Configuration Utility User Guide

CA Application Delivery Analysis

10.2

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 © 2015 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Application Delivery Analysis
- Network Instruments® (NI) GigaStor
- CA [assign itcm product name for the adsm variable]
- Network Instruments® (NI) Observer Expert
- CA Multi-Port Monitor
- CA Performance Center
- CA NetQoS Performance Center
- CA Standard Monitor
- CA Virtual Systems Monitor

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: Overview 7

Where to Run the Configuration Utility 7
Switch Port Mirroring Requirements 8
Packet Capture File Requirements 8
Start the Configuration Utility 9
Status Information 10

Chapter 2: Finding Traffic of Interest 11

Understand the List 12
    Refresh the List 13
    Hide Entries that are Already Defined 14
    Filter Criteria 15
Filter Applications 16
Filter Networks 17
Filter Servers 19
Define a Server 20
Define a Network 21

Chapter 3: Maintain Your Configuration 23

Chapter 4: Troubleshooting 25

Chapter 1: Overview

The Configuration Utility identifies TCP sessions mirrored to a monitoring device. Typically, this information is most useful when you are not sure of the traffic that is flowing across your network. Find the traffic of interest, for example, by categories:

- Server subnet
- Server VLAN
- Client network

When you find the traffic you want, export the server and network definitions to the CA ADA console and begin monitoring the traffic. The Configuration Utility does not create user-defined applications.

Where to Run the Configuration Utility

The CA ADA setup program installs the Configuration Utility, ConfigurationUtility.exe, in the <ADA_HOME>\bin folder. Depending on where the traffic is monitored, the location where you run the Configuration Utility varies. When monitoring from the:

Management Console

Run the Configuration Utility on the management console.

Standard Monitor

Run the Configuration Utility on the Standard Monitor.

Multi-Port Monitor

Run the Configuration Utility on the management console.

A large volume of traffic may be sent from the Multi-Port Monitor to the Configuration Utility, so the two computers should be located as close to each other as possible.

Cisco NAM

Open a packet capture file from the Cisco NAM on the management console.

GigaStor

Open a packet capture file from the GigaStor on the management console.

Switch Port Mirroring Requirements

To detect the application port traffic between a server and a client, the Configuration Utility must be able to see the SYN-ACK packet. The SYN-ACK packet, which acknowledges a client request, is sent from the server side of a TCP session. The Configuration Utility must see a SYN-ACK packet to display the corresponding TCP session data in its Application, Server, and Network lists.

If the Configuration Utility only shows server side traffic, for example, Bytes from Server but not Bytes to Server, you may have asymmetric routing. *Asymmetric routing* occurs when one direction of the TCP session is not flowing through the port you are mirroring. To properly monitor TCP response times for the application, you may need to mirror more source ports to the monitoring device, possibly from a redundant switch that sees the client side of the TCP session.

Packet Capture File Requirements

To configure data collection on a Cisco NAM or NI GigaStor, the Configuration Utility requires that you load network, server, and application data from a packet capture file taken on the monitoring device. When working with packet capture files:

- The Configuration Utility requires the packet capture file to be in the NA (DOS) format. The BNF format is not supported. Using any utility that converts capture file formats, save the file with the NA Sniffer (DOS) format.
- To prevent conflicts with the CA ADA packet driver, do not install packet capture utilities, such as *WireShark*, on the CA ADA management console or standard monitor.

To prepare a packet capture file **Follow these steps:**:

1. On the Cisco NAM or NI GigaStor, take a packet capture, save the results to a file, and download the file to your local computer.

   If you are taking a packet capture on a NI GigaStor, you can create a filter rule for SYN and SYN-ACK packets to capture server based communication only by using NI Observer Expert. For more information about using NI Observer Expert, see the NI Observer Expert help.

2. Using any utility that converts capture file formats, open the packet capture file and then save the file with the NA Sniffer (DOS) format.
3. To verify that the capture file is in NA Sniffer (DOS) format, check that the first line of the file begins with TRSNIFF data. From a command prompt, type the following command and press Enter:
   `type [set the File Name variable].cap | more`
4. Copy the packet capture file, in NA Sniffer (DOS) format, to the computer where you plan to run the Configuration Utility.

Start the Configuration Utility

Before you start the Configuration Utility, keep in mind:

- When you start the Configuration Utility, data collection temporarily stops on the monitoring device. For example, when you run the Configuration Utility for an hour on a Standard Monitor, there is a one hour gap in the data collected by that monitoring device.
- To load a packet capture file, the Configuration Utility requires the packet capture file to be in the NA (DOS) format.
- Close the Configuration Utility when you are not using it to reduce resource consumption.

Follow these steps:

1. On the management console or CA Standard Monitor computer, browse to the <ADA_HOME>\bin folder and double-click ConfigurationUtility.exe.

   The Configuration Utility login screen automatically detects the IP address for the management console.

2. If you are configuring data collection on a CA Standard Monitor:

   a. The IP address of the management console and the CA Standard Monitor populate automatically.

   b. If the monitor is configured with multiple NICs, for example, to monitor asymmetric traffic, select the All Adapters checkbox to see traffic on all NICs. This option is not applicable to the CA Multi-Port Monitor.

   c. Click Start Detection.

3. If you are configuring data collection for a CA Multi-Port Monitor:

   a. In the Console field, validate the IP address of the management console.

   b. In the Collector IP field, specify the IP address of the CA Multi-Port Monitor.

   c. Click Start Detection.

   d. Select the logical port you want to configure, and click OK.

4. If you are configuring data collection for a Cisco NAM or NI GigaStor, validate the IP address of the management console and load the packet capture file taken from the device:

   a. Click Load Capture File.

   b. In the Browse dialog box, specify the location of the packet capture file, in NA Sniffer (DOS) format, and click OK.

   c. In the Configuration Utility login screen, click Process File.

5. The Configuration Utility alerts you before it temporarily disables data collection on the monitoring device.

6. Click OK.
7. In the Configuration Utility, click the Refresh menu to display the detected networks, servers, and applications. The Configuration Utility does not automatically refresh the list.
8. You are now ready to find the traffic of interest.

More information:

Packet Capture File Requirements (see page 8)
Where to Run the Configuration Utility (see page 7)

Status Information

The status bar at the bottom of the Configuration Utility provides useful information. A status of:

Connected

Indicates whether or not the utility is connected and to which management console.

Listening

Indicates the IP of the local adapter being monitored.

Detected Combinations and Packets

(SPAN data only) Indicates the current number of observed client, server, and port combinations. This information is useful when you want to determine that the monitor is seeing SPAN data. When reading a packet capture file, the combination count does not change.

Now

Indicates the current time.

Last Refresh

Indicates the last time a refresh occurred, updating the display with accumulated data.

Started

Indicates the last time the utility was started or restarted.

Chapter 2: Finding Traffic of Interest

Find the traffic of interest by filtering the list of applications, servers, and networks to find related entries. For example, filtering by:

Application

Displays related servers and networks.

Server

Displays related applications and client networks.

Network

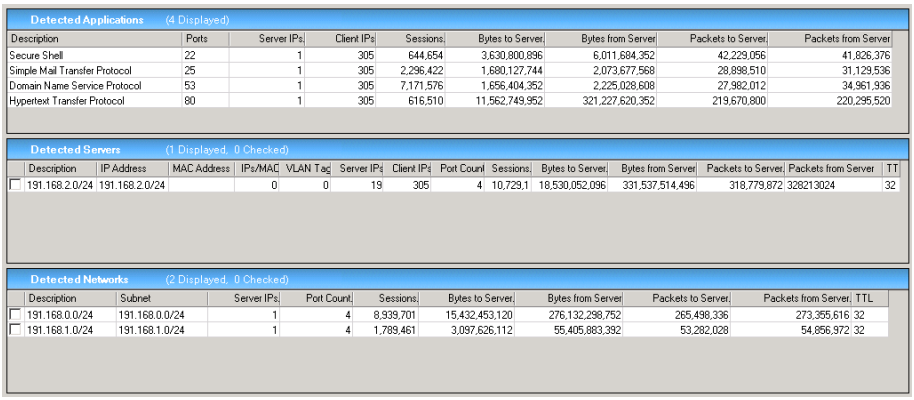
Displays related servers and applications.

Understand the List

Click Refresh to display the currently detected networks, servers, and applications. The Configuration Utility does not automatically refresh the list.

The color-coded list of entries indicates the status of the application, server, and network entries. In the example below, the traffic is not monitored by CA ADA.

Important! If the Bytes From or Bytes To column is 0, this can indicate a problem with how the TCP packets are mirrored from the switch port.



Detected Applications (4 Displayed)

Description	Ports	Server IPs	Client IPs	Sessions	Bytes to Server	Bytes from Server	Packets to Server	Packets from Server
Secure Shell	22	1	305	644,654	3,630,800,896	6,011,684,352	42,229,056	41,826,376
Simple Mail Transfer Protocol	25	1	305	2,296,422	1,680,127,744	2,073,677,568	28,898,510	31,129,536
Domain Name Service Protocol	53	1	305	7,171,576	1,656,404,352	2,225,028,608	27,982,012	34,961,936
Hypertext Transfer Protocol	80	1	305	616,510	11,562,749,952	321,227,620,352	219,670,800	220,295,520

Detected Servers (1 Displayed, 0 Checked)

Description	IP Address	MAC Address	IPs/MAC	VLAN Tag	Server IPs	Client IPs	Port Count	Sessions	Bytes to Server	Bytes from Server	Packets to Server	Packets from Server	TT
191.168.2.0/24	191.168.2.0/24		0	0	19	305	4	10,729,1	18,530,052,096	331,537,514,496	318,779,872	326213024	32

Detected Networks (2 Displayed, 0 Checked)

Description	Subnet	Server IPs	Port Count	Sessions	Bytes to Server	Bytes from Server	Packets to Server	Packets from Server	TTL
191.168.0.0/24	191.168.0.0/24	1	4	8,939,701	15,432,453,120	276,132,298,752	265,498,336	273,355,616	32
191.168.1.0/24	191.168.1.0/24	1	4	1,789,461	3,097,626,112	55,405,883,392	53,282,028	54,856,972	32

A status of:

Unconfigured (black)

Indicates that the Configuration Utility detects the entry on the monitoring device or packet capture file, but there is no definition for the entry in the Configuration Utility or the management console. Use the Configuration Utility to configure a definition for the entry.

Configured in the Management Console (green)

Indicates that a definition for the entry exists in CA ADA. To edit the server or network definition, use the CA ADA management console.

Configured in the Configuration Utility (blue)

Indicates that a definition for the entry exists in the Configuration Utility but not in the management console. Use the Configuration Utility to edit the definition for the entry.

Note that if an unconfigured server communicates on the same port as a configured (green) application, the application port appears twice, both as a configured (green) and unconfigured (black) entry. Sort the list of Detected Applications by Port to find any duplicate port entries.

Refresh the List

The Configuration Utility reports mirrored traffic from a switch port, however, you must manually refresh the list to display the current status.

If an application, server, or network disappears or its volume decreases, this is likely caused by one or more servers crossing the Maximum IPs/MAC threshold. Statistics from those servers are not counted towards their associated application and network counterparts, which can cause the totals to decrease or disappear entirely if reduced to zero. Turning the Maximum IPs/MAC filter up or to All will show these entries again.

After you load a packet capture file and refresh the view, the Configuration Utility displays the contents of the packet capture file. You do not need to refresh the view again.

Follow these steps:

- Click the Refresh menu.

More information:

Status Information (see page 10)

Hide Entries that are Already Defined

Hide entries that are already defined to more easily browse the list of applications, servers, and networks.

Important! You cannot create a server or network definition while you have hidden entries. Make sure you display all entries if you have hidden them.

To filter:

All application, server, and network entries

- Click View, All, Display All to remove filtering and display all entries. To create a definition, the view must be configured to show all application, server, and network entries.
- Click View, All, Ignore Configured to show all unconfigured (black) entries. Entries that are either configured in the Configuration Utility (blue) or configured in the management console (green) are not displayed.
- Click View, All, Configured Only to show all entries that are either configured in the Configuration Utility (blue) or configured in the management console (green). Unconfigured entries (black) are not displayed.

By application, server, or network entries

- Click View, Applications|Servers|Networks, Display All to show all application, server, or network entries.
- Click View, Applications|Servers|Networks, Ignore Configured to show all unconfigured (black) application, server, or network entries. Entries that are either configured in the Configuration Utility (blue) or configured in the management console (green) are not displayed.
- Click View, Applications|Servers|Networks, Configured Only to show all application, server, or network entries that are either configured in the Configuration Utility (blue) or configured in the management console (green). Unconfigured entries (black) are not displayed.

Filter Criteria

The Detection Criteria group shows the filter criteria that are applied to the current view:

Application Filter

Filter by:

- Single port (80). To filter a particular application port, you can also right-click in the list of Detected Applications and click Apply description (port) as Application Filter.
- Range of ports (1024-2000).

Server Filter

Filter by:

- Single IP address (192.168.0.10). To filter a particular server, you can also right-click in the list of Detected Servers or Detected Networks and click Apply description (IP) as Server Filter.
- Range of IP addresses (192.168.0.0-192.168.0.255).
- Subnet (192.168.0.0/24).

  When filtering for tagged VLAN traffic, set the Group By Mask for the Server Filter to a server subnet that corresponds to a particular VLAN. Or, set the Group By Mask to Server (/32) to display all tagged VLAN traffic.

Maximum IPs/MAC filters out data from servers sharing the same MAC address. A high ratio is a cue that a server may be on the other side of a router and should not be monitored by CA ADA. This ratio is displayed in the IPs/MAC column of the Detected Servers panel. There is an All value at the top of this list that turns this filter off.

If detected applications, servers, or networks that were previously visible disappear on a later refresh, it is likely that the servers associated with the data exceeded the Maximum IPs/MAC filter.

Network Filter

Filter by:

- Single IP address (192.168.0.10). To filter a particular network, you can also right-click in the list of networks or servers and click Apply description (IP) as Network Filter.
- Range of IP addresses (192.168.0.0-192.168.0.255).
- Subnet (192.168.0.0/24).

Group By Mask defines how to organize detected (but not configured) client IPs into subnets. For example, suppose 3 client IPs - 192.168.0.2, 192.168.1.3, and 192.168.1.23 are detected and the Group By Mask setting is 24. These IPs would be organized into 2 networks, 192.168.0.0/24 (with 192.168.0.2) and 192.168.1.0/24 (with 192.168.1.3 and 192.168.1.23).

Filter Applications

An application is a set of requests and responses on a TCP port or range of ports. The Configuration Utility automatically detects the port traffic on a server and displays the application ports in the Detected Applications pane.

Apply an Application filter on an application port to determine the servers that have networks accessing these ports. For example, filtering a port displays a list of associated servers and networks.

Sort this list by clicking a column header:

Description

Displays the name for the application port. If you see the same application name listed as both a configured application (green) and an unconfigured application (black), a server has traffic on the application port, but it is not monitored by CA ADA.

Bytes To and Bytes From, and Packets To and Packets From

Displays applications with the most traffic. As a best practice, we recommend monitoring the busiest applications.

Follow these steps:

1. In the Detected Applications pane, right-click a port and click Apply description (port) as Application Filter.

   If you want to filter an application by a port range, type the port range, for example, 60-80, in the Application Filter detection criteria field and press Enter.

2. (Optional) Add the network or server definitions to CA ADA..

More information:

Define a Server (see page 20)
Define a Network (see page 21)

Filter Networks

A network is a range of IP addresses or one IP address that represents a specific location or a logical grouping of users. The Configuration Utility automatically detects client IPs and displays them in the Detected Networks pane according to the current Group By Mask setting. For example, if the Group By Mask is set to 24, the Configuration Utility groups unconfigured client IPs into /24 networks.

When filtering networks, we recommend filtering on /24 networks. Defining /24 client networks (with 1 region) enable the QoS reporting on Users to list the actual client IPs on the network. To view the detected client IPs for a particular /24 network, place a Network filter on the /24 network you want and then set the Group By Mask to 32.

Sort the list of networks list by clicking a column header:

Bytes To and Bytes From, and Packets To and Packets From

Displays networks with the most traffic. As a best practice, we recommend monitoring the busiest networks.

TTL

Displays the Time To Live (TTL) values from all clients in the network to all viewed servers. Unlike server TTL values, monitored networks can (and usually will) have varied non-default values.

Use filtering to find a network of interest:

Network filter

Lists the servers and ports that the client network accesses. For example, applying a Network filter to a client network adds the network to the Network Filter criteria and displays a list of associated servers and application ports.

Server filter

Lists all applications on a server subnet. For example, applying a Server filter of 192.168.0.0/16 displays the servers and applications on that server subnet.

Follow these steps:

1. In the Detected Networks pane, right-click a network and click Apply *network (network) as* Network Filter or Apply *network (network)* as Server Filter.

   If you want to filter a server by a range of IPs or a subnet, type the IP range or subnet in the Network Filter detection criteria field and press Enter.

2. (Optional) Add the network or server definition to CA ADA.

More information:

Filter Criteria (see page 15)
Define a Server (see page 20)
Define a Network (see page 21)

Filter Servers

A server is a computer on the network that responds to client TCP requests. The Configuration Utility detects the SYN-ACK packet and automatically displays the corresponding server in the Detected Servers pane.

We recommend defining server subnets to monitor server traffic.

Sort the list by clicking a column header:

Bytes To and Bytes From, and Packets To and Packets From

Identifies servers with the most traffic. As a best practice, we recommend monitoring the applications on your busiest servers. If the Bytes From or Bytes To column is 0, this can indicate a problem with how the TCP packets are mirrored to the monitoring device.

VLAN

Identifies tagged server VLAN traffic.

When filtering for tagged VLAN traffic, set the Group By Mask for the Server Filter to a server subnet that corresponds to a particular VLAN. Or, set the Group By Mask to Server (/32) to display all tagged VLAN traffic.

TTL

Indicates observed Time to Live (TTL) values from the server to the client. In an ideal configuration, monitored servers are spanned directly to the monitorand this value should be a default, undecremented TTL value. 128 and 64 are common TTL values for Windows and UNIX servers, respectively.

If the TTL is not a default value, the difference between the default and the value is the number of network hops between the server and the spanned switch. As a best practice, we recommend monitoring the servers that are closest to the spanned switch. Use the Time to Live (TTL) column to find interesting candidates to monitor.

Maximum IPs/Mac and Group By Mask

Refines the filter results. Set to All to see all servers in the SPAN, and look for servers with a low ratio of IP addresses per MAC address.

Use filtering to find a server of interest:

Server filter

Lists the client networks that access the server, and which application ports are accessed. For example, applying a Server filter to a server adds the server to the Server Filter criteria and displays a list of associated application ports and client networks.

With a VLAN based SPAN (VSPAN), use the VLAN column to find the servers in the SPAN or filter with a server subnet mask that corresponds to the VLAN with the server traffic you want. For example, add a Server filter, 192.168.0.0/16, to see all servers and applications on that subnet.

Network filter

Indicates whether the server acts as a client to another server, and on which ports. Keep in mind that to monitor multi-tier applications, CA ADA automatically creates a /32 network for each server definition. For example, applying a Network filter to a server adds the server to the Network Filter criteria and displays a list of associated servers and application ports. This filter is useful for discovering a multi-tier application.

Group matching networks by selecting the mask you want from the Group By Mask list.

Follow these steps:

1. In the Detected Servers pane, right-click a server and click Apply description (port) as Server Filter or Apply description (port) as Network Filter.

   If you want to filter a server by a range of IPs or a subnet, type the IP range or subnet in the Server Filter detection criteria field and press Enter.

2. (Optional) Add the server or network definition to CA ADA.

More information:

Filter Criteria (see page 15)
Define a Server (see page 20)
Define a Network (see page 21)

Define a Server

We recommend defining the busiest servers of interest first. With a VLAN based SPAN (VSPAN), use the VLAN column to find the servers in the SPAN or filter with a server subnet mask that corresponds to the VLAN with the server traffic you want, and sort the list to find the busiest servers. After you find the busiest servers, you can apply a Server filter to find the application ports on the servers which correspond to the busiest applications.

When defining a server, we recommend the following naming conventions:

Server Type	Suggested Naming Convention	Example
Single function server	*DNSName* Note that many reporting views in CA ADA, CA PC and CA NPC append the IP address.	Goliath-196.128.34.1

One application, multiple servers in a farm	*ApplicationName-DNSName* To help you identify the application name, apply a Server filter to find the corresponding application ports.	Citrix-Zeus Citrix-Athena Citrix-Mercury
One application, multiple servers, multiple locations	*ApplicationName-DNSName-Location* To help you identify the application name, apply a Server filter to find the corresponding application ports.	Citrix-Hamlet-NewYork Citrix-Romeo-Milan Citrix-Othello-London

Follow these steps:

1. Right-click a server in the Detected Servers pane and click Define Server Subnet *description*.

   To define a group of servers, select the check box for each server you want, right-click a server, and click Quick Define Checked Servers.

2. Click Export, To Management Console to save your changes to CA ADA.

   Important! To begin monitoring the new definitions, synchronize monitor devices in CA ADA.

More information:

Filter Servers (see page 19)

Define a Network

Define client networks that correspond to the actual client subnetworks in your environment. Set the Group By Mask to filter the client traffic.

When defining a network, we recommend the following naming convention:

Network Type	Suggested Naming Convention	Example
Network	*Location-Description*	Singapore-backbone
Subnetwork	*Location-Region-Bandwidth*	Austin-Subnet10-128k

Follow these steps:

1. Right-click a network in the Detected Networks pane and click Define Network *description*.

   To define a group of networks, select each network you want, right-click a network, and click Quick Define Checked Networks.

2. Click Export, To Management Console to save your changes to CA ADA.

   Important! To begin monitoring the new definitions, synchronize monitor devices in CA ADA.

More information:

Filter Networks (see page 17)

Chapter 3: Maintain Your Configuration

We recommend using the Configuration Utility on a periodic basis to identify the traffic on your network.

Chapter 4: Troubleshooting

This section discusses frequently asked questions.

- I cannot find VLAN-tagged traffic. Why?

  When filtering for tagged VLAN traffic, set the Group By Mask for the Server Filter to a server subnet that corresponds to a particular VLAN. Or, set the Group By Mask to Server (/32) to display all tagged VLAN traffic.

- The bottom indicator shows high detected packets, however, the Configuration Utility does not display any captured data. Why?

  This is likely caused by one or more servers crossing the Maximum IPs/MAC threshold. Statistics from those servers are not counted towards their associated application and network counterparts, which can cause the totals to disappear entirely. Turning the Maximum IPs/MAC filter up or to All will show these entries.

- I clicked Refresh and an application, server, or network disappeared or its volume decreased. Is this a bug?

  This is likely caused by one or more servers crossing the Maximum IPs/MAC threshold. Statistics from those servers are not counted towards their associated application and network counterparts, which can cause the totals to decrease or disappear entirely if reduced to zero. Turning the Maximum IPs/MAC filter up or to All will show these entries again.

- When I connect to a CA Multi-Port Monitor, why do I get an exception?

  When attempting to connect the Configuration Utility to a CA Multi-Port Monitor, if you encounter the following message, close the Configuration Utility, synchronize monitor devices, and re-connect the Configuration Utility:
  `System.Exception: There is already one SuperAgent Configuration Utility request in process.`

  To avoid this issue, when you finish defining applications, servers, and networks on a logical port of a CA Multi-Port Monitor, make sure you disconnect the Configuration Utility and synchronize the configuration on the monitoring device before you attempt to configure another logical port.

- When I start the Configuration Utility, why do I get an exception?

  The computer where you run the Configuration Utility must also host the management console or the CA Standard Monitor, otherwise the following message is displayed:
  `System.NullReferenceException: Object reference not set to an instance of an object.`

- How can I tell if there is a problem with the SPAN to the monitor?

  If the Bytes From or Bytes To column is 0, this can indicate a problem with how the TCP packets are mirrored to the monitoring device.

- How are overlapping subnets in Detected Networks organized?

  Suppose two network definitions exist with subnets 192.168.0.0/16 and 192.168.10.0/24. The /24 is contained within the /16, so is data stored in the /24, the /16, or both? For both the CA ADA console and the Configuration Utility, the answer is the same: the more specific (higher /x) network definition gets the data.

  In the previous example, 192.168.10.0/24 would get the data from IPs in the range 192.168.10.0 to 192.168.10.255 while 192.168.0.0/16 would get the data from IPs in the ranges 192.168.0.0 to 192.168.9.255 and 192.168.11.0 to 192.168.255.255.

  Because of the more specific subnet data organization, the preferred workflow in the Configuration Utility is to define dense, more specific subnets and work out to wider (lower /x) ones. If you start by creating a wide user-defined subnet such as 0.0.0.0/0, everything will be aggregated into that one entry and creating more specific subnets will be difficult.

- Why can't I add a definition or export to the management console?
  - Existing console configuration entries (green) cannot be modified in the utility. This must be done from the user interface of the console.
  - Only detected but not configured entries (black) can be added.
  - Only entries configured within the utility (blue) can be edited or deleted.
  - Modifying definitions and exporting to the management console is disabled when an option from the view menu other than All is applied. This is done to avoid definition collisions between the Configuration Utility and the management console.

  In general, you should update the list of client networks and server subnets to specify the application traffic you want to monitor. If the CA ADA console does not display the application traffic you expect, use the Configuration Utility to verify that the monitoring device is seeing the application traffic.

More information:

Switch Port Mirroring Requirements (see page 8)
Where to Run the Configuration Utility (see page 7)