However, the following overview of the procedure can help you get started.

Follow these steps:

1. Click Administration, Policies, Incident Responses in the CA Application Delivery Analysis management console.
2. Click Add Monitoring Device Response.

   The Monitor Device Incident Response Properties page opens.
3. Type a name for the new incident response, and click OK.

   The new incident response appears in the Monitoring Device Incident Responses list.
4. Click the Edit icon for the new response.

   The Monitor Device Incident Response Actions page opens.
5. Click Add Action.

   The Monitoring Device Action Types page opens.
6. Select Send Email or Send SNMP Trap, and then click Next.
7. Complete the required fields, which vary depending on the action you selected.
8. Click OK.

   A description of the action appears in the Monitor Device Incident Response Actions page.

9. Enable the incident response:
   a. Click Administration, Data Monitoring, Monitoring Devices in the management console.

      The ADA Monitoring Device List opens.

   b. Click the Edit icon for the Multi-Port Monitor.

      The Multi-Port Monitor Properties page opens.

   c. Select the new incident response from the Incident Response field.

   d. Click OK.

   The selected action is performed when an Inactive Monitoring Device incident is created.

Respond to an Inactive Monitoring Device Incident

If you receive an Inactive Monitoring Device incident, perform one or more of the following tasks:

- Click the date link on the CA Application Delivery Analysis Incident page for more information.
- Review your trap receiver for alerts. Multi-Port Monitor sends SNMP traps for issues that can affect data monitoring and capture.
- Review the System Status page in the Multi-Port Monitor web interface. The page lets you assess whether the incident stemmed from a:
  - Hardware or software issue. Review the Process Information table for stopped processes.
  - Network issue. Review the Capture Card Physical Port Status table for links that are not connected or have gone down.
  - Monitor feed issue. Review the Capture Card Logical Port Status table for feeds that are inactive. An inactive WAN optimization device or CA GigaStor is not reported here.
  - Configuration issue. Review the Capture Card Logical Port Status table for logical ports that have a state of Disabled. Verify whether these ports show packet counts in the "Packets Processed" column.
  - Packet-capture issue. Review the Capture Card Physical Port Statistics table for abnormal error counts and values of "0" in the "Packets" or "Bytes Received" columns.
  - RAID drive issue. Review the RAID table for RAID status and failed drives.

Chapter 4: Support for Special Initialization (.ini) Files

Multi-Port Monitor supports scenarios in which more parameters are required to instruct monitoring devices to ignore irrelevant data. These parameters are distributed to monitoring devices by the following supported initialization (.ini) files.

DataTransferManager.ini

Sets the TCP port number on which the sadatransfermanager process listens for client connections. Do not change this port number.

DTMDistributedConsoles.ini.sav

Controls which IP addresses receive shared packet digest data. For more information, see the DTMDistributedConsoles.ini.readme file located in the /opt/NetQoS/bin directory on the Multi-Port Monitor appliance.

LimitDTTParams.ini.sav

Controls the Data Transfer Time threshold.

LimitServerResponseParams.ini.sav

Controls the Server Response Time threshold.

RetransPacketDefs.ini.sav

Controls software deduplication.

saCollectorOptions.ini

Contains the default debug trace logging flags that the nqmetricd service uses. A CA Technical Support technician can tell you which flags to enable when more logging is required.

saLinuxCollectorDirectives.ini

Defines the naming formats for log files and the parameters for accessing the local MySQL database. Do not change this information.

saMetricEngine.ini.sav

Controls the size of the Active Sessions report. For more information, see the saMetricEngine.ini.readme file located in the /opt/NetQoS/bin directory on the Multi-Port Monitor appliance.

Other initialization files are documented in the *CA Application Delivery Analysis Administrator Guide*.

This section contains the following topics:

Eliminate Duplicate Packets (see page 28)
Filter Out Keep-Alive Messages (see page 29)

Eliminate Duplicate Packets

Multiple mirror port configurations can result in packet duplication on a Multi-Port Monitor feed. This section discusses the best practices for mirroring TCP traffic to Multi-Port Monitor in environments where the typical hardware filtering options do not suffice.

Discarded packets in the SuperAgentErrors.log file are not a factor here. The CA Application Delivery Analysis single-port monitor *discards* a packet that does not match the CA Application Delivery Analysis configuration. By contrast, *dropped packets* can cause problems because CA Application Delivery Analysis does not analyze dropped packets.

When you mirror VLANs to a CA Application Delivery Analysis monitoring device, CA Application Delivery Analysis receives two copies of each VLAN packet. To correct this duplicate packet situation, you can pass more configuration parameters to Multi-Port Monitor. Use the "sudo" command prefix because superuser permissions are required to modify the files in this directory.

Follow these steps:

1. Navigate to the /opt/NetQoS/bin/ directory on the Multi-Port Monitor appliance.

   ```
   cd /opt/NetQoS/bin
   ```

2. Copy the RetransPacketDefs.ini.sav file to remove the extension.

   ```
   sudo cp RetransPacketDefs.ini.sav RetransPacketDefs.ini
   ```

   The .ini file is activated during the next monitor synchronization or when the nqmetricd process is restarted.

3. Add the following lines of code to the RetransPacketDefs.ini file:

   <nologging>

   50 1000

   10 20 30 40 50 60

   The first line instructs CA Application Delivery Analysis not to log information about duplicate packets. The single-port monitor supports this type of logging. Multi-Port Monitor does not.

   The second line indicates how the retransmitted data filtering is applied. The numbers 50 and 1000 instruct CA Application Delivery Analysis to maintain a buffer of 50 packets to look for duplicates. If you reduce this parameter, Multi-Port Monitor consumes fewer CPU cycles when looking for duplicates. As a result, Multi-Port Monitor performance is improved, but fewer duplicates are found. These default values are recommended.

   The third line describes the bins of the histogram of duplicates. The single-port monitor supports the histogram as part of the logging option. Multi-Port Monitor does not.

4. Restart the nqmetricd process from the Multi-Port Monitor web interface.

Filter Out Keep-Alive Messages

You can limit the impact of application keep-alive messages on monitoring statistics in reports. Limit Server Response Time (SRT) or Data Transfer Time (DTT) to a maximum value so that unnecessary SRT or DTT observations are ignored. You can set the value to a number of seconds that falls below the keep-alive frequency.

If you suspect that an application sends keep-alive messages, look for the inverse relationship between observations and SRT. Also look for SRT averages in seconds instead of the milliseconds. Apply a threshold to the SRT when you verify that the application sends keep-alive messages.

If your application uses keep-alive messages that result in high DTT, you can apply a similar limit to filter DTT.

If you are unsure of the keep-alive frequency of a selected application, use 10 seconds as a starting point. In general, a server is unlikely to take more than 10 seconds to start responding to a user request. In most cases, the keep-alive frequency is greater than 10 seconds.

Note: You can also apply SRT and DTT filters on the CA Application Delivery Analysis single-port monitor. For more information, see the *CA Application Delivery Analysis Administrator Guide*.

Follow these steps:

1. Navigate to the /opt/NetQoS/bin directory on the Multi-Port Monitor appliance.

   ```
   cd /opt/NetQoS/bin
   ```

   Note: Root permission is required to modify files in the /opt/NetQoS/bin directory. Therefore, use the "sudo" prefix with all commands described in this procedure.

2. Specify an SRT threshold.

   a. Copy the LimitServerResponseParams.ini.sav file to remove the extension:

      ```
      sudo cp LimitServerResponseParams.ini.sav LimitServerResponseParams.ini
      ```

      The .ini file is activated during the next synchronization or when the nqmetricd process is restarted.

   b. Verify that the new file is writeable:

      ```
      sudo chmod u+w LimitServerResponseParams.ini
      ```

   c. Edit the .ini file to change the SRT threshold for each port that you want to filter.

      For each application, type the port number and the maximum amount of acceptable SRT. Set the maximum SRT to a value that is slightly less than the keep-alive frequency. For example, to ignore Citrix keep-alive messages that occur at a frequency of 60 seconds, enter the following values:

      ```
      -port=1494 -max seconds=59
      ```

      Note: In this example, max seconds is a single parameter name that contains a space.

   d. Save the file.

3. Specify a DTT threshold for each port that you want to filter.

   a. Copy the LimitDTTParams.ini.sav file to remove the extension:

      ```
      sudo cp LimitSDTTParams.ini.sav LimitDTTParams.ini
      ```

   b. Configure the new file as writeable:

      ```
      sudo chmod u+w LimitDTTParams.ini
      ```

   c. Edit the .ini file to change the DTT threshold as described in step 2.

   d. Save the file.

4. Restart the nqmetricd process in the Multi-Port Monitor web interface.

Chapter 5: Monitoring in a WAN-Optimized Environment

CA Application Delivery Analysis integrates with WAN optimization solutions, such as Cisco Wide Area Application Services (WAAS), to monitor application performance. In a WAN-optimized environment, application data is not visible to a monitoring system. The data appears to be from the WAAS device and not from the actual hosts. CA Application Delivery Analysis integrates with WAN optimization devices to gain visibility into how WAN optimization affects individual application response times.

Cisco WAAS requires multiple Cisco Wide Area Application Engine (WAE) devices at key points in the network, such as data centers and branch offices. Cisco WAE devices and WAN optimization devices send performance data to CA Application Delivery Analysis monitoring devices. This data provides visibility into how WAN optimization affects application response times at segments of the network.

Multi-Port Monitor receives performance data from a WAN optimization device as it sends that data over a monitored mirror port. You manually activate WAN optimization support during Multi-Port Monitor configuration. The process is described in the *CA Application Delivery Analysis Administrator Guide*.

This section contains the following topics:

CA Application Delivery Analysis Support for Cisco WAAS (see page 31)
How Multi-Port Monitor Integrates with a WAN Optimization Device (see page 32)
The CA Application Delivery Analysis Optimization Report (see page 33)
Sharing Data from WAN Optimization Devices (see page 34)

CA Application Delivery Analysis Support for Cisco WAAS

When CA Application Delivery Analysis is configured for monitoring a Cisco WAAS environment, the WAE devices export FlowAgent data to a CA data source. Cisco WAAS effectively creates three distinct TCP segments for the network. Transaction performance data is collected from each segment and correlated. CA Application Delivery Analysis monitors from multiple monitoring points for one optimized application-server-network combination. Therefore, CA Application Delivery Analysis generates a separate set of metrics for each TCP segment and treats each set as a separate application.

To provide full visibility into Cisco WAAS effectiveness, CA Application Delivery Analysis reports application performance per segment, as follows:

- [Client] segment: The network segment between the clients in a branch location and the WAE device for that branch location
- [WAN] segment: The network segment between the branch WAE device and the WAE device running in the data center
- [Server] segment: The network segment between the WAE device and the servers in the data center

Application behavior on all three segments is analogous to that of a three-tier application. The source and destination ports and addresses remain the same throughout the tiers. A new CA Application Delivery Analysis application property monitors the WAN-optimized applications and identifies each segment.

CA Application Delivery Analysis reports append a segment identifier to the application name. For example, HTTP application traffic can be identified as three separate items: HTTP [Client], HTTP [WAN], and HTTP [Server]. An additional report, the CA Application Delivery Analysis Optimization page, shows data for optimized transactions. The default view, Client Experience for Optimized Transactions, provides a performance map of client segments for applications with segmented data.

How Multi-Port Monitor Integrates with a WAN Optimization Device

The sadatatransfermanager process aggregates data on the TCP headers that it receives from WAN Optimization devices. The process is always running, even when not actively transferring or aggregating data. You can stop or restart it.

The WAN Optimization device polls the Multi-Port Monitor appliance every 5 minutes for a list of servers to monitor. The device sends packet digest files to the appliance. These files contain TCP headers from the optimized traffic that matches the server list on the WAN Optimization device. The device does not send TCP headers for unoptimized traffic.

The appliance performs the following tasks for the packet headers it receives from the WAN Optimization device:

- Calculates performance metrics for the optimized traffic on the Client and WAN segments.
- Replaces the Server segment performance data that is sent from the WAN Optimization device with more accurate data that is sent from the mirrored port.
- Automatically detects application traffic in the port mirror and provides an updated list of servers. CA Application Delivery Analysis propagates this list to all WAN Optimization devices to verify that all servers are monitored.

The sadatatransfermanager process listens on port 7878 for incoming packet headers from the WAN Optimization device.

The CA Application Delivery Analysis Optimization Report

Multi-Port Monitor processes the contents of packet digests and sends performance metrics to CA Application Delivery Analysis. These metrics are displayed on the Optimization page in the management console.

The default view on the Optimization page is the Client Experience for Optimized Transactions, a performance map of transaction times and observations. The applications with the longest transaction times (response times) are listed first.

The Optimization page does not let you navigate to a Session Analysis in Multi-Port Monitor. However, the name of each application is a link to a Components report for that application. This report breaks transaction time into the following components:

- Server response time
- Network round-trip time
- Retransmission delay
- Data rates and volumes

The Components report page provides links to information about related incidents and availability.

Sharing Data from WAN Optimization Devices

One CA Application Delivery Analysis management console can typically support all WAN optimization devices in your environment. However, you can distribute the load when your WAN optimization deployment requires more monitoring devices than a management console can support. The following procedure describes how to share the performance data for [Client], [WAN], and [Server] segments among several Multi-Port Monitors.

Follow these steps:

1. Create a configuration file named DTMDistributedConsoles.ini.
2. Open the .ini file.
3. Type the IP address of the management console that is assigned to Multi-Port Monitor. The management console instructs Multi-Port Monitor how to find other monitoring devices to receive the shared data.

   Note: A sample file is provided. The sample contains invalid IP addresses to illustrate the proper file format. Locate the sample in the /opt/NetQoS/bin folder.
4. Separate each IP address on a new line using dotted decimal notation.
5. Copy the DTMDistributedConsoles.ini file to all monitoring devices. For Multi-Port Monitor, copy the file to the /opt/NetQoS/bin folder.
6. Restart the sadatatransfermanager process.

   Up to 25 minutes can elapse before WAN-optimized client segment data is shared between the monitoring devices.
7. To share data with more monitoring devices, repeat steps 2 through 5.

Note: More information about sharing data from WAN optimization devices is available in the *CA Application Delivery Analysis Administrator Guide*.

Index

A

appliance
  port requirements • 14
Application Delivery Analysis
  architecture • 9
  data in Multi-Port Monitor • 13
  packet-capture investigations • 8
  review TCP sessions • 20
  verify port status • 20
architecture
  Multi-Port Monitor and CA ADA • 9

C

capture files
  investigations • 8
Cisco Wide-Area Application Service, monitoring • 31
collector feed
  port requirements • 14

F

filters
  keep-alive messages • 29

G

GigaStor, port requirements • 14

I

incidents
  enable • 24
  inactive • 25

K

keep-alive messages, filtering • 29

L

logical ports
  and TCP sessions • 20
  view status in Application Delivery Analysis • 20

P

packets
  deduplication • 28
port mirroring, best practices • 28
port requirements • 14

S

sadatatransfermanager process • 32
session analysis, examples of • 13
SNMP traps
  port requirements • 14

U

UDP, port requirements • 14