

Analysis Guide

CA Application Delivery Analysis Multi-Port Monitor

Version 10.1



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.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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?	7
---	----------

Chapter 2: How to Log In to the Web Interface	9
--	----------

Chapter 3: What is an Analysis?	11
--	-----------

The Analysis Page	12
Analysis Menu	13
Predefined Analyses	14
Create a Custom Analysis	16
Duplicate an Analysis	17
Delete a Custom Analysis	17
Data Views.....	18

Chapter 4: Using Filters to Customize Data in the Display Area	21
---	-----------

View the Current Filter Conditions.....	23
Analysis Filters.....	23
Create an Analysis Filter	23
Change the Properties of an Analysis Filter	30
Delete an Analysis Filter	31
Global Filters	31
Global Filters Dialog	32
Modify a Global Filter.....	33
Clear a Modification to a Global Filter	34

Chapter 5: Understanding the Data in the Display Area	35
--	-----------

Types of Charts.....	36
Bar Chart	36
Line Trend Chart.....	37
Pie Chart.....	37
Stacked Trend Chart.....	38
Summary Trend Chart	38
Types of Data.....	39
Data on the Traffic Tab.....	39
Data on the TCP Tab.....	43
Byte Counts for Networks and Hosts	48

Add or Remove Columns in a Data Table.....	48
Chapter 6: Exporting Data	49
Export Data to a PDF File.....	49
Export Data to a CSV File.....	50
Export Data to a PCAP File.....	51
Share Data by Email	52
Appendix A: Command Line Syntax	55
Appendix B: Regular Expression Syntax	57
Index	59

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 analyze data.

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 web interface opens.

Chapter 3: What is an Analysis?

An analysis is a description of a troubleshooting path into packet-level session data that is stored on the Multi-Port Monitor appliance. The description proceeds as a series of hierarchically organized views of the data.

Multi-Port Monitor offers two types of analysis.

Predefined Analysis

Provides access to IPv4-based TCP session-level information that is used when drilling in from a CA Application Delivery Analysis report or CA APM Defect Details page.

For example, you examine the CA Application Delivery Analysis Components report and narrow the data for the 192.94.5.6 network. When you click the Session Analysis button, an analysis for the selected report appears on the Multi-Port Monitor Analysis page. The selected network and time frame filter the session-level data in the analysis.

Custom Analysis

Provides options for filtering and viewing session-level metrics that speed up the troubleshooting process. The Multi-Port Monitor user can create, save, and reuse custom analyses.

For example, the drilldown, or Session Analysis, path from CA Application Delivery Analysis places you in a preselected context that is not applicable to your situation. You create an analysis or open a saved analysis to save some steps in selecting the desired views and their hierarchical arrangement. The associated charts and tables provide a sufficiently narrowed perspective on the data you want to analyze.

All analyses are displayed in the Analysis pane, to the left of the Display area on the Analysis page.

Filters are added to analyses at the view level and are applied to all subordinate views within the same analysis.

New analyses do not contain default data views. Add a view to data before applying a new analysis.

This section contains the following topics:

[The Analysis Page](#) (see page 12)

[Analysis Menu](#) (see page 13)

[Predefined Analyses](#) (see page 14)

[Create a Custom Analysis](#) (see page 16)

[Duplicate an Analysis](#) (see page 17)

[Delete a Custom Analysis](#) (see page 17)

[Data Views](#) (see page 18)

The Analysis Page

Granular views of session-level network data appear on the Analysis page in the web interface. The Analysis page contains two panes.

Display area

The right pane, which contains a chart and a data table. Tabbed views provide easy access to formatted performance metrics. The chart and table provide multiple options for viewing data, selecting chart formats, and sorting metrics to find outliers.

Note: Although Multi-Port Monitor reports data at a 1-minute granularity, it loads collected metrics to the database every 2 minutes, for performance reasons. This difference causes a delay before you can view the most recent collected data in the Display area.

Analysis pane

The left pane, which contains options for selecting data views and filtering the data shown in the Display area. You can create analytical filters for data views and can save them as reusable troubleshooting work flows. A list of active filters appears at the top of the Analysis pane. The primary filtering types are:

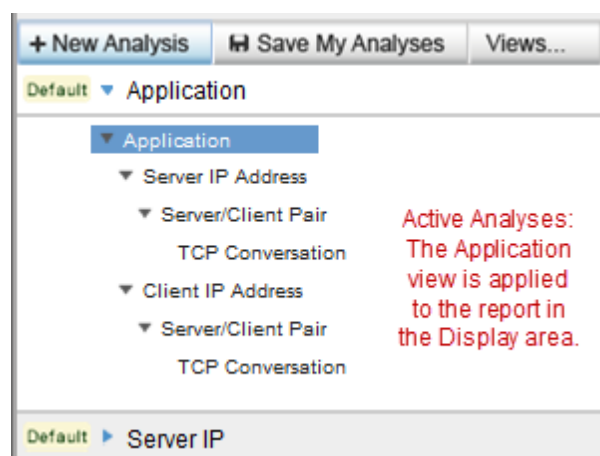
- [Analysis filters](#) (see page 23) are explicitly applied to data when you click Add Analysis Filter. They are implicitly created when you double-click an item in the Display area.
- [Global filters](#) (see page 31) apply to all analyses and are based on a drill-down context from CA Application Delivery Analysis.

Analysis Menu

Use the Analysis menu for viewing, creating, and modifying analyses. The menu is visible by default in the Analysis pane of the Analysis page. You can hide it to expand the available viewing area for charts and tables.

Click the << or >> symbol (labeled Analysis Menu) to hide or display the Analysis pane.

Within the Analysis pane, the active analysis is highlighted in blue with white text. The active analysis and its filters are applied to the report that is visible in the Display area.



Child views of the active analysis are available to report increasing levels of detail, down to the TCP conversation level in some analyses. Their associated filters are designed to include or exclude specific sessions in the metrics shown in the Display area.

Expand an analysis to see the associated views. Click the blue arrow next to the analysis name to expand or collapse it. Collapsing or expanding an active analysis does not remove or add filters.

You can apply another view to the current time frame to look at the data in a different context. To apply another analysis, expand it in the Analysis pane, and then click an associated view.

Predefined Analyses

Predefined analyses are sorting and display options that help you analyze data. They have a designation of "Default" in the Analysis menu.

You can temporarily customize predefined analyses by adding analysis filters. You cannot save these modifications, which persist only for the current login session.

All analyses mine the data to an increasing level of granularity. Each view into the data is associated with a predefined analysis. When you select an analysis, it expands to show a list of views in a hierarchical structure. This structure represents the increasing level of detail that you can access from the monitored data. Each view thus provides access to more detailed metrics stored in the database for the selected time frame.

Analyses aid troubleshooting efforts by helping you investigate a particular item. With any analysis, it is helpful to think of the initial data view as corresponding to the item being investigated. For example, the Client IP Address analysis helps you find the source of an issue with a client computer whose IP address is known. First, the Client view is applied. Double-click a client to drill down to the next view in the analysis, which shows all servers that conversed with that client.

Multi-Port Monitor offers the following predefined analyses.

Application

Use this analysis to identify an application that has a problem. This analysis identifies the IP address of the server where the application is running and the port numbers that the application uses. Contains the following data views:

Server IP Address --> Server/Client Pair --> TCP Conversation

Client IP Address --> Server/Client Pair --> TCP Conversation

Server IP or Client IP

Use this analysis to identify a single host that has a problem. Contains the following data views:

Server IP Address --> Server/Client Pair --> TCP Conversation

Client IP Address --> Server/Client Pair --> TCP Conversation

Network

Use this analysis to identify the problem for multiple hosts on a subnet. Contains the following data views:

Server IP Address --> Server/Client Pair --> TCP Conversation

Client IP Address --> Server/Client Pair --> TCP Conversation

IP Address

Use this analysis to identify a single host that has a problem. Contains the following data views, which are organized into several possible filtering paths through the captured data:

Server IP Address --> Server/Client Pair --> TCP Conversation

Client IP Address --> Server/Client Pair --> TCP Conversation

IP Address Pair --> IP Session

Protocol

Use this analysis to identify the problem for traffic that uses a single protocol. Contains the following data views:

IP Address --> IP Address Pair --> IP Session

Create a Custom Analysis

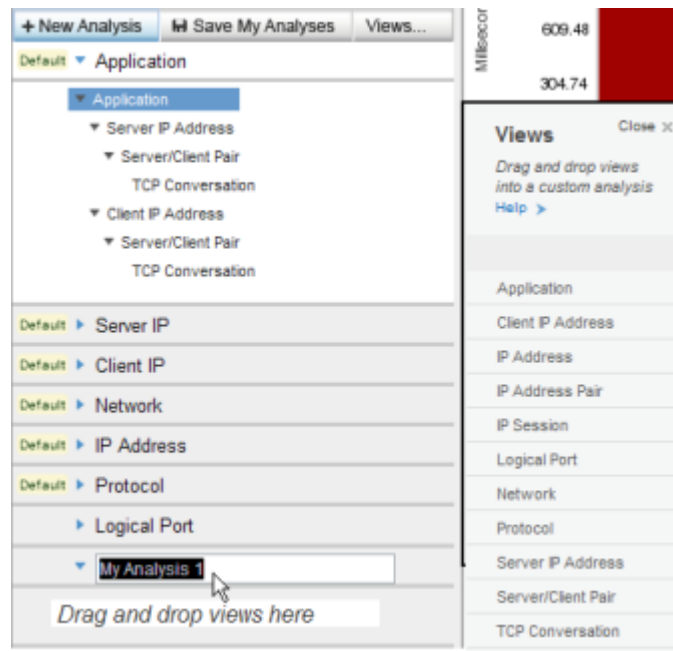
Predefined analyses cannot be permanently modified. Create a custom analysis to preserve filters or analytical work flows.

Follow these steps:

1. Click New Analysis in the Analysis pane.

A new item appears in the Analysis pane. The default name, My Analysis 1, is highlighted.

The Views pane opens to the right of the Analysis pane.



2. Type a name for the new analysis in the highlighted field.
3. Select a view to add to your custom analysis in the Views pane.
4. Drag the view to the "Drag and drop views here" section of the Analysis pane.
5. Repeat Steps 3 and 4 to add data views to your analysis. We recommend adding views in a hierarchical flow of increasing granularity, with more items filtered out as the views proceed downward.

6. *(Optional)* Add advanced filters. Right-click a view and select Add Analysis Filter.
The Add Analysis Filter dialog opens. For descriptions of the fields, see [Filters for Data Views](#) (see page 23).
7. Click Save My Analyses.
The custom analysis is saved. Multiple changes can be saved simultaneously.
Important: If you are viewing an emailed analysis, clicking Save My Analyses overwrites all saved analyses.

Duplicate an Analysis

You can duplicate custom and predefined analyses. The duplication feature lets you save modifications to an analysis.

Follow these steps:

1. Right-click the analysis that you want to duplicate in the Analysis pane.
2. Select Duplicate.
A new analysis appears in the Analysis pane, with the naming convention of "My Analysis #."
3. Type a new name for the duplicated analysis.

Delete a Custom Analysis

You can delete a custom analysis. You cannot delete a predefined analysis.

Follow these steps:

1. Right-click the name of the analysis you want to delete in the Analysis pane.
2. Select Delete Analysis.
3. Click OK in the confirmation message.
The analysis is removed from the Analysis pane.

Data Views

Data views help you investigate an area of network performance. Predefined analyses contain data views. You can create and modify custom analyses with their own sets of views.

The Views menu opens automatically when you create an analysis. You can also click the Views button to see the list of available data views.

You can use the following items to customize data views:

- Filters, which focus on the traffic of interest.
- Chart formats, which graphically display performance metrics of interest.
- Data table settings, which selectively display metrics of interest. For each view, a default sorting method is applied. For example, in the Protocol analysis, protocols are sorted from highest byte rate to lowest.

You can customize data views. Some changes are automatically saved to views, such as a change in the chart format.

Application

Highlights response time (Transaction Time in milliseconds) per application. Application names are derived from CA Application Delivery Analysis configuration or from well-known port usage. Where available, the application name is supplied. Otherwise, the port number is shown.

The default chart shows the trend in response times and their composition. The Transaction Time is broken down into Network Round-Trip Time, Retransmissions, Data Transfer Time, and Server Response Time.

Client IP Address

Highlights response time (Transaction Time in milliseconds) per client. Multi-Port Monitor identifies client computers from on the three-way handshake that initiates a TCP conversation. The chart shows the trend in response times and their composition.

IP Address

(Traffic tab) Highlights throughput (Byte Rate in bits per second) per host IP addresses, which are sorted by highest to lowest byte rate. The chart shows the directional Byte Rate, *to* and *from* the host with the highest rate.

IP Address Pair

(Traffic tab) Highlights throughput (Byte Rate in bits per second) per conversing pair of host IP addresses, which are sorted by highest to lowest byte rate. The chart shows the directional Byte Rate, *to* and *from* the pair of hosts with the highest rate.

IP Session

(*Traffic tab*) Highlights throughput (Byte Rate in bits per second) per session. Each session represents a conversing pair of host IP addresses. Sessions are sorted by highest to lowest Byte Rate. The chart shows the composition of the Byte Rate *to* and *from* the top ten sessions with the highest throughput.

Logical Port

Highlights response time per logical port, that is, per switch mirror port session, coming in to Multi-Port Monitor. The chart shows the trend in response times (as Byte Rate).

Network

Highlights response time (Transaction Time in milliseconds) per network. Networks are identified based on CA Application Delivery Analysis configuration. The chart shows the trend in response times and their composition.

Protocol

(*Traffic tab*) Highlights throughput (Byte Rate in bits per second) for each protocol that passes hardware filtering. The total number of bytes sent and received is shown, and the number of TCP bytes. The Layer 3 protocol is also indicated. The chart shows the throughput trend (as Byte Rate) over time.

Server IP Address

Highlights response time (Server Response Time in milliseconds) per server. The chart shows the trend in response times and their composition.

Server/Client Pair

Highlights response time (Transaction Time in milliseconds) per pair of hosts (client and server). The chart shows the trend in response times and their composition.

TCP Conversation

Highlights response time (Transaction Time in milliseconds) per session. Each session consists of a server host plus a client host and port. The chart shows the trend in response times and their composition.

More information:

[Create an Analysis Filter](#) (see page 23)

[View the Current Filter Conditions](#) (see page 23)

Chapter 4: Using Filters to Customize Data in the Display Area

Multi-Port Monitor offers several methods for narrowing the scope of session-level metrics shown in the Display area of the Analysis page. The following options can be applied to the data displayed from a selected analysis.

Data views

You can select different data views to focus on the network aspect that makes the most sense for the current troubleshooting task. For example, if an application has slow response time, select the Server IP view or the Application view to see the associated metrics.

Use [analysis filters](#) (see page 23) to filter the data in a view.

Note: Analysis filters are distinct from the Hardware filters you apply to captured data. Hardware filters affect the *capture* of data. Analysis filters affect the *display* of data.

Context-specific filtering

- Select a row or a series of rows in the data table. Right-click and select Apply As Filter to narrow the scope of data in the current analysis. To highlight multiple rows, use Ctrl+Click or Shift+Click.
- Use the mouse pointer to select a specific section of the chart. Release the mouse pointer and click Set. The chart refreshes to focus on a narrower segment, such as a spike in the line graph indicating exceptions to baseline metrics.

Drill-down filtering

- Double-click a row in the data table to drill one level down to the next view in the analysis.
- Drill down from an APM defect to view associated data on the Analysis page. An analysis filter is automatically created based on the context of the defect.
- Click Session Analysis in a CA Application Delivery Analysis report to view associated data on the Analysis page. [Global filters](#) (see page 31) on the Analysis page are based on the context of the CA Application Delivery Analysis report.

Zoom filtering

Line graphs provide more filtering options. The Zoom In and Zoom Out links let you focus more closely on the performance metrics from a smaller segment of captured data.

- Zoom In reduces the current time frame so that a smaller segment of data is charted.
- Zoom Out restores the time frame to a broader segment of data.

Time frame filtering

The Summary Trend chart, Line Trend chart, and Stacked Trend chart formats include a time-navigation component above the Display area. The default time frame is 15 minutes. The Time Period Selector enables precise selection of another time frame.

- The Backward and Forward buttons let you move forward or backward in time through the captured data. This type of time navigation lets you view trend data and follow each trend as it proceeds.
- The date, hour, and minutes are menus from which you can select other date and time parameters.
- The date is a graphical calendar menu with forward and backward navigation.
- The Timeframe link provides quick access to larger time segments, from "Last 15 Minutes" to "Last 180 Minutes."

This section contains the following topics:

[View the Current Filter Conditions](#) (see page 23)

[Analysis Filters](#) (see page 23)

[Global Filters](#) (see page 31)

View the Current Filter Conditions

You have several options for viewing the information about the filters that are applied to an analysis.

- Click the Show Filters link in the Analysis pane or in the Display area to see the following information:
 - A list of all global filters that are inherited from the CA Application Delivery Analysis report.
 - A list of analysis filters that are applied to the current data view.
- In an analysis, use the mouse pointer to hover over a filtered data view. The flyover text describes the conditions and syntax of the filter.
- In an analysis, right-click a data view and select Edit Analysis Filter. The Conditions field in the Edit Analysis Filter dialog identifies the conditions and syntax of the filter.
- In an analysis, click the filter icon. The Conditions field identifies the conditions and syntax of the filter.

Analysis Filters

You can apply regular expressions to data views to limit the data in the Display area. This type of filtering is an *analysis filter*.

Regular expression filters are applied directly to a data view that is a component of an active analysis. You can only save the filters as part of analysis customization.

Create an Analysis Filter

You can apply regular expressions to data views to limit the data in the Display area. This type of filtering is an *analysis filter*.

Regular expression filters are applied directly to a data view that is a component of an active analysis. You can only save the filters as part of analysis customization.

When you add an analysis filter to a data view, the new filter and any inherited filters are applied to the view. You can see the inherited filters in the Add Analysis Filter dialog.

Note: New filters do not modify inherited global filters. Instead, they provide an additional filter to the data that passed the global filters.

Follow these steps:

1. Right-click a view within an analysis and select Add Analysis Filter.

The Add Analysis Filter dialog opens. Filters that are inherited from another view in the same analysis are indicated in the Inherited Analysis Filters field.

2. Select filters from the Parameter field. As you click each item, help appears with the appropriate syntax for the Value.

3. Select an operator.

- Equals (=)
- Does Not Equal (!=)

4. Type a value to complete the expression. Use the syntax online help for guidance.

Note: The use of certain expressions in the Value field effectively disables the filter. Do not use the expressions from the list of [Reserved Filter Expressions](#) (see page 25).

5. Click Add to Conditions.

The filter statement appears in the Conditions field.

Note: To remove the filter statement, click [Clear] above the Conditions field. You can also edit the statement by typing in the Conditions field.

6. (*Optional*) Select a Boolean operator and repeat steps 3 through 5 to add conditions in relationship to the existing filter statement.

- AND (concatenation)
- OR (alternation)

7. Click OK.

The filter is validated. If valid, it is applied to the data table and chart in the Display area. A filter icon appears next to the view name in the Analysis pane to indicate that analysis filtering is applied.

More information:

[Create a Custom Analysis](#) (see page 16)

Reserved Filter Expressions

The following filter expressions are reserved. Do not use these case-sensitive expressions in the Value field in the Add Analysis Filter dialog.

ApplicationName, ApplicationTypeID, ApplicationNameTypeID
ClientNetworkName, ClientNetwork
HostName, Host
L4Port
LogicalPortName, LogicalPort
L3ProtocolName, L3ProtocolNumber, L4ProtocolName, L4ProtocolNumber, L34ProtocolName,
L34ProtocolNumber
MAC
NetworkName, Network
PairName, Pair
ServerName, Server
SessionID, ToS, or VLAN

The analysis filtering function cannot create the query syntax when the parameters include a reserved expression and "=" or "!=". If you use a reserved expression, use a different case than the one specified in the list.

Values Associated with the Parameter Field

The following table describes the syntax for the Values field, which changes based on the item selected in the Parameter field.

Application Name

Filter for an application name. Application names in the Display area are derived from CA Application Delivery Analysis configuration or from well-known port usage. Type a name or a comma-separated list of names. Wildcards are accepted.

Examples:

Secure HTTP*
Secure HTTP (443)

Application Name/Type/ID

Filter for three values that represent an application name, type, and ID number. These values can be seen when the Application Name, Application Type, and Application ID columns are enabled in the Edit Columns dialog. Specify the trio as "name/type/ID." Example:

MySQL (3306)/Monitored/3

Note: The Application Type/ID and Application Name/Type/ID parameters require internally assigned values. Apply them directly from the data table with the right-click menu.

Application Type/ID

Filter for two values that represent an application type and its ID number. These values are available when the Application Type and Application ID columns are enabled in the Edit Columns dialog. Specify the pair as "type/ID." Example:

Monitored/10

Client Network

Filter for the IP address of a client network subnet, or a comma-separated list of subnets. Use a slash (/) to separate the mask from the address. Examples:

192.3.45.0/24
192.3.45.0/24,192.3.46.0/24,192.3.50.0/24

Client Network Name

Filter for the name of a client network, or a comma-separated list of networks that are defined for monitoring in CA Application Delivery Analysis.

Host

Filter for an IP address. The default filter parameter in any combination of the following formats:

- One IP address
- A range of IP addresses
- A comma-separated list of IP addresses
- A comma-separated list of address ranges

Use hyphens but no spaces in address ranges. Examples:

198.168.0.1, 198.165.0.1-198.165.1.255

Host Name

Filter for a client or server DNS host name. Type a DNS host name or a comma-separated list of host names. Wildcards (*) are supported. This parameter is the default. Examples:

exchangeserver1, *noc*, database*

Layer 3 Protocol Name

Filter for a Network Layer protocol. Type the name of a Layer 3 protocol, or a comma-separated list of names. Example:

IP

Layer 3 Protocol Number

Filter for a Network Layer protocol. Type the decimal registry number of a Layer 3 protocol, or a comma-separated list of registries.

Layer 3-Layer 4 Protocol Name

Filter for a pair of protocols from Layers 3 and 4. Type a pair of protocol names, or a list of pairs of names. Use a slash (/) to separate a pair. Example:

IP/TCP

Layer 3-Layer 4 Protocol Pair

Filter for a pair of protocols from Layers 3 and 4. Type a pair of protocol registry numbers, or a list of pairs of numbers. Use a slash (/) to separate a pair. Example, for IP/TCP:

2048/6

Layer 4 Port

Filter for Transport Layer port numbers. Type a port number or a comma-separated list of port numbers. Example, for HTTPS:

443

Layer 4 Protocol Name

Filter for a Transport Layer protocol. Type the name of a Layer 4 protocol, or a comma-separated list of names.

Layer 4 Protocol Number

Filter for a Transport Layer protocol. Type the decimal registry number of a Layer 4 protocol, or a comma-separated list of registries.

Logical Port

Filter for a logical port number. Type a logical port number or a comma-separated list of numbers. This parameter lets you see only the data that is mirrored from specific sources.

Logical Port Name

Filter for a logical port name that you defined on the Multi-Port Monitor appliance. Type a logical port name or a comma-separated list of names.

MAC Address

Filter for a Media Access Control address, or a comma-separated list of MAC addresses. Example:

00:19:2f:aa:bb:cc

Network Name

Filter for a CA Application Delivery Analysis network name. When you configure networks in CA Application Delivery Analysis Administration, you can provide a name for each. In this field, type a network name or a comma-separated list of names.

Network

Filter for a network subnet. Type the IP address of a network subnet, or a comma-separated list of subnets. Use a slash (/) to separate the mask from the address. Examples:

```
192.3.45.0/24
192.3.45.0/24,192.3.46.0/24,192.3.50.0/24
```

Pair

Filter for a pair of conversing hosts by IP address. Type a pair of IP addresses or a comma-separated list of pairs of IP addresses. Use a slash (/) between a pair of addresses. Example:

```
198.168.0.1/198.168.0.18
```

Pair Name

Filter for a pair of conversing hosts by DNS host name. Type a pair of host names or a comma-separated list of pairs for the value. Use a slash (/) between a pair of host names. Example:

```
MyServer1/MyClient1
```

Server

Filter for a server IP address. Type the IP address of a server, or a comma-separated list of addresses. Use dotted notation. Example:

```
192.3.45.0
```

Server Name

Filter for a server host name. Type a host name or a comma-separated list of host names.

Session ID

Filter for a TCP session ID number. Type a session ID number or a comma-separated list of ID numbers.

The session ID is an internal identifier that is available when the Session ID column is enabled in the Edit Columns dialog.

ToS

Filter for a Type of Service bit setting. Type a ToS setting, in decimal format, or a comma-separated list of settings. Example for 0100, maximize throughput:

```
4
```

VLAN Number

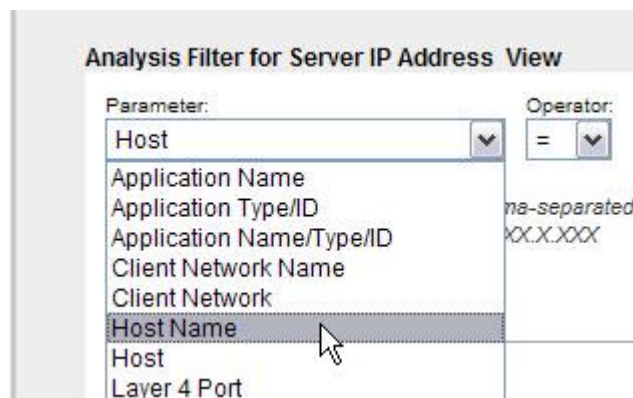
Filter for a Virtual LAN ID number. Type a VLAN ID number or a comma-separated list of numbers.

More information:

[Add or Remove Columns in a Data Table](#) (see page 48)

How Filters Query the Database

Some analysis filters are paired sets in the Add Analysis Filter dialog. For example, you can filter by Host (the IP address) or by Host Name:



These filter parameters are applied intelligently to create a useful chart. For example, select the Host parameter to filter data on the TCP tab of the Client IP Address view. The data shows only client addresses that match the filter value. Then apply the same Host filter to the Server IP Address view. The data shows only server addresses that match the value.

Some data views do not limit the display in this way. The Protocol and Application views filter by clients and servers. And the Traffic tab applies less filtering in general.


The Network data view and the Network analysis filters do not always search all networks defined in CA Application Delivery Analysis. CA Application Delivery Analysis classifies networks as either client or server networks. The classifications are based on the role these hosts play in captured transactions. The Network and Network Name filters, which match network address or name values, default to matching on client networks. However, they also issue different database queries that are based on the selected data view and tab.

- When the Network view and TCP tab are selected, only client networks are queried for matching values.
- When the Server IP view is selected, only the Network and Network Name analysis filters send queries for matching server networks.

Change the Properties of an Analysis Filter

You can modify an analysis filter that is applied to a data view. You can modify filters from the Analysis menu, using the following procedure detailed. Or you can modify a parent filter using the right-click options on the data table. Changes to a parent filter overwrite any analysis filters that are applied to child views.

Follow these steps:

1. Locate the filter that you want to change. A filter icon () identifies an active filter.
2. Right-click the filter and select Edit Analysis Filter.

The Edit Filter dialog identifies the active filters in the Conditions field. Filters that are inherited from another view in the same analysis are shown in the Inherited Analysis Filters field.

Note: Within an analysis, filter inheritance proceeds downward from a preceding view to all subsequent views in the same analysis.

3. Select a Boolean operator to add conditions in relationship to the existing filter statement.
 - AND (concatenation)
 - OR (alternation)
4. Select filters from the Parameter field. As you click each item, help with the appropriate syntax for the Value field appears.
5. Select an operator.
 - Equals (=)
 - Does Not Equal (!=)
6. Type a value to complete the expression. Use the syntax online help for guidance.

Note: Certain expressions disable the filter when supplied for the Value field. Do not use the expressions from the list of [Reserved Filter Expressions](#) (see page 25).

7. Click Add to Conditions.

The filter statement appears in the Conditions field.

Note: To remove the statement, click [Clear] above the Conditions field. You can also edit the statement by typing in the Conditions field.

8. Click OK.

The modified filter is validated. If valid, the filter is applied to the data table and chart in the Display area.

More information:


[Reserved Filter Expressions](#) (see page 25)

[Values Associated with the Parameter Field](#) (see page 25)

Delete an Analysis Filter

You can delete an analysis filter that is applied to a data view. Use the mouse pointer to hover over a filter to see the current filter conditions. You can delete one filter or all filters for an analysis.

Follow these steps:

1. Locate the filter that you want to delete. A filter icon () identifies a filter.
2. Right-click the filtered view and select Remove Analysis Filter to delete one filter.
The table and chart in the Display area are refreshed to include data that had been filtered out.
3. Right-click the name of the analysis and select Remove All Filters to delete all filters.
The table and chart in the Display area are refreshed to include data that had been filtered out.

Global Filters

Global filters are inherited from the CA Application Delivery Analysis report context that was in effect when you initiated a Session Analysis. Each global filter setting indicates the context.

A list of active global filters appears at the top of the Analysis pane. Domain, Application, Server, and Network global filters appear first, and then the Logical Port that was selected during the Session Analysis procedure.

Queries to the Multi-Port Monitor database filter the data. The queries depend on the type of filter and on the selected data view, and are selected to optimize the data that is returned.

- The Domain global filter focuses attention on the specified domain. The list of available domains is based on the domain groups that are given to the user in CA Performance Center.
- The Server global filter focuses attention on the specified server.
- The Network global filter focuses attention on clients within that network.

You can modify a global filter to limit the data that is presented in the Display area. You can also clear a global filter to return it to the default setting.

Global Filters Dialog

The Global Filters dialog provides the following information.

Domain tab

- Name. The name of the domain, if domains are defined. The list of available domains is based on the domain groups that are given to the user in CA Performance Center.

Application tab

- Name. The name of the application, if available. The port number is shown in parentheses.
- Application Type/ID. The application identifier. Usually two values that represent an application type and its ID number. Each pair identifies an application in the Multi-Port Monitor database.

Server tab

The Server tab contains a list of hosts. The role of a server in monitored transactions identifies it as a host. Multi-Port Monitor can distinguish servers and clients within the captured conversation data.

- Name. The name of the server as configured in CA Application Delivery Analysis, usually the DNS host name.
- IP Address. The IP address of the server.

Network tab

The Network tab identifies client networks. The CA Application Delivery Analysis concept of *networks* is based on monitoring client regions and observing client-server transactions from those regions.

- Name. The name of a network as defined in CA Application Delivery Analysis. A network is treated as a client region for purposes of CA Application Delivery Analysis performance monitoring.
- Subnet. The client region is based on the combination of subnet IP address and mask.

Logical Port tab

- Name. The name of the logical port that the Multi-Port Monitor Administrator defined. The default name is the same as the port number.
- Logical Port. The number of the logical port that appears on the Logical Ports page. The default logical port definition corresponds to the port ID number on the adapter.

Modify a Global Filter

You can change a global filter to restrict the data included in an analysis.

Note: If you change the Logical Ports global filter, you effectively change the entire dataset for the selected analysis.

Follow these steps:

1. Click [change] next to the global filter you want to change in the Analysis pane.
The Global Filters dialog opens.
2. Click the tab that corresponds to the global filter you want to change. For example, to filter the analysis by an application running on the monitored network, click the Application tab.
The tab displays a list of all known applications whose traffic is reflected in the captured packets from the time frame you are viewing.
3. Select an application in the list. For example, select "Simple Mail Transfer Protocol."
The selected application appears as Currently Selected. The application port number appears in parentheses. The selected application also filters the lists of items on the other tabs in the Global Filters dialog.

4. Click another tab to apply more restrictions to the data included in the analysis.

For example, click the Server tab. Only servers that are running the selected application (SMTP, in this example) are shown in the list. Select a server.

5. Click OK.

The chart and table for the current analysis are filtered to show only data from the SMTP application and its application servers.

Clear a Modification to a Global Filter

You can remove, or clear, a change you made to a global filter. By clearing a change, you return the global filter to the default setting, "All."

Follow these steps:

1. Click [change] next to the global filter you want to clear in the Analysis pane.

The Global Filters dialog opens and displays active global filters as Currently Selected.

2. Click [Clear] next to the selected filter.
3. Click another tab to see which filters are selected and then repeat step 2.
4. Click OK.

The data table and chart are refreshed to include the information that had been filtered out.

Chapter 5: Understanding the Data in the Display Area

The Display area contains a chart and a data table. The following items affect the data in the chart and table:

- Domain
- Time frame
- Global filters
- Analysis filters
- The active tab in the data table: either the TCP or Traffic tab

The chart provides a series of format buttons down the right side to let you apply other chart formats for the same data. You can expand the size of the Display area by hiding the Analysis pane. Click the Hide icon (<<) on the Analysis pane to hide it.

The chart and table are linked so that they always display data in complementary formats. The table displays more data than the chart. However, the chart reflects the filters that you apply to the table, such as changing the sort order and selecting a new page.

The data table presents performance data for troubleshooting and analysis. You can sort each column to view outliers and minimum results. Two filters always affect the data table:

- The current time frame
- The filtering parameters of the current analysis

A predefined analysis includes minimal filters and applies some logic to limit the data to a manageable quantity. This technique speeds up database queries and also makes the Display area more coherent for the typical user.

Data from the first ten table rows is represented in the chart for all but the Summary Trend chart. The Summary Trend chart reflects data from all table rows. You can display more table rows by increasing the Max Per Page setting.

This section contains the following topics:

[Types of Charts](#) (see page 36)

[Types of Data](#) (see page 39)

Types of Charts

The chart in the Display area is refreshed in the following circumstances:

- You initiate a Session Analysis from a CA Application Delivery Analysis report.
- You click a data view in the Analysis pane.
- You select a column in the data table in the Display area.
- You drill down from a CA APM defect.

The chart and table offer mutually supported filtering options. When you click a column heading in the data table, the table is refreshed to sort all the available rows by the selected item. The chart is refreshed to display the selected item.

When you click the TCP or Traffic tab, the data in the chart automatically changes accordingly. Most charts are restricted to the top ten entries. One exception is the Summary Trend chart, which conforms to CA Application Delivery Analysis conventions and includes data from the entire data table.

Each trend chart lets you select the time frame and zoom options.

Bar Chart

The Bar chart format presents data averages from across the selected time period. Each bar shows the data in a row in a table. The Y-axis identifies each table row. A maximum of ten rows can be included in a single Bar chart. The Y-axis label indicates the columns that identify the row. For example, the Y-axis shows each corresponding server name for the Server IP Address view. The X-axis usually displays the metric values and their units.

This type of chart format is most useful for comparing performance metrics from different entities. For example:

- Compare the server response time of one server to another server.
- Compare the TCP Byte Rate of the top ten applications.

Each part of the bar provides flyover text to identify a metric and its value. This feature is useful for understanding which component metric contributed the most to the total. Click a bar in the chart to highlight the corresponding row in the data table. You can then right-click the table row and select Apply as Filter to view data that is associated solely with the selected entity.

Important: Certain metrics are shown as a single value, such as Server Response Time. Other metrics are shown in a composite format, such as Transaction Time. A composite chart displays as selected metric as a portion of the whole metric. The composite Bar chart shows a breakdown of a single value to its units.

Line Trend Chart

In the Line Trend chart format, a line represents data from each row in the data table. The line plots the selected metric across the time period. Up to ten data rows are plotted per chart. The Y-axis identifies buckets of metric values, such as Server Response Time (SRT) in milliseconds. The X-axis displays time units to indicate trends.

This type of chart format provides a quick overview of system status and trends. For example:

- You can access the Server IP Address view to compare server response time trends and drill down into a spike in SRT.
- You can filter on one IP address to find the source of gradually increasing transaction times.

Pie Chart

The Pie chart format represents the top ten entries for a selected metric as pieces of a pie. Each piece is a percentage of a whole. All pieces add up to 100 percent of the selected metric total for the top 10 table entries. Each pie piece represents a row in the data table.

Note: Certain metrics, such as TCP Byte Loss Percentage, are inappropriate for display in the Pie chart format.

The top 10 entries do not always account for 100 percent of all activity observed during the selected time period. You can enable an eleventh pie piece to represent an aggregate of the rest of all the table rows (Other). Flyover text for each pie piece identifies the hosts. Click a pie piece to highlight the associated hosts in the data table. You can then filter by that data. Drill-in to the “Other” piece is not supported.

This type of chart format is most useful for comparing the relative contributions of hosts to a selected metric. For example, filter on a particular server and select the Server/Client Pair view. Then select the TCP Bytes metric and see which clients contribute most to the data volume of a server.

Stacked Trend Chart

The concept behind the Stacked Trend chart is similar to that of the Pie chart, except that the values are plotted over time. One line of a different color is displayed per table row. Up to ten rows are plotted per chart. The lines are filled and stacked, with the highest table row plotted on the bottom of the chart. A downward fill below each line helps you see how each region of data is related to the others and to the larger metric.

A thick line labeled "Total" identifies where 100 percent of the plotted metric falls along the Y-axis. To remove this line from the chart, click the Hide link next to the legend.

This type of chart is most useful for comparing the relative contributions of selected entities to a performance metric over time. For example, filter on a particular server and select the Server/Client Pair view. A Stacked Trend chart for the TCP Bytes metric indicates whether data volumes from different clients are changing over time.

The Stacked Trend chart is not applicable for certain types of metrics, such as TCP Byte Loss Percentage.

Summary Trend Chart

The Summary Trend chart uses a stacked format to display the data points from all table rows and all pages in the data table. The chart displays a layered view of the values for a selected metric. Each value equals the vertical distance between the upper and lower metric boundary lines, not the distance from 0 to the upper boundary line.

This chart format resembles the Stacked Trend chart, with the following differences:

- The Stacked Trend chart displays a single metric, representing a single column in the data table, for only the current page of the data table.
- The Summary Trend chart displays multiple metrics from all rows and table columns, with values averaged across all columns.

The stacked format is useful for showing composite data. The value for each metric is treated as a portion of the whole metric. Each data point shows a breakdown of a single metric into its component parts.

Lines of different colors show the data points that compose an overarching value, such as the components of TCP transaction response time: network round-trip time, server response time, and data transfer time.

To represent the trends in the plotted metrics, the chart is plotted over the selected time period, with time values shown on the X-axis.

Types of Data

The data table consists of two tabbed views that provide different perspectives on captured data from the same time frame. Each view provides different metrics and applies filters in different ways.

TCP tab

The TCP tab contains data specific to TCP-based applications and metrics for CA Application Delivery Analysis reports. The tab also contains performance metrics that are calculated from the captured packets. The label on the Name column changes to indicate whether clients or servers are displayed.

Note: The TCP tab is selected by default when you drill down from CA Application Delivery Analysis. In general, the format of the data on the TCP tab closely resembles the format of data in CA Application Delivery Analysis reports.

Traffic tab

The Traffic tab contains all other available data, not restricted to TCP applications. The Traffic tab does not apply a concept of client or server. Therefore, the Name column can show the names of both clients and servers, depending on the selected view. The Traffic tab also includes non-TCP traffic, which can result in the inclusion of more hosts.

The names of some performance metrics are abbreviated in the data table to reduce the width of the table. To see the full name of a metric, position the mouse pointer over the abbreviated column name or its check box. The flyover text provides the full name of the selected metric.

Data on the Traffic Tab

The Traffic tab of the data table provides a comprehensive view of the packets passing through the monitored mirror ports. Only the columns applicable to the selected view are shown in the table. The following list describes all possible columns for the Traffic tab.

Application

Application names are derived from CA Application Delivery Analysis configuration or from well-known port usage. Where available, the application name is supplied. Otherwise, the port number is shown in parentheses.

Application ID

The second value in a pair of values that identifies an application. An internal identifier.

Application Type

Identifies an application in the Multi-Port Monitor database. In most cases, conveys the state of this application as it pertains to CA Application Delivery Analysis. One of the following types:

- **n/a:** Unknown protocol.
- **Monitored:** Application uses TCP. CA Application Delivery Analysis monitors this application.

If multiple collection devices report to one CA Application Delivery Analysis management console, it is possible that a different collection device monitors this application for CA Application Delivery Analysis. The Application Type designation refers to items that only this Multi-Port Monitor actively monitors.

- **UDP-Not monitored:** Application is defined in CA Application Delivery Analysis, but uses UDP. CA Application Delivery Analysis does not monitor UDP.
- **TCP-Not monitored:** Application is defined in CA Application Delivery Analysis and uses TCP. However, CA Application Delivery Analysis is not monitoring the application.
- **TCP-Unknown:** Application uses TCP, but is not defined in CA Application Delivery Analysis. Application column shows "Port X."
- **UDP-Unknown:** Application uses UDP, which CA Application Delivery Analysis does not monitor. Application is not defined in CA Application Delivery Analysis or in the Multi-Port Monitor list of well-known UDP ports. Application column shows "Port X."

Byte Rate

Server processing efficiency that is measured in bits per second (bytes per second x 8). This throughput value is significant for capacity planning, because it provides a sense of server load or usage.

Byte Rate From, Byte Rate To

Throughput in bits per second (bytes per second x 8) for the data that the selected host sent or received.

Bytes

Data volume in bytes. The total number of Application-Layer bytes sent and received during the selected time period and selected client-server sessions.

Bytes From, Bytes To

Data volume in bytes. The total number of Application-Layer bytes that the selected host sent or received during the selected time period.

IP Address, IP Address 1, IP Address 2

The IP address of the host. The "1" or "2" designation appears for the paired data views and indicates the direction of data flow between hosts.

Layer 3 Protocol

The name of the Network Layer protocol (IP or ARP), or an ID number from the Ethertype field in the packet header. Indicates "Ethertype=X" when an IEEE 802 Ethertype value is found.

Layer 3 Protocol Number

The decimal registry number of a Network Layer protocol, such as 2048 for IPv4.

Layer 4 Protocol

The name of the Transport Layer protocol, such as TCP.

Layer 4 Protocol Number

The decimal registry number of a Transport Layer protocol, such as 6 for TCP.

Logical Port, Logical Port Number

The logical port and port number on the Multi-Port Monitor appliance that is the source of the data in the table.

MAC Address, MAC Address 1, MAC Address 2, IP Address MAC

The Media Access Control address of the server that had the assigned IP address indicated during the selected session. The "1" or "2" designation appears for the paired data views and indicates the direction of data flow between hosts.

Name, Name 1 or 2, Server Name, Client Name

The name of the host, either a client or a server. For some views, a Client or Server designation is indicated. For other views, hosts are shown without regard to their client or server role. The "1" or "2" designation appears for the paired data views and indicates the direction of data flow between hosts.

Network Name, Network Name 1, Network Name 2

The name of a network as it is defined for monitoring in ADA. The "1" or "2" designation appears for the paired data views and indicates the direction of data flow between networks.

Network Subnet, Network Subnet 1, Network Subnet 2

The IP address of a network subnet. The "1" or "2" designation appears for the paired data views and indicates the direction of data flow between subnets.

Packet Rate

Server processing efficiency that is measured in packets per second. This throughput value is significant for capacity planning, because it provides a sense of server load or usage.

Packet Rate From, Packet Rate To

Throughput in packets per second for the data that the selected host sent or received.

Packets

Data volume in packets. The total number of packets that were sent and received during the selected time period and selected client-server session.

Packets From, Packets To

Data volume. Total number of packets that the selected host sent or received.

Port 1, Port 2

The port on the host that sent or received data that is related to conversations or sessions.

Session ID

The ID number of the TCP session. An internal identifier.

ToS

The bit setting for the Type of Service field in the IPv4 header.

ToS Description

A standard description of the TOS setting, such as "Default Traffic" or "Max throughput."

TCP Bytes

TCP data volume in bytes. The total number of TCP bytes sent and received during the selected time period by the selected host or pair of hosts.

TCP Packets

TCP data volume in packets. The total number of TCP packets that the selected host (or pair of hosts) sent and received during the selected time period.

VLAN

The ID number of the Virtual Local Area Network.

Data on the TCP Tab

The TCP tab of the data table excludes non-TCP packets and displays the data that CA Application Delivery Analysis and CA APM monitor from all Multi-Port Monitor logical ports. Only the columns applicable to the selected view are shown in the table. The following list describes all possible columns for the TCP tab.

Application

Application names are derived from CA Application Delivery Analysis configuration or from well-known port usage. Where available, the application name is supplied. Otherwise, the port number is shown in parentheses.

Application ID

The second value in a pair of values that identifies an application. An internal identifier.

Application Type

Identifies an application in the Multi-Port Monitor database. In most cases, conveys the state of this application as it pertains to CA Application Delivery Analysis. One of the following types:

- **n/a**: Unknown protocol.
- **Monitored**: Application uses TCP. CA Application Delivery Analysis monitors this application.

If multiple collection devices report to one CA Application Delivery Analysis management console, it is possible that a different collection device monitors this application for CA Application Delivery Analysis. The Application Type designation refers to items that only this Multi-Port Monitor actively monitors.
- **UDP-Not monitored**: Application is defined in CA Application Delivery Analysis, but uses UDP. CA Application Delivery Analysis does not monitor UDP.
- **TCP-Not monitored**: Application is defined in CA Application Delivery Analysis and uses TCP. However, CA Application Delivery Analysis is not monitoring the application.
- **TCP-Unknown**: Application uses TCP, but is not defined in CA Application Delivery Analysis. Application column shows "Port X."
- **UDP-Unknown**: Application uses UDP, which CA Application Delivery Analysis does not monitor. Application is not defined in CA Application Delivery Analysis or in the Multi-Port Monitor list of well-known UDP ports. Application column shows "Port X."

Client IP Address

The IP address of the client computer in the client-server session.

Client Name

The host name of the client computer in the client-server session (a conversation pair).

Client Port

The port on the client that sent or received the data.

CT Obs

Connection Time Observations. The number of monitored TCP connections occurring during the selected time interval. A good indication of usage levels and a gauge of metric significance. For example, many observations can indicate an event that can affect users.

DTT

Data Transfer Time. Elapsed time between when the server starts responding and when it finishes sending data. Several factors affect this value, such as response size, available bandwidth, and interaction between the application and the network. Excludes the initial server response time and includes only NRTT if there is more data to send than fits in the TCP window. This value is related to the number of network round trips required to deliver all data and the delay per round trip.

ENRTT

Effective Network Round-Trip Time. Includes NRTT and Retransmission Delay, which is the delay that retransmissions cause for a transaction. Reflects the latency that users actually experience and serves as an indicator of the performance degradation that retransmissions cause.

Layer 3 Protocol

The name of the Network Layer protocol (IP or ARP), or an ID number from the Ethertype field in the packet header. Indicates "Ethertype=X" when an IEEE 802 Ethertype value is found.

Layer 3 Protocol Number

The decimal registry number of a Network Layer protocol, such as 2048 for IPv4.

Layer 4 Protocol

The name of the Transport Layer protocol, such as TCP.

Layer 4 Protocol Number

The decimal registry number of a Transport Layer protocol, such as 6 for TCP.

Logical Port, Logical Port Number

The logical port and port number on the Multi-Port Monitor appliance that is the source of the data in the table.

NCT

Network Connection Time. The amount of time that it takes the client to confirm the server connection acknowledgment. In general, network latency causes delay in connection times. NCT serves as a baseline for carrier latency and comparison to NRTT values.

NRTT

Network Round-Trip Time. The amount of time it takes for a packet to travel to and from the server and clients on a network, excluding latency from retransmissions. Application and server processing times are excluded from this value. This value is often useful when compared to the NCT value.

Retrans

Retransmission Delay. The additional delay in the NRTT that retransmission cause. Retransmissions are packets that are retransmitted after data loss. The data is expressed as an average across all observations, not the actual retransmission time for each transaction. The NRTT value increases when Retransmission Delay causes a delay in client acknowledgment. This metric does not reveal the impact of losses on the DTT because of TCP congestion. This metric reflects only data loss from the server to the clients, not from clients to the server.

SCT

Server Connection Time. The amount of time from when the server receives the SYN packet from the client until the server sends the first SYN/ACK.

Opening a TCP connection involves exchanging three packets: SYN, SYN/ACK, and ACK. The TCP header has SYN (synchronize) and ACK (acknowledge) bits. The first packet has the SYN bit set. The second packet has both bits set. The third packet has only the ACK bit set. This exchange establishes the initial sequence numbers of the connection.

SCT and NCT comprise the Connection Setup Time metric.

Server IP Address

The IP address of the server in the client-server session.

Server MAC, Client MAC

The unique Media Access Control address that identifies a host.

Server Name

The host name of the server in the client-server session (a conversation pair).

Server Network Name, Client Network Name

The name of a network as it is defined for monitoring in CA Application Delivery Analysis. The “Client” or “Server” designation appears for the paired data views and indicates the direction of data flow between networks.

Server Network Subnet, Client Network Subnet

The IP address of a network subnet. The “Client” or “Server” designation appears for the paired data views and indicates the direction of data flow between subnets.

Server Port

The port on the server that sent or received the data.

SRT

Server Response Time. The amount of time a server takes to respond to a client request. Server speed, application design, and volume of requests affect SRT.

TCP Byte Loss

Data loss, expressed as a percentage of TCP bytes sent and received.

TCP Byte Rate From, TCP Byte Rate To

TCP throughput in bits. The data rate in bits per second (bytes per second x 8) between the selected server and clients during the selected time period.

TCP Byte Rate Retransmtd

Ratio of retransmitted data to total data, percentage of data that was lost on the monitored network, and loss rate in bits per second.

TCP Bytes

TCP data volume in bytes. The total number of Application-Layer bytes seen on the network during the selected time period.

TCP Bytes From, TCP Bytes To

TCP data volume in bytes. Total number of Application-Layer bytes that the selected server sent to or received from clients during the selected time period.

TCP Packet Loss

Data loss, expressed as a percentage of TCP packets that were sent and received.

TCP Packet Rate

TCP throughput in packets. The data rate in packets per second during the selected time period. ADA reports use the term Data Rate.

TCP Packet Rate From, TCP Packet Rate To

TCP throughput in packets. The data rate in packets per second from the selected server to clients, or from clients to the server, during the selected time period.

TCP Packet Rate Retransmtd

Ratio of retransmitted data to total data, percentage of data that was lost on the monitored network, and loss rate in packets per second.

TCP Packets

TCP data volume in packets. The total number of packets on the network during the selected time period. Includes zero-byte packets, such as TCP acknowledgments.

TCP Packets From, TCP Packets To

TCP throughput in bits. The data rate (bytes per second x 8) during the selected time period. CA Application Delivery Analysis reports use the term Data Rate.

TCP Retransmtd Bytes

The number of TCP bytes that were retransmitted due to data loss.

TCP Retransmtd Packets

The number of TCP packets that were retransmitted due to data loss.

ToS

The bit setting for the Type of Service field in the IPv4 header.

ToS Description

A standard description of the TOS setting, such as "Default Traffic" or "Max throughput."

Transaction Time

The amount of time from the moment a client sends the request (packet-level or transaction-level) to the moment the client receives the last packet in the response.

Transaction Time Obs

Transaction Time Observations. The number of monitored TCP transactions that occurred during the selected interval. A good indication of usage levels and a gauge of metric significance. For example, many observations can indicate an event that can affect many users.

VLAN

The ID number of the Virtual Local Area Network.

Byte Counts for Networks and Hosts

The TCP tab shows activity from the client network perspective. The Traffic tab shows generic network activity, without regard to which conversing host is the client and which the server. If a pair of hosts in the same subnet exchanges data, the byte counts for the same conversation can be different on each tab.

On the Traffic tab, byte totals for conversations within the same subnet can appear to be double the totals on the TCP tab. The total bytes exchanged between the *two hosts* are tallied as they exit the network *and* as they reenter it. Both directions are included in the total, rather than broken out per host.

On the TCP tab, which reflects the client perspective, the bytes that *one host* sent and received are tallied for the same time period. The result is a total bytes value that is smaller than the total bytes value on the Traffic tab.

Add or Remove Columns in a Data Table

By default, some data is excluded from the data table on the Traffic and TCP tabs. You can include more columns of data.

Follow these steps:

1. Click Edit Columns.
The Edit Columns dialog opens.
2. Select the check boxes for the metrics you want to add to the data table.
3. Clear the check boxes for the metrics you want to remove from the data table.
4. Click Default to restore default column settings.
5. Click Save.

Your changes are reflected in the data table after it refreshes.

Chapter 6: Exporting Data

This section contains the following topics:

[Export Data to a PDF File](#) (see page 49)

[Export Data to a CSV File](#) (see page 50)

[Export Data to a PCAP File](#) (see page 51)

[Share Data by Email](#) (see page 52)

Export Data to a PDF File

The charts in analyses can be shared in PDF format, with the following limitations:

- The data table is not exported.
- Legends that explain the colors in a chart are not exported. Therefore, for the Line Trend and Stacked Trend chart formats, send the view as a link by email.

All filters that are applied to the current chart are preserved in the exported analysis.

Follow these steps:

1. Display the data that you want to export:
 - a. Click a data view in the Analysis pane.
 - b. Apply more filters or sort the data table by a selected column.
2. Click Export, To PDF.

The File Download dialog opens.
3. Select whether to open or save the file.
 - When you click Open, the PDF is displayed in the Acrobat Reader application.
 - When you click Save, use the Save As dialog to browse to the file save location and click Save.

The current chart is exported to a file with a .pdf file extension. A label identifies the data view, the active filters, the time frame of the data, and the time when the PDF was generated.

Export Data to a CSV File

You can export the data table in an analysis to a spreadsheet in comma-separated values (.csv) format. All filters that are applied to the data table are preserved in the exported analysis.

As a best practice, select a precise segment of data to limit the size of the spreadsheet:

- Apply hardware filters to the logical ports you defined.
- Apply filters to the data views you selected.
- Select a relatively small time period using the Time Period selector.

Follow these steps:

1. Display the data that you want to export:
 - a. Click a data view in the Analysis pane.
 - b. Apply more filters or sort the data table by a selected column.
2. Click Export, To CSV.

The Export To CSV dialog opens.
3. (*Optional*) Type the maximum number of data table rows to export in the Export Row Limit field. Or, select No Limit to export all rows in the data table from the selected time period.
4. Click OK.

The File Download dialog opens.
5. For fastest download times, click Save.

Note: We do not recommend the option to open the file. The download takes longer when you select this option while attempting to export a large amount of data.

6. Enter or browse to the file save location, and click OK.

The selected details are exported to a file with a .csv file extension. The process can take a few minutes to complete, depending on the amount of data available in the database and the row limit you supplied.

Export Data to a PCAP File

You can export the packet-capture data for the current view to a packet-capture file, in PCAP format. The packet-capture file is built from raw capture files and displays packets for all sessions included in the current analysis.

The PCAP format is widely used for network trace files and other methods of examining and exchanging packet-level data. PCAP is compatible with WinPcap (Windows) and libpcap (UNIX). Applications that use these application programming interfaces easily read and display PCAP.

The administrator and a user with rights for the CA Application Delivery Analysis Investigations role can use the Export to PCAP feature. By default, only the IT Engineer and IT Manager roles allow access to this feature.

Tips:

- PCAP file exports can take a while to complete. The amount of time necessary to open the File Download dialog depends on the amount of data being exported.
- Narrow the time frame of the analysis to improve the performance of the Export to PCAP feature. A narrower time frame reduces the number of raw capture files that are searched for relevant packets. Use the Time Period selector or the chart time control to zoom in on the time frame of interest.
- The ability to export to PCAP is not available when the raw capture files containing the data of interest are deleted. Capture files are not retained as long as the metric data in the metrics database.
- The "Header Only" option for the "Maximum Bytes per Packet" parameter applies to IPv4 (TCP and UDP) headers, including extension headers. If you select "Header Only" when you export non-IP traffic, you receive only the Layer 2 MAC headers. Instead, select a byte value, such as 128, to see more of each frame.
- Session-level performance data is available only for the IPv4-based port mirror data that is received on the Multi-Port Monitor logical ports.
- The PCAP files can be viewed in a protocol analyzer, or *packet sniffer*, such as the freeware tool Wireshark. Protocol analyzers observe data flows passing across the network and inspect copies of each packet. They display the contents of each field in the packet header in a graphical user interface, where data can be filtered, sorted, and analyzed.
- A protocol analyzer is a valuable tool for troubleshooting or analyzing the data that Multi-Port Monitor captures. Use of a protocol analyzer requires an understanding of Ethernet, IP, and Layer 4 protocol packet structures.

Follow these steps:

1. Display the data that you want to export:
 - a. Click a data view in the Analysis pane.
 - b. Apply more filters or sort the data table by a selected column.
2. Click Export, To PCAP.

The Export To PCAP dialog displays the time range of the packet trace to export.
3. Select the port that received the data that you want to export in the Logical Port field. The number of sessions and the traffic volume in bytes are shown for each available port. These statistics are based on the current filters, such as the time frame and the view. They are not an indication of the size of the file you want to export.

Select only one port for each exported PCAP file.
4. Select the maximum number of bytes to include from each packet in the Maximum Bytes per Packet field. The default option is to include only headers in the PCAP file.
5. Click OK.

The Save As dialog opens.
6. Select a location in which to save the exported PCAP file.
7. Click Save.

Share Data by Email

Sending a link to an analysis is often the quickest way to share data. The Email option constructs a URL from an analysis and uses the default mail client to create an email message.

Restrictions

- An email client is required. To use the email feature, install an email client and configure an SMTP server on the computers where users access the web interface.
- The recipient must have a user account with permission to view the Analysis page.
- The recipient must view the analysis within a few days, before the underlying data is purged from the database.

Follow these steps:

1. Display the data that you want to export:
 - a. Click a data view in the Analysis pane.
 - b. Apply more filters or sort the data table by a selected column.

2. Click Email.

A blank message opens in your messaging application. The URL appears in the body of the message. The date and time appear in the Subject line. The date and time represent the moment when the email message is generated, not the time frame of the analysis. The time frame of the analysis is shown in the Display area of the Analysis page.

3. Type a recipient address and click Send.

The email that is sent to the recipient contains a link to the URL for the analysis.

Appendix A: 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.

Appendix B: 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:

```
Conditions:
(((mIPSrcAddr==[192.168.32.15] AND mIPDestAddr!= [10.10.21.10]) OR (mIPSrcAddr==
[10.10.21.10] AND mIPDestAddr!= [192.168.32.15])) OR (mIPSrcAddr= [192.168.32.15],
{10.10.21.10}))
```

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 "!=".

Index

A

analysis

- create • 16
- data views • 18
- delete • 17
- duplicate • 17
- global filters • 31
- predefined • 14

analysis filters

- apply to data view • 23
- change • 30
- delete • 31

appliance

- Linux commands • 55

application metrics, defined • 39, 43

B

Boolean operator • 23, 30

byte rate metrics, defined • 39, 48

C

capture files

- export to PCAP • 51

chart types

- bar • 36
- line • 37
- pie • 37
- stacked • 38
- summary • 38

client metrics, defined • 43

components, description • 7

connection time observations, defined • 43

CSV, exporting data to • 50

CT Obs, defined • 43

D

data table

- add or remove columns • 48
- description • 39
- TCP tab • 43
- Traffic tab • 39

data transfer time, defined • 43

data views

description • 18

filter • 23

database

shut down • 55

display area

charts • 36

data tables • 39

DTT • 43

E

email, sharing data by • 52

ENRTT • 43

export data

in email • 52

to CSV • 50

to PCAP • 51

to PDF • 49

F

filters

analysis • 23

global • 31

regular expression syntax • 57

G

global filters

change • 33

description • 31, 32

remove • 34

L

layer 3 and 4 protocol metrics, defined • 39, 43

Linux commands • 55

logical ports

metrics • 39, 43

M

MAC address metrics, defined • 39

N

NCT • 43

network metrics, defined • 39, 43, 48

nqmaintd process • 55

NRTT • 43

P

packet rate metrics, defined • 39

PCAP, exporting data to • 51

PDF, exporting data to • 49

processes

- stop or start • 55

R

regular expression syntax • 57

retransmission delay, defined • 43

S

SCT • 43

server metrics, defined • 43

session analysis, examples of • 31, 36

shut down appliance • 55

SRT • 43

T

TCP metrics, defined • 39, 43

TCP tab

- add or remove columns • 48

- data • 43

- filters • 31

ToS metrics, defined • 39, 43

Traffic tab

- add or remove columns • 48

- data • 39

- filters • 31

transaction time metrics, defined • 43

V

VLAN

- filters • 25

- metrics defined • 39, 43