CA Network Flow Analysis

Operator Guide

Release 9.3.0

CA Technologies Product References

This document references the following CA Technologies products:

- CA Infrastructure Management
- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Performance Center
- CA ReporterAnalyzer
- CA Single Sign-On

Related Documentation

CA provides a full set of technical documentation in the CA Network Flow Analysis Documentation Bookshelf. Access the bookshelf by clicking the Help link in the CA Network Flow Analysis user interface. You can open the guides in PDF and HTML format from the Documentation Bookshelf.

The documentation may have been updated since its release. To get the latest CA Network Flow Analysis documentation updates and localized documentation, download the Bookshelf from CA Support.

The documentation set for CA Network Flow Analysis 9.3.0 includes the following guides:

- *Online help*: Assistance for Administrators and operators, available through the Help link in the user interface.
- *Administrator Guide*: How to set up and maintain CA Network Flow Analysis.
- *Operator Guide*: How to use the NFA console to create, view, and manage reports.
- *Installation Guide*: How to install the software and perform one-time configuration tasks.
- *Upgrade Guide*: How to upgrade the software and perform initial configuration tasks.
- *Release Notes*: Summary of CA Network Flow Analysis enhancements, fixes, and open issues.
- *CA Anomaly Detector Guide:* How to install, upgrade, configure, and use CA Anomaly Detector.
- *CA Anomaly Detector Release Notes:* Overview of the product, system requirements/recommendations, and features.

The product PDFs are in the following directory:
<install_path>\Reporter\NetQoS.ReporterAnalyzer.WebSite\help\en_US\NFA_Bookshelf\Bookshelf_Files\PDF

To view the documentation PDF files, make sure that Adobe Reader is installed.

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: CA Network Flow Analysis 13

Introducing CA Network Flow Analysis 13
Third Party Acknowledgment and License Agreements 14
Capabilities of CA Network Flow Analysis 14
Product Components 15
NFA Console 15
Console Tips and Shortcuts 16
Introduction to Performance Center 21
About Collected Data and Reports 21

Chapter 2: Using Enterprise Overview 23

Enterprise Overview Page 23
Interface Utilization 26
Interface Utilization Data 26
Configure the Display of Interface Utilization 27
Top Interfaces 28
Review Interface Use 29
Display Additional Information 30
Top Protocols and Hosts 30
Review the High-Traffic Protocols and Hosts 30
Drill Down to Protocol Details 31
Drill Down to Details About a Host 32

Chapter 3: Interface Reports 33

Open Interface Reports 33
Use the Interface Index 34
Open an Interface Report from Other Pages 36
Interface Report Types 36
Interface Overview Report 37
Top N Protocols Report 38
Top N ToS Report 41
Top N Hosts Report 43
Top N Conversations Report 46
Flows Report 48
Utilization (Calendar Chart) Report 50
Growth Report 51

Capacity Planning Report 52
Top N Autonomous System Numbers Report 59
Work with Interface Reports and Data Views 60
Change the Interface for a Report 60
Set the Time Period for a Report 61
Set the Presentation Options 64
Analyze Interface Report Data 67
Display Charts and Graphs 76
Stacked Trend Charts 76
Trend Charts 77
Pie Charts 79
Summary Tables 80
Calendar Charts 81
Mixed Display Options 82

Chapter 4: Custom Reports 83

Report Types and Usage 84
Report on Network Utilization 84
Report on Application Distribution 84
Report on ToS Distribution 84
Report on Server Activity 85
Set Up Custom Reports 85
Create a Custom Report 86
Review Settings for Custom Reports 90
Customize Which Interfaces Are in Custom Reports 91
Specify Custom Report Filters 95
Define Custom Report Periods and Schedules 103
View Custom Reports 106
Manage Custom Reports 107
Create a Report Folder 107
Rename a Report Folder 108
Move a Report to Another Folder 108
Delete Saved Report Definitions 109
Delete Report Folders 109

Chapter 5: Flow Forensics Reports 111

Flow Forensics Report Types 111
Address Report Group 112
Application Response Time Report Group 113
ICMP Report Group 115

MAC Report Group 118
MPLS Reports 119
Network Reports Group 119
QOS Report Group 121
Session Report Group 122
TCP Reports 125
VLAN Report Group 126
WAAS Segment Report Group 127
Work with Flow Forensics Reports 128
Open the Flow Forensics Page 128
Create a Flow Forensics Report 128
View a Flow Forensics Report 133
Create a Report Folder 133
Rename a Report Folder 134
Move a Report to Another Folder 134

Chapter 6: Analysis Reports 135

Set Up Analyses 135
Create an Analysis Report 136
View an Analysis Report 140
Edit an Analysis Report 142
Manage Analysis Reports 143
Create a Report Folder 143
Rename a Report Folder 144
Move a Report to Another Folder 144

Chapter 7: Site to Site Reports 145

Open the Site to Site Page 145
Create a Site to Site Report 146
Define Site to Site Report Periods and Schedules 148
Specify a Reporting Period for Site to Site Reports 148
Specify Schedules for Auto-Generated Reports 149
View a Site to Site Report 150
Create a Report Folder 151
Rename a Report Folder 151
Move a Report to Another Folder 152

Chapter 8: Views in Performance Center 153

Dashboards and Views 153
Performance Center Dashboards 154

Types of Report Pages 154
Context Page Navigation 155
CA Network Flow Analysis Views in CA Performance Center 156
CA Network Flow Analysis Views in CA NetQoS Performance Center 157
Enterprise-Level Views 159
Calendar Chart (Flow) 169
Interface: Stacked Trend Charts 172
Interface: ToS Summaries 177
Interface: Top Conversations 182
Interface: Top Hosts 189
Interface: Top Protocols 195
CA Anomaly Detector Views in Performance Center 202
Anomaly Activity 203
Anomaly Detector Overall Status 204
Top Enterprise-Wide Network Anomalies 204
Top Anomalies by Host 205
Top Anomalies by Interface 206
Enterprise-Wide Correlated Anomalies 206
Enterprise-Wide Anomalies 208
Anomaly Drill-In 210
Anomaly Trend 212
Customizing Dashboards and Views 212
View Options in CA Performance Center 213
View Options in CA NetQoS Performance Center 214
Change the View Settings 215
Change the Context for a View 217
Set a Custom Time Frame 218
Zoom In to Narrow the Time Frame 219
Custom Dashboards 220
Create a Custom Dashboard 220
Edit a Dashboard 221
Change the Context for a Dashboard 223
Change the Time Frame for a Dashboard 223
Change the Time Frame for a Dashboard 225
Build a Custom View for a Single Interface 226
Sharing Data with Other Users 227
Print a Report 228
Send a Report by Email 228
Set Up a Recurring Email Schedule 229
Manage Email Schedules 232
Generate a URL for a View 232
Organizing Dashboards in Menus 234

View a List of Menus 235
Custom Menus 236
Add a Menu 236
Edit a Menu 238

Glossary 239

Index 243

Chapter 1: CA Network Flow Analysis

CA Network Flow Analysis provides network traffic analysis with real-time visibility into the traffic throughout your enterprise. You can access as much as one year of flow data for your entire network.

This section contains the following topics:

Introducing CA Network Flow Analysis (see page 13)
Third Party Acknowledgment and License Agreements (see page 14)
Capabilities of CA Network Flow Analysis (see page 14)
Product Components (see page 15)
About Collected Data and Reports (see page 21)

Introducing CA Network Flow Analysis

CA Network Flow Analysis gives you an enterprise-wide view into the composition of traffic on every link and helps you detect threatening traffic patterns in the making. Network groups can quickly identify the source of performance problems, validate the impact of planned and unplanned changes within the network, and avoid unnecessary WAN costs. In addition, management can make accurate decisions regarding cost reduction, capacity planning, troubleshooting, and network traffic analysis across the enterprise.

The following topics provide information and procedures to help you effectively use the CA Network Flow Analysis reporting capabilities.

- CA Network Flow Analysis (see page 13)

  Introduces the product components and explains key concepts that you need to use the product effectively.

- Using Enterprise Overview (see page 23)

  Explains how to use the Enterprise Overview page to identify high-level patterns, anomalies, trends, and issues with network traffic.

- Interface Reports (see page 33)

  Describes how to use the Interface page to access interface-level reports. You can use Interfaces views to identify the cause of network problems or to anticipate upcoming problems.

- Custom Reports (see page 83)

  Explains how to use Custom Reports to solve specific questions and issues. Custom reports can be adapted to your needs.

- Flow Forensics Reports (see page 111)

  Describes how to use Flow Forensics reports to leverage the detailed data that Flow Forensics provides, such as reporting data from multiple interfaces in real time.

- Analysis Reports (see page 135)

  Explains how to create an Analysis report. An Analysis report lets you set a threshold for comparing data.

Third Party Acknowledgment and License Agreements

Third-party software was used in the creation of CA Network Flow Analysis. All third-party software has been used in accordance with the terms and conditions for use, reproduction, and distribution as defined by the applicable license agreements.

Information about third-party license agreements is provided in the following document, which is installed automatically with the software:

<install_path>\ThirdPartyContent\ThirdPartyLicenseInfo.pdf

Capabilities of CA Network Flow Analysis

CA Network Flow Analysis capabilities help you analyze network traffic and make informed decisions about resolving issues. The capabilities described in the following list can give you valuable data for capacity planning, troubleshooting, and traffic analysis.

- Identify network traffic that exceeds a specified threshold so you can manage your network proactively.
- Identify bandwidth requirements for applications and users so you can evaluate network capacity precisely.
- Immediately identify the interfaces, hosts, and applications that generate the most traffic in your enterprise. This information is essential for short-term and long-term troubleshooting.
- View the impact of application rollouts on WAN links and measure application traffic growth using protocol-level trend analyses, application baseline trend comparisons, and percent-growth tables. These analyses help you make more informed infrastructure investments.
- Pinpoint the exact cause of a network problem by examining 100 percent of all NetFlow and IPFIX traffic from the last four hours.
- Review automatic alerts and detailed reports so you discover network problems quickly.
- Design and run reports that are based on criteria that you select.

- View real-time NetFlow and IPFIX monitoring reports and alarms for every interface on the network for past 30 days with 1-minute granularity.
- Establish baselines for protocol and flow data so you can compare current data with past performance.
- Analyze trends in applications, hosts, and conversations per class of service. This information helps you optimization your network infrastructure for application performance.
- Drill into raw flows per interface to assist with troubleshooting.
- Review trend settings for historical data and for future projections to perform more effective capacity planning.

Product Components

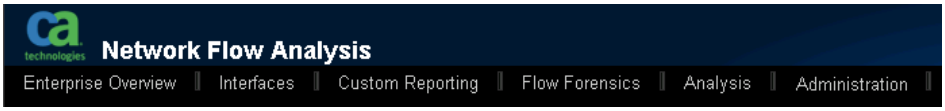
CA Network Flow Analysis software components can be installed on a single, standalone server or on separate servers in your network.

NFA Console

The primary CA Network Flow Analysis user interface is the NFA console, a web interface that you use to view the collected data, as well as perform administrative tasks. To start using the NFA console, open a browser window and enter the server name or IP address of the server that hosts the NFA console:

```
http://<IP_Address>
```

You are prompted to log in when you first access the NFA console. You can get the CA Network Flow Analysis server name or IP address and your login information from your Administrator.



When you log in to the NFA console, the Interfaces page opens. You can open the six primary pages from the NFA console menu:

- Enterprise Overview Page (see page 23): Quickly determine whether any of the interfaces in your network are nearing or have surpassed an acceptable utilization level.
- Interfaces Page (see page 33): Select one or more interfaces and run reports.
- Custom Reporting Page: Define and run Custom Reports.

- Flow Forensics Page (see page 111): Define and run reports on raw data.
- Analysis Page (see page 135): Create proactive troubleshooting reports designed to compare collected network data to a threshold, identifying potential bottlenecks, anomalies, and viruses.
- Administration Page: Perform administrative tasks for CA Network Flow Analysis, as described in the *CA Network Flow Analysis Administrator Guide.*

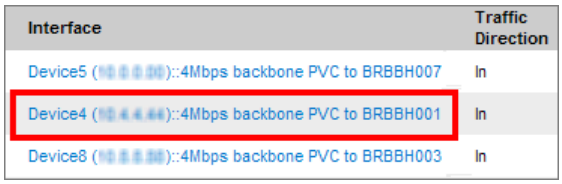
As you use the navigation links to move between console pages, some product settings are saved and other settings are cleared as you leave the page. For example, when you navigate to Enterprise Overview, Interfaces, or Flow Forensics pages, the previous settings are preserved. As you navigate to Custom Reporting, Analyses, or Administration, your previous settings are cleared and the default values are restored.

Console Tips and Shortcuts

The NFA console simplifies viewing and using CA Network Flow Analysis data. Some of the common NFA console features are described in the following topics.

Use Drilldown Links

When you view reports in the NFA console, many items are displayed in blue. Click the blue links for interfaces, hosts, conversations, and other items to drill down to additional information about the items.



From the Interface report page that opens, you can open other detailed reports specific to the selected interface, host, conversation, or other traffic type.

Display Tooltips

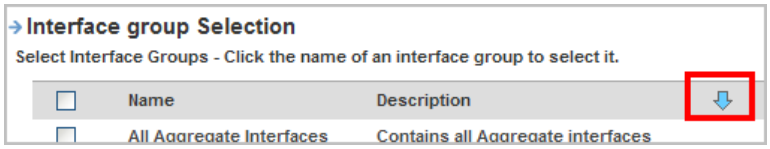
You can display detailed information for some items in report views by positioning your cursor over the item. For example, place your cursor over a bar that represents an interface to open a Tooltip. The Tooltip shows additional details about the interface, such as its parent router, description, and number of bytes.

Sort Tables by Column Heading

Sortable column headings are provided for tables of interfaces, reports, or other items. Click a column heading to sort the data. Click a second time to switch the sort mode between descending and ascending order.

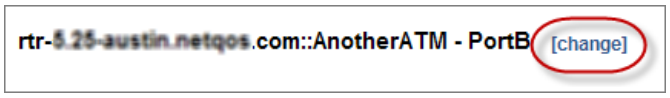
Jump Down

Some selection dialogs include a blue Jump Down arrow, which you can use to jump to the bottom of the page. For example, you can use the Jump Down arrow to locate the Save button quickly in the Interface Group Selection dialog.



Change the Interface for a Report

When you click an interface link on the Interface page, you drill down to an interface report. To view a report for a different interface, click the [change] link at the top of the page, then select another interface from the Interface Index. The report is updated to show data for the selected interface.



Also See:

Open Interface Reports (see page 33)

Search for a Router, Interface, or Interface Group

The Interface Index page includes a Search utility that you can use to filter the list and locate a router or interface. To perform a search, enter a text string in the text box and click Search.

You can include the wild card * as part of your search term. (The wild card * by itself is not a valid entry.) For example, to search for an IP address you can enter 10.0.7* to display only the addresses that begin with 10.0.7. In this example, the filtered list could include 10.0.7.1, but would not include 10.0.8.1.

The page displays a list of items that match the filter expression.

- Under the listed items, click the Next arrow or click a page number to display another page of list items.
- To display a different number of items per page, select a different value from the Max per Page list.

Save Report Data to CSV Files

You can save a report to a comma-separated value (CSV) file.

Follow these steps:

1. Display the data that interests you in one of the following locations: the Enterprise Overview page; an interface drilldown view; or a report you run on the Custom Reporting, Flow Forensics, or Analysis page.
2. Click the blue arrow next to a report view name.
3. Select the Export to CSV option from the menu that opens.

   The File Download dialog opens.
4. Click Save.

   The Save As dialog opens.
5. Specify a name and location for the .csv file, then click Save.

Open Online Help

Online help provides useful information that is easy to access when you are working in the NFA console. You can access the help system at any time by clicking the Help link that is near the top-right corner.

Email Reports

You can send a displayed report in an email immediately, or you can set up a schedule to generate an updated, complete report automatically as a PDF file.

The Email icon is included at the top of all report views:

- Enterprise Overview page views.
- Interface drilldown views.
- Reports that you run from the Custom Reporting, Flow Forensics, and Analysis pages.

If you are logged in with Administrator rights, you can email any of the reports by clicking the Email icon and you can schedule reports to be sent as PDFs by email.

Note: To email reports, an email server must be configured for CA Network Flow Analysis. If no email server is configured, an error message is displayed when you attempt to use the email function. For information about setting up an email server, contact your Administrator or see the *CA Network Flow Analysis Administrator Guide.*

Follow these steps:

1. Display a completed report.
2. Click the Email icon at the top-right corner of the report page.

   The Email Information dialog opens.
3. Enter the following information:

   Send To

   Enter the email address to which you want to send the report page. Separate multiple email addresses with commas.

   Subject

   Enter the subject line for the email.

   Message

   Enter a message to explain the report or the purpose of the email.

   Scheduling Options: Select one of the following options:

   Send Now

   Send the report by email immediately.

   Send on a Schedule

   Schedule the report to generate and send on multiple days a week or to send once a week, month, quarter, or year.

   If you select Send on a Schedule, select one of the following options:

   - Send Daily: Select which days of the week to send the email.
   - Send Weekly: Select which day of the week to send the email.
   - Send Monthly: Sets the email to be sent on the last day of the month.
   - Send Quarterly: Select the month that designates the end of the first quarter to send the email. The email is sent on the last day of each reporting quarter.
   - Send Yearly: Select the last month of the year. The email is sent on the last day of the year.

   Note: Scheduled emails generate a report PDF by using a stored URL address. The saved report definition is used to generate the scheduled report that is sent.

4. Click OK.

   - Send Now: The email is sent immediately with the current report page attached as a PDF file.
   - Send on a Schedule: The email schedule is configured. The report is generated and sent according to the schedule.

     If you have administrator privileges, you can view, edit, or delete the email schedules that you configure in the Administration pages of the NFA console. For more information, see the CA *Network Flow Analysis Administrator Guide.*

Print Reports

You can print a report view from the browser window or save the report as a PDF file.

The Print icon is included at the top of all report views:

- Enterprise Overview page views
- Interface drilldown views
- Reports that you run from the Custom Reporting, Flow Forensics, and Analysis pages

If you are logged in with Administrator rights, you can print any of the reports by clicking the Print icon.

Follow these steps:

1. Select the completed report to display it.
2. Click the Print icon at the top-right corner of the report page.

   A printable version of the report opens in a new browser window.
3. In the browser toolbar, click the Printer icon.

   Your browser displays a Print dialog box, which you use to select a printer and set other printing options.
4. Click OK to print the PDF file.

Refresh the View Data

Turn on Refresh mode for the report page to make it automatically update to reflect the most recently collected 15-minute data. When the Refresh icon is green and revolving, the page is in Refresh mode. To disable Refresh, click the icon again. Once you enable Refresh, data continues to be refreshed even when you navigate away from the page. If you leave the Enterprise Overview page, be sure to turn off Refresh.

Note: The Refresh function is available for real-time data you view in CA Network Flow Analysis--in the Enterprise Overview page and in Interface drilldown reports.

Introduction to Performance Center

CA Network Flow Analysis is designed to be integrated as a data source for either CA Performance Center or CA NetQoS Performance Center--whichever program your enterprise uses. The Performance Center Console displays report data from CA Network Flow Analysis and any other programs that are integrated as data sources.

When your administrator adds CA Network Flow Analysis as a data source for Performance Center, several changes occur:

- The NFA console banner contains a link the Performance Center Console (either *CA PC* or *NPC*).
- If your user account enables it, you can see CA Network Flow Analysis views in customizable dashboards and context pages in the Performance Center Console.
- Properly credentialed users also can drill in to details in the NFA console from views in Performance Center.

Notes:

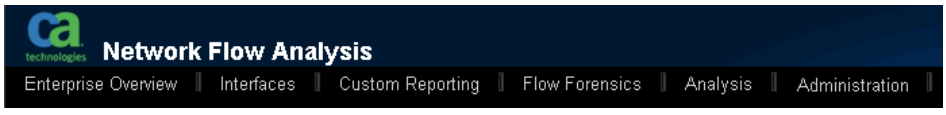
- This guide uses the term *Performance Center* to refer to CA Performance Center and CA NetQoS Performance Center collectively. Program-specific page names or functions may be identified by the full program name or acronym, which is *CA PC* for CA Performance Center and *NPC* for CA NetQoS Performance Center.
- To learn more about Performance Center views and customization options, see the online help for Performance Center.

About Collected Data and Reports

CA Network Flow Analysis uses collected data to generate statistics that are formatted and displayed in reports. Reports can be customized to suit your enterprise and your reporting requirements. This section provides information about the collected data and the types of CA Network Flow Analysis reports that are available. To learn how to access or create the available reports, see the topics that follow.

CA Network Flow Analysis collects, displays, and stores flow data. For detailed information about the data that the product collects, see the *CA Network Flow Analysis Administrator Guide.*

Note: CA Network Flow Analysis calculates a kilobyte as 1000 bytes, not 1024 bytes, in compliance with the International Systems of Units.



CA Network Flow Analysis analyzes, formats, and displays collected data in the following page views:

Enterprise Overview Page

Summarizes information about the interfaces that exceed or are close to exceeding a utilization threshold that product administrators can establish. The Enterprise Overview page also shows the top interfaces, protocols, and hosts for your enterprise. The timeframe for this report is the most recent 24 hours available to the NFA console.

Interfaces Page

Lists available routers and their component interfaces. Click an interface to drill down to more detailed information about the interface. You can choose a timeframe and can choose a report type.

Custom Reporting Page

Displays the current list of defined Custom Reports and provides options for running, creating, editing, and managing the reports. You can use a wizard to create Custom Reports. Several report types are available, including interface, protocol, ToS, host, and conversation. You can combine the types to produce the results you want. You can save and run these reports on demand or on a schedule.

Flow Forensics Page

Displays the current list of defined Flow Forensics reports and provides options for running, creating, editing, and managing the reports. You can open the Report Settings dialog to create a Flow Forensics report. You can add filters and can specify the data collection time span. For example, you can analyze protocols, hosts, or conversations on your network. You can export the data on the screen to a file in comma-separated value (CSV) format. You can save and run these reports on demand or on a schedule.

Analysis Page

Displays the current list of defined Analysis reports and provides options for running, creating, editing, and managing the reports. You can use a wizard to create an Analysis report. An Analysis report lets you establish a threshold for comparing collected data. For example, you could use an Analysis report to see which interfaces exceeded 70 percent utilization over a certain timeframe. You can save and run these reports on demand or on a schedule.

Administration Page

Provides access to administrative tasks for Administrators of CA Network Flow Analysis, as described in the *CA Network Flow Analysis Administrator Guide.*

Chapter 2: Using Enterprise Overview

The views on the Enterprise Overview page give you an overview of network traffic across the enterprise. These topics describe the enterprise-level built-in reports.

This section contains the following topics:

Enterprise Overview Page (see page 23)
Interface Utilization (see page 26)
Top Interfaces (see page 28)
Top Protocols and Hosts (see page 30)

Enterprise Overview Page

The Enterprise Overview page shows a set of built-in views of real-time network performance data. To display the Enterprise Overview page, click Enterprise Overview in the NFA console menu.

Depending on your access settings, the Enterprise Overview page may contain data for some or all of the following views:

- Interface Utilization: A table of data about the interfaces with the highest utilization levels
- Top Interfaces - In: Utilization and volume information for the interfaces that have high volumes of inbound traffic
- Top Interfaces - Out: Utilization and volume information for the interfaces that have high volumes of outbound traffic
- Top Protocols: Total volume of traffic associated with the most heavily used protocols
- Top Hosts: Traffic volumes of the most active hosts (inbound, outbound, and total traffic)

The Enterprise Overview displays data for the most recent 24-hour period that is available. The reporting timeframe is noted under the title of each view.

Available Actions for the Enterprise Overview Page

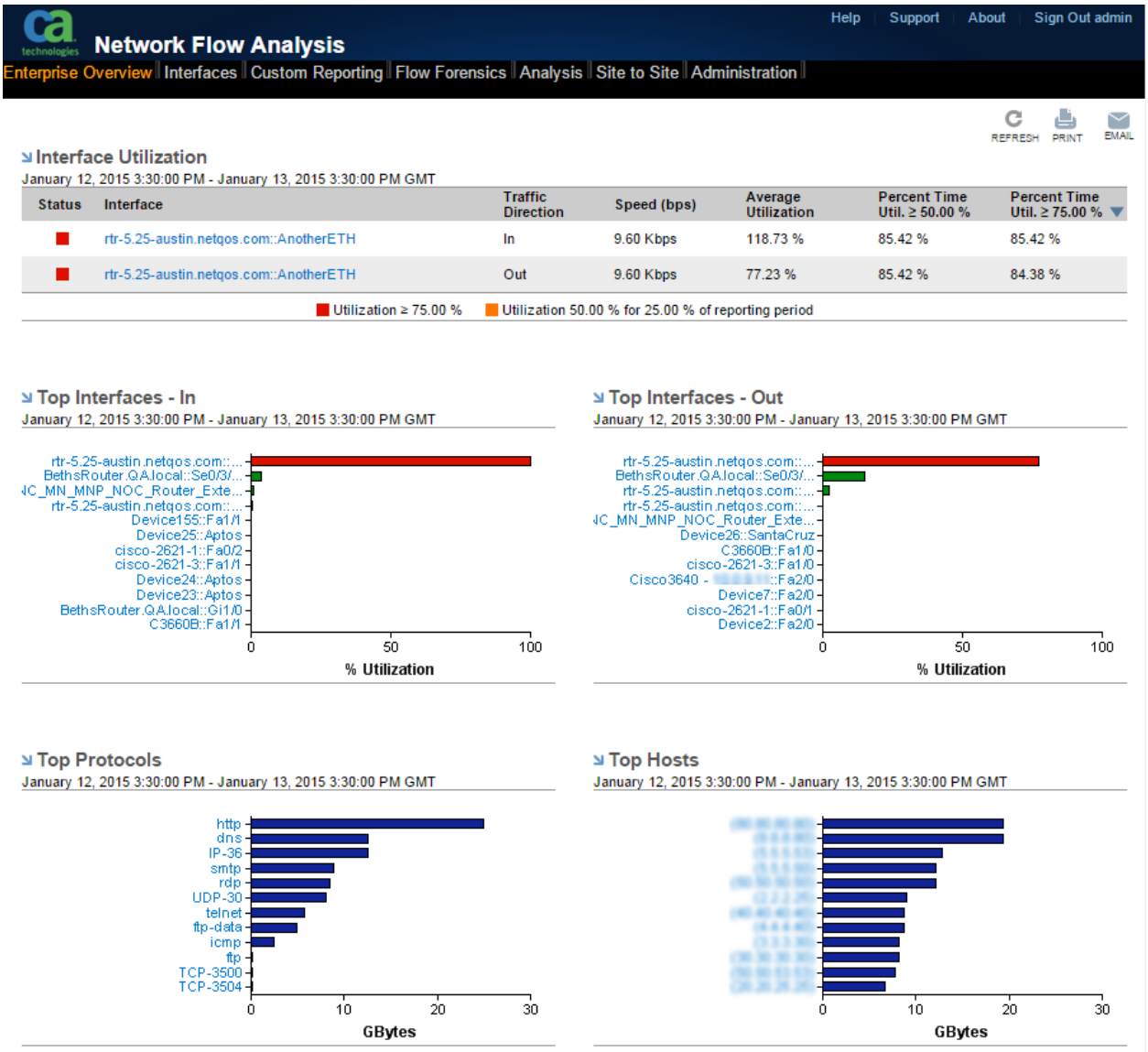
You can perform the following actions on the Enterprise Overview page, provided that you have the required access:

- Display data about each interface, protocol, or host in bar graphs by opening Tooltips.

You can display detailed information for some items in report views by positioning your cursor over the item. For example, place your cursor over a bar that represents an interface to open a Tooltip. The Tooltip shows additional details about the interface, such as its parent router, description, and number of bytes.

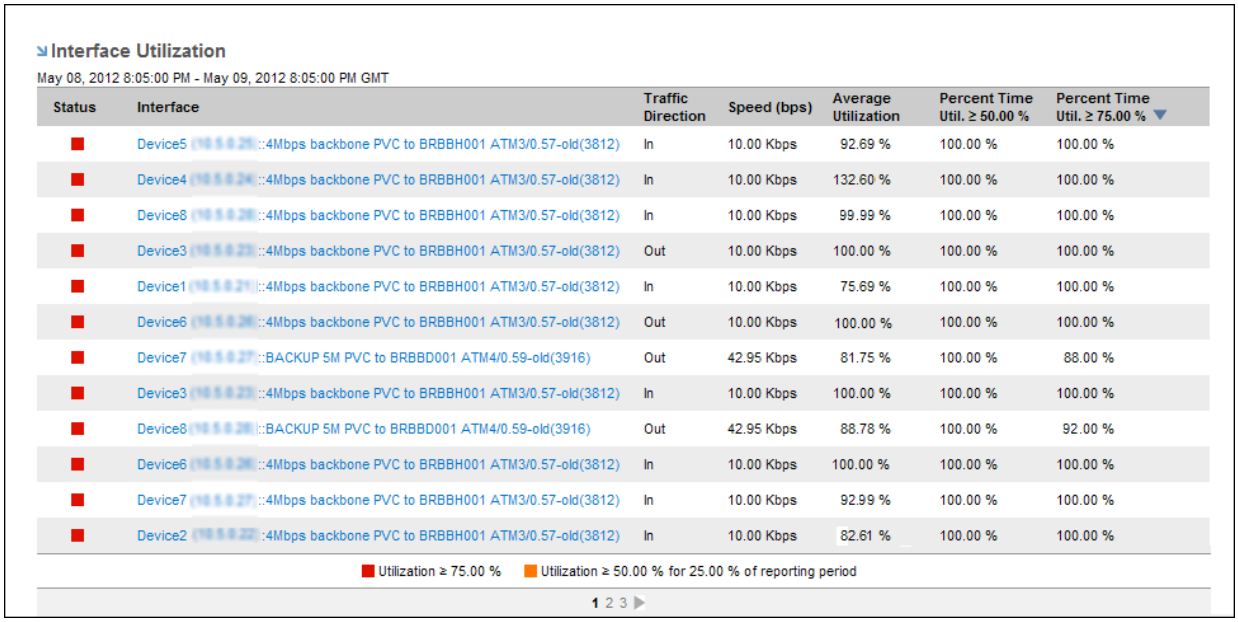
- Open additional reports about each interface, protocol, or host by clicking the bars or the blue drilldown links (see page 16).
- In the Interface Utilization view, customize the status thresholds (see page 27).
- Export the data for each view to a .CSV file (see page 18).
- Update the data by using the Refresh icon (see page 20).

- Print the Enterprise Overview page to a PDF file (see page 20) (Administrator or Power User accounts only).
- Email PDF files of the current views or schedule PDFs to be sent out to one or more recipients on a schedule (see page 18) (Administrator or Power User accounts only).



Interface Utilization

The Interface Utilization view lists the interfaces throughout the enterprise that are the most heavily used. The view is a table summary of the interfaces whose utilization exceeds the user-configured thresholds. This view is located on the Enterprise Overview page.



Interface Utilization

May 08, 2012 8:05:00 PM - May 09, 2012 8:05:00 PM GMT

Status	Interface	Traffic Direction	Speed (bps)	Average Utilization	Percent Time Util. ≥ 50.00 %	Percent Time Util. ≥ 75.00 %
■	Device5 (10.5.0.25)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	In	10.00 Kbps	92.69 %	100.00 %	100.00 %
■	Device4 (10.5.0.24)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	In	10.00 Kbps	132.60 %	100.00 %	100.00 %
■	Device8 (10.5.0.28)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	In	10.00 Kbps	99.99 %	100.00 %	100.00 %
■	Device3 (10.5.0.23)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	Out	10.00 Kbps	100.00 %	100.00 %	100.00 %
■	Device1 (10.5.0.21)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	In	10.00 Kbps	75.69 %	100.00 %	100.00 %
■	Device6 (10.5.0.26)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	Out	10.00 Kbps	100.00 %	100.00 %	100.00 %
■	Device7 (10.5.0.27)::BACKUP 5M PVC to BRBBD001 ATM4/0.59-old(3916)	Out	42.95 Kbps	81.75 %	100.00 %	88.00 %
■	Device3 (10.5.0.23)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	In	10.00 Kbps	100.00 %	100.00 %	100.00 %
■	Device8 (10.5.0.28)::BACKUP 5M PVC to BRBBD001 ATM4/0.59-old(3916)	Out	42.95 Kbps	88.78 %	100.00 %	92.00 %
■	Device6 (10.5.0.26)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	In	10.00 Kbps	100.00 %	100.00 %	100.00 %
■	Device7 (10.5.0.27)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	In	10.00 Kbps	92.99 %	100.00 %	100.00 %
■	Device2 (10.5.0.22)::4Mbps backbone PVC to BRBBH001 ATM3/0.57-old(3812)	In	10.00 Kbps	82.61 %	100.00 %	100.00 %

■ Utilization ≥ 75.00 % ■ Utilization ≥ 50.00 % for 25.00 % of reporting period

1 2 3 ▶

Find Interface Utilization Information in the Performance Center Console

The Performance Center Console has a similar view, Interfaces Over Threshold. This view is located by default on the Infrastructure Overview dashboard in CA Performance Center and on the Traffic Analysis page in CA NetQoS Performance Center.

Interface Utilization Data

The Interface Utilization view displays the following information for each interface listed:

Status

Indicates utilization level: Green (Normal), Orange (Warning or Elevated), Red (Critical).

Interface

Identifies the interface by name.

Traffic Direction

Identifies whether the reported traffic is inbound or outbound.

Speed

Lists the speed that is set for the interface by the Administrator.

Average Utilization

Lists the percentage of total utilization of the interface on average.

Percent Time Utilization ≥ Warning Level

Identifies the percentage of the time that interface utilization meets or exceeds the Warning level. The default Warning level is 50 percent utilization for 25 percent of the reporting period. The Interface Utilization list contains only the interfaces that meet the Warning level. If an operator changes this setting, the contents of the interface list may change.

Percent Time Utilization ≥ Critical Level

Identifies the percentage of the time that interface utilization meets or exceeds the Critical level. The default Critical level is 75 percent utilization of the interface capacity for 25 percent of the reporting period. The operator can change the Critical level.

Legend

Describes the criteria that determine which interfaces are displayed and what the status icons represent. In the example, the icons are defined as follows:

- Critical (red) status: The interface utilizes 75 percent or more of its bandwidth over 25 percent of the reporting period (default settings).
- Warning/Elevated (orange) status: The interface utilizes 50 percent or more of its bandwidth over 25 percent of the reporting period (default settings).

Information about changing the utilization thresholds is in Configure the Display of Interface Utilization Data (see page 27).

Configure the Display of Interface Utilization

If your user account has the Administrator or Power User role, you can change the configuration of the data displayed in the Interface Utilization view of the Enterprise Overview page.

For example, you could display the orange status indicator next to interfaces that utilize 65 -74.9 percent of their bandwidth (instead of 50-74.9 percent) for at least 25 percent of the reporting period.

Follow these steps:

1. Click the menu arrow next to the Interface Utilization label and select Configure.

   The legend at the bottom of the Interface Utilization view changes to include editable fields.

2. Enter utilization threshold values for the following settings:

   Red Utilization %

   Set the minimum threshold for assigning a Critical status to interfaces. Interfaces are flagged at the Critical level when their utilization approaches or exceeds this value.

   Orange Utilization %

   Set the minimum threshold for assigning a warning status to interfaces. Interfaces are flagged at the Warning level when their utilization is at or above this value, but is below the minimum threshold for Critical status.

   For ... % of reporting period

   Set the reporting period percentage to use for calculating the thresholds.

   For example, if the value is 25, the report includes only the interfaces that have a utilization level above the threshold for 25 percent of the reporting period. For the default reporting period of 24 hours, this list includes interfaces at or above the threshold value for six hours or more during that period.

   Show

   (Optional) Change the number of interfaces that are displayed on each list page.

3. Click Submit Changes when the configuration changes are complete.

   The Interface Utilization table and legend are updated to reflect your modified threshold settings.

Top Interfaces

The Top Interfaces views display the interfaces that have the most inbound and outbound traffic in your network during the reporting period. These two views are located on the Enterprise Overview page

Each bar is identified on the left by its parent router and interface name. By default, a red bar indicates that the interface exceeds a utilization threshold of 75 percent. An orange bar indicates that the interface utilization is less than 75 percent, but has a utilization of at least 50 percent. A green bar indicates that the interface utilization is less than 50 percent.

You can perform the following tasks in the Top Interfaces - In and Top Interfaces - Out views:

- Review the information in the graphical display.
- Display a Tooltip with additional details about the interface by holding your cursor over an interface bar or name.

  Tooltips display the parent router name, interface name, interface description, flow volume, flow rate, interface utilization, and inbound speed.
- Drill down to display details on corresponding Interface page views by clicking a bar or name.
- Export the view data to a .CSV file.
- Change the utilization thresholds by editing the threshold values in the Interface Utilization view.

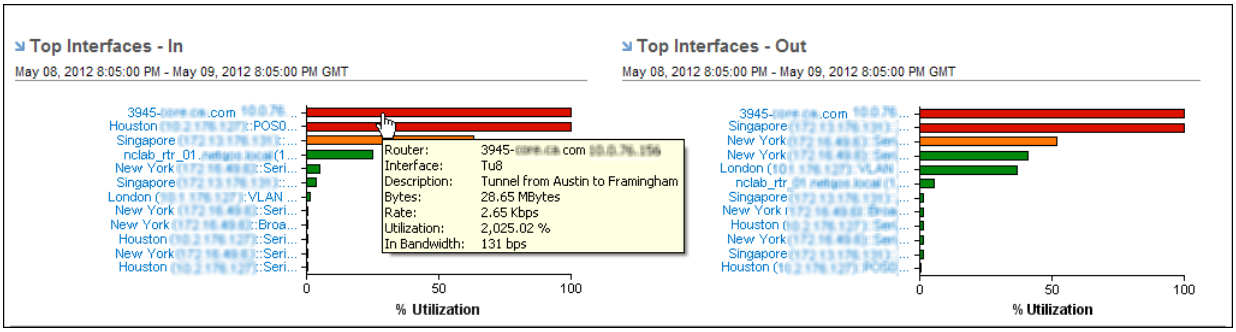
Find Similar Information in the Performance Center Console

The Performance Center Console has a similar view, Top IP Interface Utilization (Flow). In CA Performance Center, this view is located on the Infrastructure Overview dashboard by default. In the CA NetQoS Performance Center Console, the view is located on the Traffic Analysis report page by default.

Review Interface Use

The Top Interfaces views give you quick visual indicators of the interfaces in your network that are used the most heavily. The Top Interfaces views also give you easy access to more detailed information about specific interfaces.

For example, an interface that exceeds 75 percent utilization for outbound traffic could have degraded application performance. To investigate the issue, click the interface name in the graph. A more detailed report for the interface opens.



Display Additional Information

You can display detailed information for some graphical elements by positioning the cursor over the element. For example, place the cursor over an interface bar or name to display additional details about the interface, such as its parent router and flow volume.

Top Protocols and Hosts

The bottom view of the Enterprise Overview page displays the protocols and hosts in your enterprise that are most heavily utilized. These views display the protocols and hosts that are transferring the most data in your enterprise and how many bytes of data that each one is transferring.

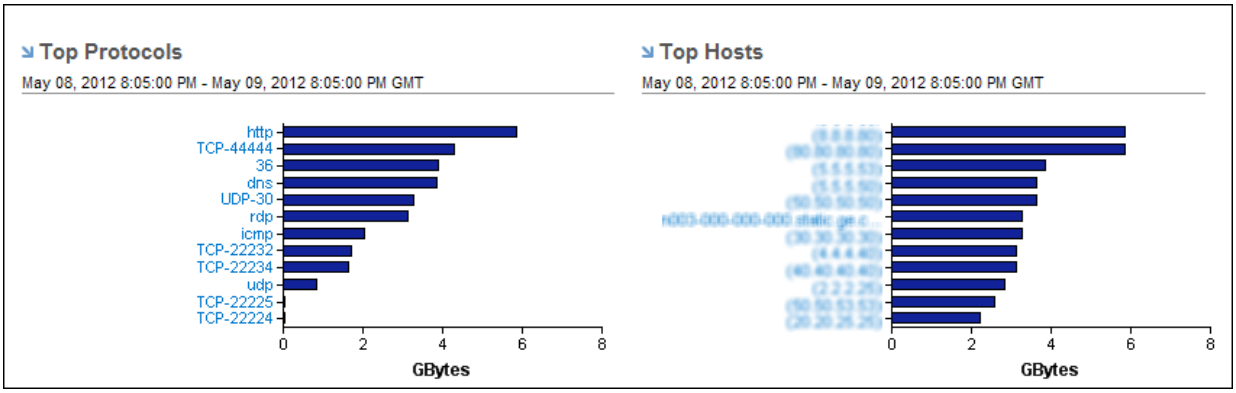
This section contains the following topics:

Review the High-Traffic Protocols and Hosts (see page 30)
Drill Down to Protocol Details (see page 31)
Drill Down to Details About a Host (see page 32)

Review the High-Traffic Protocols and Hosts

The Top Protocols and Top Hosts views provide quick visual indicators of the most utilized protocol and hosts in your network. You can use the links to drill down to more detailed information about a specific protocol or host.

For example, suppose a protocol has a high volume of traffic. To investigate whether the traffic is correctly routed over the network, you click the protocol name in the graph and drill down to details.



Display Tooltips in the Top Protocols and Top Hosts views by holding your cursor over a name or bar.

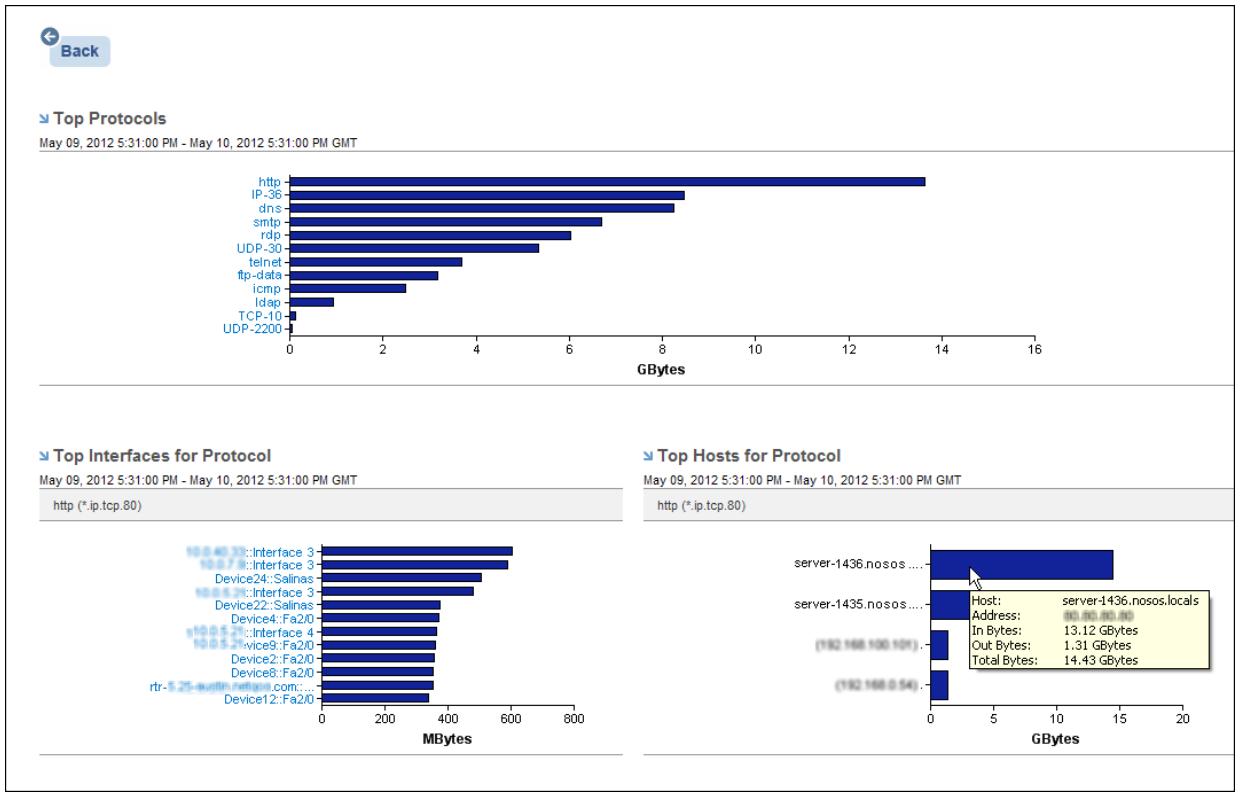
- Protocol: Display the protocol name (keyword), encapsulation (transport protocol and port number), and total traffic volume.
- Host: Display the host name, IP address, and volume of inbound, outbound, and total traffic.

Find Similar Views in the Performance Center Console

The Performance Center Console has similar views, the Top Enterprise Protocols by Volume and Top Enterprise Hosts by Volume. These views are on the Infrastructure Overview dashboard (CA PC) and the Enterprise Dashboard (NPC).

Drill Down to Protocol Details

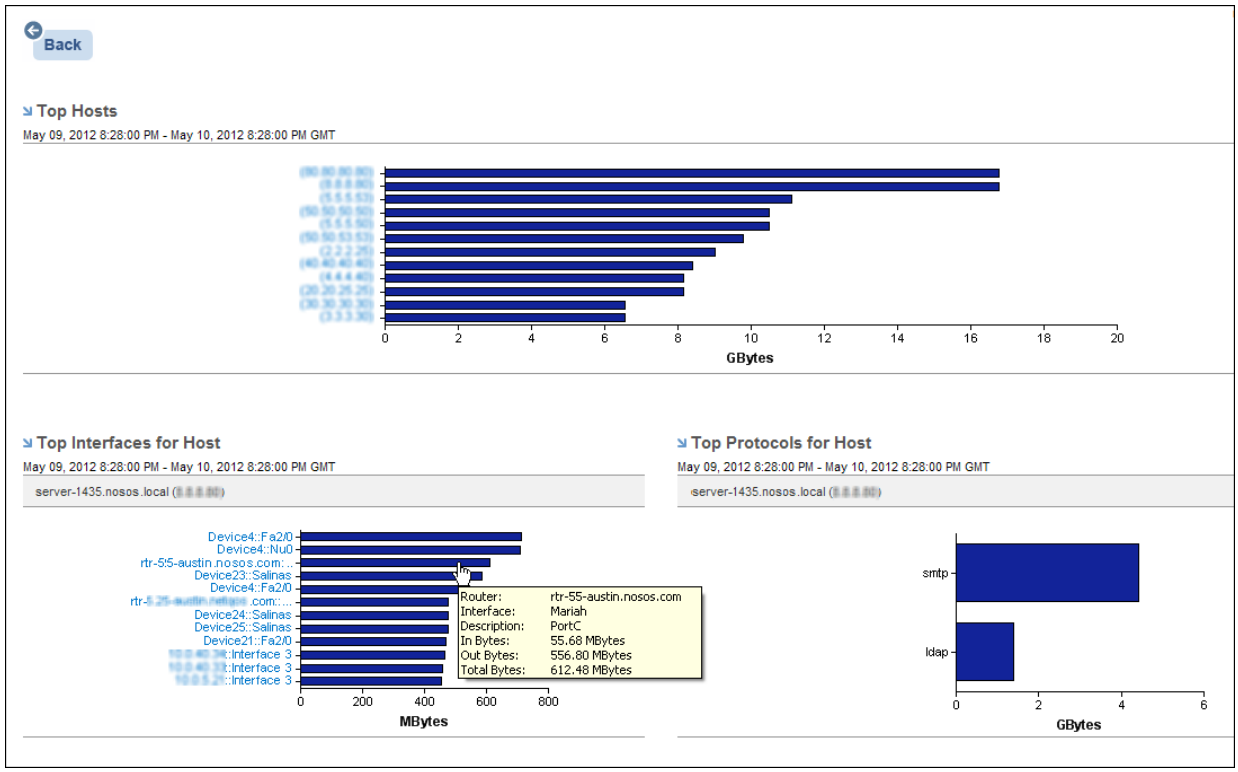
In the Top Protocols report view on the Enterprise Overview page, click an individual protocol to see a more detailed summary report for the protocol, including its top interfaces and hosts. You can use this report to perform a high-level investigation of the related interfaces.



To open an Interface Protocols report and see detailed protocol data for the interface, click the interface name or bar. You can drill down to the Interface Protocols report from the view in the NFA console. Properly credentialed users also can drill down from the view in the Performance Center Console.

Drill Down to Details About a Host

In the Top Hosts view on the Enterprise Overview page, you can click a host name to see a more detailed summary report for the host, including its top interfaces and protocols. You can use this report to perform a high-level investigation of the protocols and interfaces for the host traffic.



In the Top Interfaces for Host report view, click the name of an interface to open an Interface Hosts report and see detailed protocol data specific to that interface.

To drill down to details, click the host name or bar. Properly credentialed users also can drill down from the view in the Performance Center Console.

Chapter 3: Interface Reports

You can use Interface page reports to review traffic for specific interfaces. You can get an overview of network traffic from the Enterprise Overview reports, then get more detail from the Interface page reports. The following topics describe how to view reports on the Interface pages.

This section contains the following topics:

Open Interface Reports (see page 33)
Interface Report Types (see page 36)
Work with Interface Reports and Data Views (see page 60)
Display Charts and Graphs (see page 76)

Open Interface Reports

Interface reports show details about a specific interface. If you click an interface name on the Enterprise Overview page, for example, you drill down to details on the Interface report page. You can change the report presentation mode or open other types of interface reports.

The top right corner of the report page has following options:

Refresh

Click the Refresh icon to make the page update automatically. In Refresh mode, the page shows the most up-to-date data available. The Refresh icon is green and revolving as long as the page is in Refresh mode. Data continues to be refreshed even if you navigate away from the page.

To turn off Refresh mode, click the icon again. Make sure to turn off the Refresh mode before you leave the page.

The Refresh function is available for real-time data that you view--on the Enterprise Overview page and in interface drilldown reports.

Email

Send the reports by email to one or more users (Administrator or Power User accounts only).

Print

Print the entire page of reports (Administrator or Power User accounts only).

The Flow Forensics links near the top and bottom of the report page open the page for configuring and running Flow Forensics reports. A Flow Forensics report lets you view detail for the raw data flows.

Use the Interface Index

When you log in to the NFA console, the Interfaces page opens and shows the Interface Index. You can use the Interface Index to select an interface and view reports for it. You can search for an interface on the Router or Group tab.

Note: The Group tab appears only if the product is registered as a data source for Performance Center. If the product is not registered, the Interface tab appears in place of the Group tab.

Open an Interface Report: Router Tab

You can use the Router tab in the Interface Index to locate an interface by router. The Interface Index shows the available routers in an alphanumerically sorted list. By default, 20 routers are shown on each page of the list.

Follow these steps:

1. Select Interfaces in the NFA console menu.

   The Interfaces page opens and shows the Interface Index.

2. Make sure the Router tab is displayed.

3. Locate the interface that interests you. Use any of the following options to locate the interface:

   - Click the name of the parent router to expand a list of its interfaces.
   - Search: Search for whole or partial text strings. Searching filters the list to show only the entries that have an Interface or Description column value that matches your search term.
   - Max per Page: Change the Max per Page setting to show more routers and interfaces on each page.

4. Click the interface that interests you.

   An Interface Overview report page opens, which displays data for the selected interface.

5. (Optional) Change the format or type of data displayed in the report:

   a. Click the gray bar on the left.

      The Presentation menu opens.

   b. Select the desired display and metric options, as described in Set the Presentation Options (see page 64).

   c. (Optional) Click the bar again to hide the menu.

Open an Interface Report: Group Tab

You can locate and select an interface by using the Group tab in the Interface Index. The Group tab shows the groups organized in a tree. The tree can help you locate a specific interface, especially when in an enterprise that has large numbers of routers and interfaces.

Note: The Group tab appears only if the product is registered as a data source for Performance Center. If the product is not registered, the Interface tab appears in place of the Group tab.

Follow these steps:

1. Select Interfaces in the NFA console menu, if the Interface Index page is not already visible.

   The Interfaces page opens and shows the Interface Index. This is the first page that you see when you log in to the NFA console.

2. Click the Group tab.

   The group tree is displayed in the left pane.

3. Locate the interface that interests you. Use any of the following options to locate the interface:

   - Click the group that interests you.

     To expand the contents of a high-level group, click its arrow icon. For example, you could click the Inventory group or expand the Inventory group and select a domain sub-group.

     If the selected group or its sub-groups contain interfaces, the list of the interfaces opens in the right pane.

   - Sort by Column Heading: Click a column heading to re-sort the list. The entire list is sorted, not just the items on the current page.

   - Filter by: Click a 'Filter by' option to display active, inactive, or all interfaces.

   - Search: Search for whole or partial text strings. Searching filters the list to show only the entries that have an Interface or Description column value that matches your search term.

   - Max per Page: Change the Max per Page setting to show more routers and interfaces on each page.

4. Click the interface that interests you.

   An Interface Overview report page opens, which displays data for the selected interface.

5. (Optional) Change the format or type of data displayed in the report:
   a. Click the gray bar on the left.

      The Presentation menu opens.

   b. Select the desired display and metric options, as described in Set the Presentation Options (see page 64).

   c. (Optional) Click the bar again to hide the menu.

Interface Tab

The Interface tab displays a list of the available interfaces in an alphanumerically sorted list. By default, 10 interfaces are shown on each page. To re-sort the table data, click a column heading.

.

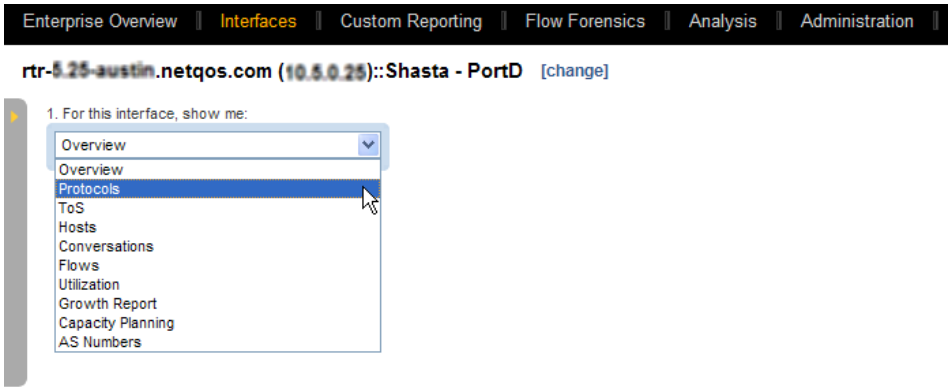
Open an Interface Report from Other Pages

In addition to opening an interface report from the Interface Index, you can drill down to detailed reports by clicking links in other reports. For example, you can drill down to details by clicking an interface name in an Enterprise Overview page report.

You can also drill down to interface reports from some Performance Center Console views. This option is available for views of CA Network Flow Analysis data, provided that your administrator has enabled the drill down function.

Interface Report Types

If you select an interface in the Interface Index or you click a drilldown link, a report opens in the Interface pages. The initial report is an Overview report. To display a different report type, select an option from the list in the upper left corner.



Use the icons at the top to refresh, print, or email the report page (see page 33).

Note: If the product is registered with CA Performance Center you can click the blue arrow next to the report title and select CA PC Interface Performance. The CA Performance Center Console opens to show Interface Pages: Details page for the Interface.

Interface Overview Report

An interface Overview report is a broad summary of information about the selected interface. This topic describes how to display an Overview report.

Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Make sure that Overview is selected as the report type at the top of the page.

   The report page is shows the following interface data:
   - Protocol data that is Inbound and outbound on the interface
   - ToS data that is Inbound and outbound on the interface
   - Data that travels to and from hosts
   - Total volume of conversation data

   If you want to display another report type, select an option from the report menu at the top-left corner of the page.
3. (Optional) Change the type of data presentation and measurement by using the Presentation options (see page 64).
   - Mixed Chart of Rate, Volume, or Utilization data:
     - Stacked trend charts of incoming and outgoing protocol and ToS data
     - Pie charts that show the volume of data to and from hosts
     - Pie chart that shows the total volume of conversation data
   - Mixed Trend of Rate, Volume, or Utilization data:
     - Stacked trend charts of incoming and outgoing protocol and ToS data
     - Trend summary charts that show the volume of data to and from hosts
     - Trend summary chart that shows the total volume of conversation data

     Use the Show Top setting to specify the maximum number of conversations to include. (Default setting)

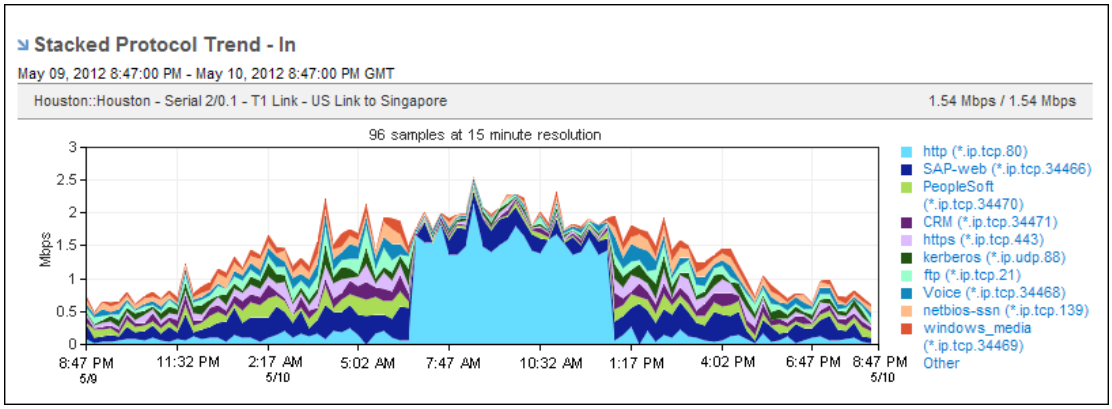
- Pie Chart: Shows pie charts of the following data:
  - Incoming and outgoing protocol and ToS data
  - Volume of data to and from hosts
  - Total volume of conversation data

4. (Optional) Change the reporting period: Open the Timeframe dialog by clicking the timeframe link (see page 61).

   The reporting period is the most recent 24-hour period by default.

Top N Protocols Report

A Top N Protocols report provides information about the protocols that generate the most traffic on a specific interface. This topic describes how to display a Top N Protocols report.



Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select Protocols from the report type menu at the top of the page.
3. Make sure that the report scope is set to Top N Protocols. The Top N Protocols link should appear next to the report type at the top.

   The report page is updated to show protocol data in stacked trend charts by default. The report includes views for inbound, outbound, and total protocol data.

4. (Optional) Change the type of data presentation and measurement by using the Presentation options (see page 64).
   - Stacked Trend Chart of Rate, Volume, or Utilization data
   - Trend Chart of Rate, Volume, or Utilization data:

     Use the Show Top setting to specify the maximum number of conversations to include. (Default setting)
   - Pie Chart
   - Summary Table of Rate, Volume, or Utilization data

   Each option displays data that is inbound and outbound on the selected interface.
5. (Optional) Change the reporting period: Open the Timeframe dialog by clicking the timeframe link (see page 61).

   The reporting period is the most recent 24-hour period by default.

Note: You also can display Protocol Summary views in a Custom report.

Open a Drilldown Protocol Report

To drill down to more detailed, protocol-specific data for the selected interface, click the name of a protocol in any of the Top N Protocol views. An overview report opens for the protocol on the selected interface.

Display an Interface Report for a Single Protocol

To drill down to details about a specific protocol, click one of the protocol links in a Top N Protocols view. A report opens, which you can display in Overview, Details, Hosts, or Conversations mode. The options in the Presentation menu are mode-specific. You can display any of the following types of data and views:

- Overview mode Mixed Chart or Mixed Trend chart: Rate, volume, or utilization data for the protocol on the selected interface
- Overview or Hosts mode Pie Chart in the following views: From (outbound on the interface), To (inbound on the interface), and Total
- Details mode Multi-Period Trend chart: Rate, volume, or utilization data in any combination of the following views, which are shown with or without baselines:
  - (Displayed by Default) Last Hour, Last 2 Hours, Last 8 Hours, and Daily
  - Weekly, Monthly, and Yearly
- Details mode Calendar Chart Rate in either of the following views:
  - Direction In: Protocol data coming into the interface
  - Direction Out: Protocol data going out from the interface

- Hosts mode Trend Chart: Rate, volume, or utilization data for the number of top hosts that you specify
- Hosts mode Summary Table: Table of rate, volume, or utilization data for hosts who used the protocol on the selected interface
- Conversations mode Trend Chart or Summary Table: Rate, volume, or utilization data for conversations that used the protocol on the selected interface
- Conversations mode Pie Chart: Data for all conversations that used the protocol on the selected interface

To return to the summary view of all protocols on the interface, click the link that is named for the currently selected protocol and click Select Top N Protocols.

Find Protocol Views in the Performance Center Console

Protocol data from CA Network Flow Analysis is displayed in the following locations in the Performance Center Console. (The built-in dashboards and report pages that are noted here show the views by default.)

- Top Enterprise Protocols by Volume
  - (CA PC) Infrastructure Overview and Network Overview dashboards; Summary context view in a custom dashboard
  - (NPC) Enterprise, Traffic Analysis, Network Overview, and custom dashboards
- Top Protocols (Bar) and Top Protocols (Pie)
  - (CA PC) Custom dashboards
  - (NPC) Custom dashboards; Interface Pages: Interface QoS and custom tab views
- Top Protocols (Table)
  - (CA PC) Custom dashboards
  - (NPC) Custom dashboards; Interface Pages custom tab views
- Stacked Protocol Trend
  - (CA PC) Interface Pages: IP Performance and CBQoS report pages
  - (NPC) Interface Pages: Interface Capacity, Interface QoS, and custom tab views

See Also:

Stacked Protocol Trend (see page 172)
Protocol Trend Views (see page 67)
Protocol Summary Views (see page 72)

Top N ToS Report

The Top N ToS report provides information about the Types of Service (ToS) markings of the packets that generate the most traffic for the selected interface. This topic describes how to display a Top N ToS report.

Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select ToS as the report type at the top of the page.
3. Make sure the report scope is set to Top N ToS. The Top N ToS link should appear next to the report type setting.

   The report page is updated to show ToS data in stacked trend charts. The report includes views for inbound, outbound, and total ToS data.
4. (Optional) Change the type of data presentation and measurement by using the Presentation options (see page 64).
   - Stacked Trend Chart of Rate, Volume, or Utilization data (Default setting)
   - Trend Chart of Rate, Volume, or Utilization data: Use the Show Top setting to specify the maximum number of conversations to include.
   - Pie Chart
   - Summary Table of Rate, Volume, or Utilization data

   Each option displays data that is inbound and outbound on the selected interface.
5. (Optional) Change the reporting period: Open the Timeframe dialog by clicking the timeframe link (see page 61).

   The reporting period is the most recent 24-hour period by default.

Display an Interface Report for a Single ToS

To drill down to more detailed, ToS-specific data for the selected interface, click a ToS link in a Top N ToS view. An overview report for the ToS value on that interface opens.

You can view the report in Overview or Details mode by selecting one of the following report types:

- Overview mode Mixed Chart or Mixed Trend chart: Rate, volume, or utilization data for the ToS on the selected interface

- Overview mode Pie Chart views:
  - ToS Protocol Summary - In or Out: Data going in or out of the interface for the protocols that use the ToS
  - ToS Hosts Summary - From or To: Data going from or to the hosts that use the ToS
  - ToS Conversations Summary - Total: Data for all conversations that use the ToS (coming in and going out of the interface)
- Details mode: Charts of rate, volume, or utilization data in any combination of the following views, which are shown with or without baselines:
  - (Displayed by Default) Last Hour, Last 2 Hours, Last 8 Hours, and Daily
  - Weekly, Monthly, and Yearly
- Protocols mode Trend Chart or Summary Table: Rate, volume, or utilization data
- Protocols mode Stacked Trend Chart or Pie Chart views of data for the protocols that used the ToS: In (inbound on the interface), Out (outbound on the interface), or Total
- Hosts mode Trend Chart: Rate, volume, or utilization data for the number of top hosts you specify
- Hosts mode Summary Table: Table of rate, volume, or utilization data for hosts who used the ToS on the selected interface
- Hosts mode summary Pie Chart views of data for the hosts that used the ToS: From (data from the host), To (data to the host), or Total
- Conversations mode Trend Chart: Rate, volume, or utilization data for the number of top conversations you specify
- Conversations mode Summary Table: Table of rate, volume, or utilization data for conversations that used the ToS on the selected interface
- Conversations mode Pie Chart: Data for all conversations that used the ToS on the selected interface

To return to the summary view, click the link named for the currently selected ToS and click Select Top N Hosts.

Find ToS Views in the Performance Center Console

ToS data from CA Network Flow Analysis is displayed in the following Performance Center Console locations. (The built-in dashboards and report pages that are noted here show the views by default.)

- Stacked ToS Trend
  - (CA PC) Interface Pages: CBQoS report page or a custom dashboard
  - (NPC) Interface Pages: Interface QoS or custom tab views

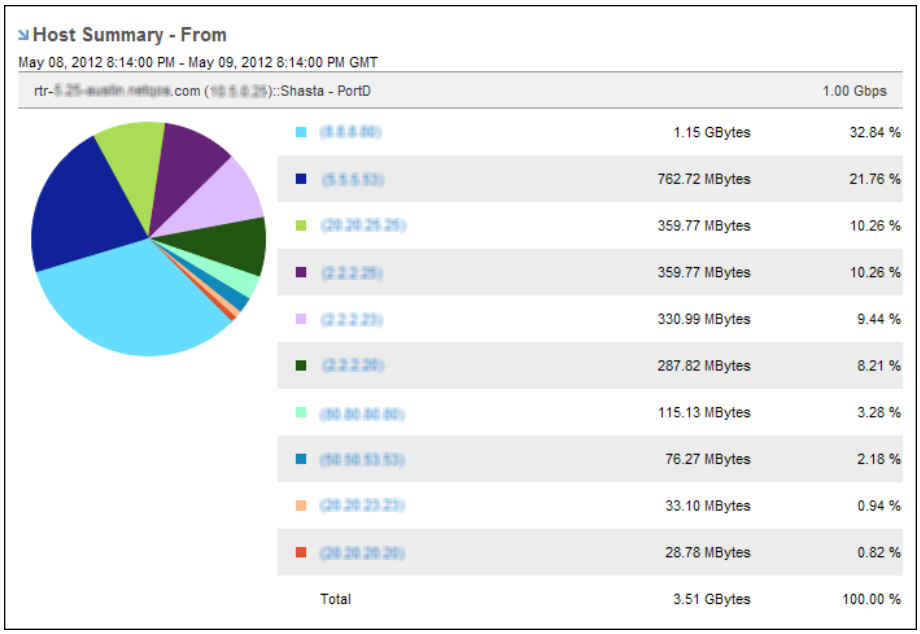
- ToS Summary Pie
  - (CA PC) Custom dashboard; Interface Pages: IP Performance tab
  - (NPC) Interface Pages or custom tab views
- ToS Summary Table
  - (CA PC) Custom dashboard
  - (NPC) Interface Pages: Interface QoS or custom tab views

Also See:

ToS Summary (Pie) (see page 178)
ToS Summary (Table) (see page 180)
Stacked ToS Trend (see page 175)

Top N Hosts Report

The Top N Hosts report provides information about the hosts that generate the most traffic on the selected interface. This topic describes how to display a Top N Hosts report.



Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select Hosts as the report type at the top of the page.
3. Make sure the report scope is set to Top N Hosts. The Top N Hosts link should appear next to the report type setting.

   The report page is updated to show host summary pie charts by default. The report includes views for the following host data:
   - From: Top hosts who sent data to the interface.
   - To: Top hosts who received data from the interface.
   - Total: Top hosts who either sent data to the interface or received data from the interface.
4. (Optional) Change the data presentation type and the data measurement type by using the Presentation options (see page 64).
   - Trend Chart of Rate, Volume, or Utilization data: Show trend charts for data that travels to and from the hosts.

     Use the Show Top setting to specify the maximum number of conversations to include.
   - Pie Chart: Show pie charts for data that travels to and from the hosts, with lists of hosts and their data volumes. (Default setting)
   - Summary Table of Rate, Volume, or Utilization data: Show a table of data that travels to and from the hosts.
5. (Optional) Change the reporting period: Open the Timeframe dialog by clicking the timeframe link (see page 61).

   The reporting period is the most recent 24-hour period by default.

Display an Interface Report for a Single Host

To drill down to more detailed, host-specific data for the selected interface, click a host name in a Top N Host view. An overview report for the host on that interface opens. You can view the host details or the host protocols.

You can view this type of report in Details mode or Protocols mode, which have the following options:

- Details mode: Charts of rate, volume, or utilization data in any combination of the following views:
  - (Displayed by Default) Last Hour, Last 2 Hours, Last 8 Hours, and Daily
  - Weekly, Monthly, and Yearly
- Protocols mode Trend Chart or Summary Table: Rate, volume, or utilization for the protocols that the hosts used. You see the data coming into the interface and the data going out from the interface.
- Protocols mode Stacked Trend Chart: Data for all protocols that the hosts used (coming into and going out of the interface).

To return to the summary view, click the link that is named for the currently selected host and click Select Top N Hosts.

Find Host Views in the Performance Center Console

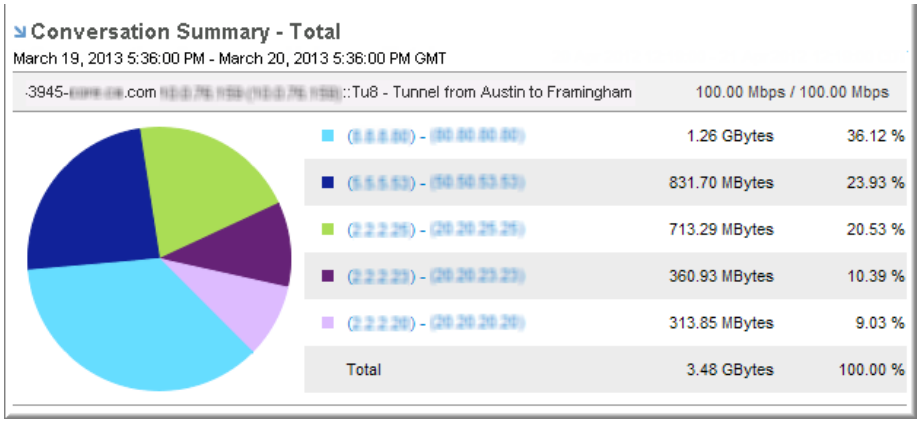
Host data from CA Network Flow Analysis is displayed in the following Performance Center Console locations. (The built-in dashboards and report pages that are noted here show the views by default.)

- Top Enterprise Hosts by Volume or Top Hosts (Bar)
  - (CA PC) Infrastructure Overview, Network Overview, and custom dashboards
  - (NPC) Enterprise, Traffic Analysis, Network Overview, and custom dashboards
- Top Hosts (Bar)
  - (CA PC) Custom dashboards; Interface Pages: IP Performance report page
  - (NPC) Custom dashboards; Interface Pages: Interface Capacity, Interface QoS, and custom tab views
- Top Hosts (Pie)
  - (CA PC) Custom dashboards; Interface Pages: IP Performance report page
  - (NPC) Custom dashboards; Interface Pages: Interface QoS, and custom tab views

- Top Hosts (Table)
  - (CA PC) Custom dashboards
  - (NPC) Custom dashboards; Interface Pages custom tab views

Top N Conversations Report

The Top N Conversations report provides information about the hosts that generate the most traffic on the selected interface. This topic describes how to display a Top N Conversations report.



Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select Conversations as the report type at the top of the page.
3. Make sure the report scope is set to Top N Conversations. The Top N Conversations link should appear next to the report type setting.

   The report page is updated to show a conversation summary pie chart by default.

4. (Optional) Change the data presentation type and the data measurement type by using the Presentation options (see page 64).

   - Trend Chart of Rate, Volume, or Utilization data: Show a trend chart for data that travels to and from the source host in the conversations. (Default setting)

     Use the Show Top setting to specify the maximum number of conversations to include.

   - Pie Chart: Show a summary pie chart with a list of conversations and their data volumes.

   - Summary Table of Rate, Volume, or Utilization data: Show a table of data that travels to and from the source host in the conversations.

5. (Optional) Change the reporting period: Open the Timeframe dialog by clicking the timeframe link (see page 61).

   The reporting period is the most recent 24-hour period by default.

Display an Interface Report for a Single Conversation

To drill down to details about a specific conversation, click one of the conversation links in the Top N Conversations view. A report opens, which you can configure to show any of the following data:

You can view this type of report in Details mode or Protocols mode, which have the following options:

- Details mode: Charts of rate, volume, or utilization data in any combination of the following views:
  - (Displayed by Default) Last Hour, Last 2 Hours, Last 8 Hours, and Daily
  - Weekly, Monthly, and Yearly
- Protocols mode Trend Chart or Summary Table: Rate, volume, or utilization for the protocols that the conversations used. You see the data coming into the interface and the data going out from the interface.
- Protocols mode Stacked Trend Chart: Data for all protocols that the conversations used (coming into and going out of the interface).

To return to the summary view of all conversations on the interface, click the link that is named for the currently selected conversation and click Select Top N Conversations.

Find Conversation Views in the Performance Center Console

Conversation data from CA Network Flow Analysis is displayed in the following Performance Center Console locations. (The built-in dashboards and report pages that are noted here show the views by default.)

- Top Conversations (Bar)
  - (CA PC) Custom dashboards
  - (NPC) Interface Pages: Interface Capacity and custom tab views
- Top Conversations (Pie)
  - (CA PC) Custom dashboards; Interface Pages: IP Performance report page
  - (NPC) Interface Pages: Interface QoS and custom tab views
- Top Conversations (Table)
  - (CA PC) Custom dashboards
  - (NPC) Interface Pages custom tab views

Flows Report

A Flows report is a trend plot that shows the rate of the flows that enter and leave the selected interface. A Flows report helps you find patterns or anomalies.

Viruses typically generate large increases in flow counts. The flow rate can indicate the load on the Harvester.

Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select Flows as the report type at the top of the page.

   The report page is updated to show flow trend charts.
3. (Optional) Change the data measurement type by using the Presentation options (see page 64):

   Rate (default setting) or Volume

   Each option displays trend charts of data that is inbound and outbound on the selected interface.

   You can also select Show Baselines to view +/- 1 Standard Deviation. The baseline is computed by calculating the average and standard deviation for a maximum of 10 samples (the last six weeks and the last four days). This rolling baseline feature provides a visual representation of a current and historical trend overlay. When a current trend line is above or below the baseline, the performance is out of the norm. When the current trend is within the baseline, the performance is within the range of historical behavior.
4. (Optional) Change the reporting period: Open the Timeframe dialog by clicking the timeframe link (see page 61).

   The reporting period is the most recent 24-hour period by default.

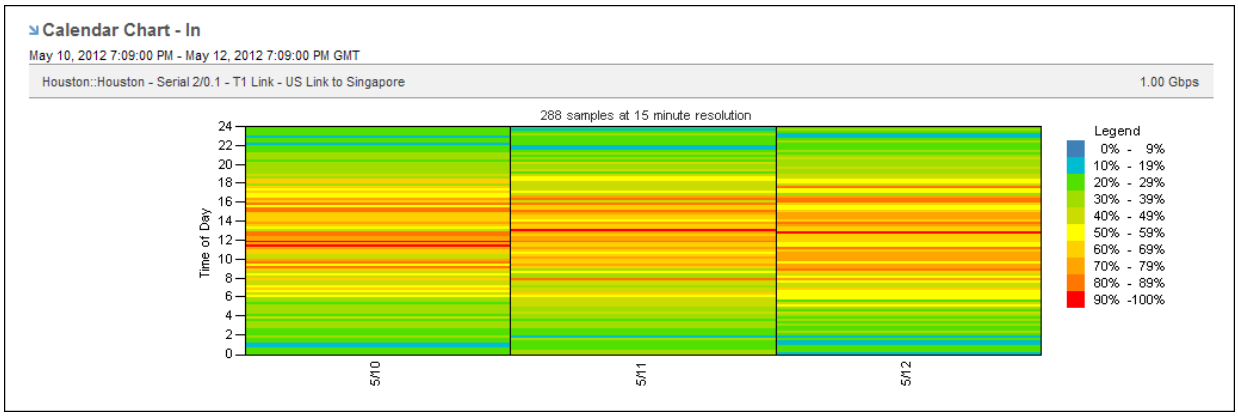
Find Flows Views in the Performance Center Console

The Top Flows by Interface view is displayed in the following Performance Center Console dashboards.

- (CA PC) Infrastructure Overview dashboard (by default)
- (CA PC) Management Overview dashboard (by default)
- (CA PC) Summary context view in a custom dashboard (see page 220)
- (NPC) Custom dashboard

Utilization (Calendar Chart) Report

The Utilization (Calendar Chart) report maps the utilization percentage of the selected interface over time. Utilization is calculated on either inbound or outbound traffic, depending on the selected Presentation mode.



This view makes it easy to detect recurring data patterns. Finding a pattern can help you identify the source of high traffic rates and potential performance issues. You might discover that the high traffic rates you thought were intermittent actually follow a pattern. The view can show the hour of each day when utilization is the highest, for example.

Each color represents a severity range that is calculated as a percentage of total capacity. High utilization is shown in orange and red. Low utilization is shown in green and blue.

Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select Utilization from the report type menu at the top of the page.

   The report page is updated.
3. (Optional) Choose the direction of the traffic by using the Presentation options (see page 64):
   - Direction In: Show traffic that is inbound on the interface.
   - Direction Out: Show traffic that is outbound on the interface.
4. (Optional) Change the reporting period: Open the Timeframe dialog by clicking the timeframe link (see page 61).

   The reporting period is the most recent 24-hour period by default.

Find Calendar Chart Views in the Performance Center Console

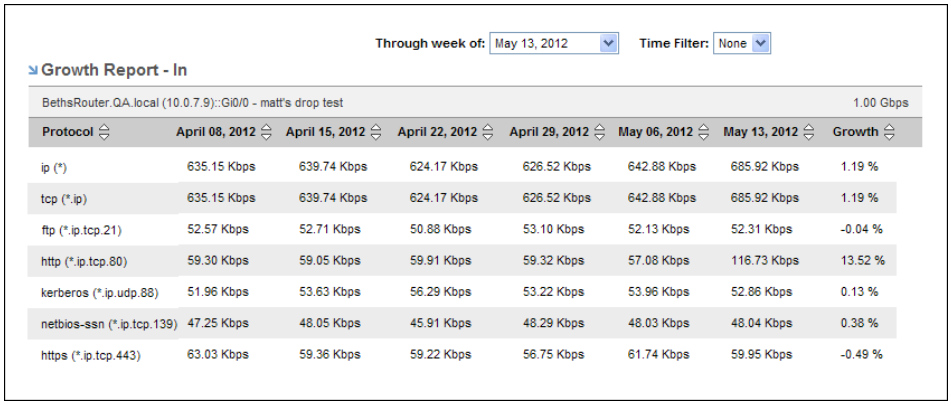
To see the utilization calendar chart for an interface in the Performance Center Console, add it to a custom dashboard or report page:

- (CA PC) Custom dashboard with Calendar Heat Chart (Flow) - In or - Out
- (NPC) Interface pages: Custom report page with Calendar Chart (Flow) - Total

Growth Report

The Growth report provides historical growth statistics for the top protocols on the selected interface--so you can see which applications have increasing capacity needs. This knowledge helps you make decisions about adding capacity in the future.

This topic describes how to display a Growth report.


Through week of: May 13, 2012 Time Filter: None

Growth Report - In

BethsRouter.QA.local (10.0.7.9)::Gi0/0 - matt's drop test 1.00 Gbps

Protocol	April 08, 2012	April 15, 2012	April 22, 2012	April 29, 2012	May 06, 2012	May 13, 2012	Growth
ip (*)	635.15 Kbps	639.74 Kbps	624.17 Kbps	626.52 Kbps	642.88 Kbps	685.92 Kbps	1.19 %
tcp (*.ip)	635.15 Kbps	639.74 Kbps	624.17 Kbps	626.52 Kbps	642.88 Kbps	685.92 Kbps	1.19 %
ftp (*.ip.tcp.21)	52.57 Kbps	52.71 Kbps	50.88 Kbps	53.10 Kbps	52.13 Kbps	52.31 Kbps	-0.04 %
http (*.ip.tcp.80)	59.30 Kbps	59.05 Kbps	59.91 Kbps	59.32 Kbps	57.08 Kbps	116.73 Kbps	13.52 %
kerberos (*.ip.udp.88)	51.96 Kbps	53.63 Kbps	56.29 Kbps	53.22 Kbps	53.96 Kbps	52.86 Kbps	0.13 %
netbios-ssn (*.ip.tcp.139)	47.25 Kbps	48.05 Kbps	45.91 Kbps	48.29 Kbps	48.03 Kbps	48.04 Kbps	0.38 %
https (*.ip.tcp.443)	63.03 Kbps	59.36 Kbps	59.22 Kbps	56.75 Kbps	61.74 Kbps	59.95 Kbps	-0.49 %

Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select Growth Report as the report type at the top of the page.

   The report page is updated to show a Growth Report table.
3. (Optional) Choose the direction of the traffic to display by using the Presentation options (see page 64).
   - Direction In: Show traffic that is inbound to the interface.
   - Direction Out: Show traffic that is outbound from the interface.

4. (Optional) Change the reporting time period:
   a. Select Last 6 Weeks (default setting) or Last 6 Months in the Presentation options (see page 64).
      - Last 6 Weeks: Sets the report to show six weeks of data. The six most recent weeks are selected by default.
      - Last 6 Months: Sets the report to show six months of data. The six most recent months are selected by default.
   b. (Optional) Use the 'Through week of' or the 'Through month of' option to select an alternative ending week or month for the six-week or six-month time period.
   c. (Optional) Restrict the reporting range by selecting a time filter from the Time Filter option list.

      Time filters are created by the Administrator for CA Network Flow Analysis. For example, the Administrator could create a time filter to restrict the report data to business hours and business days. If the Time Filter list is empty, your Administrator has not created any time filters.

Also See:

Set the Time Period for a Report (see page 61)

Capacity Planning Report

Capacity Planning reports show traffic trends, which are useful for planning. Future traffic is calculated by analyzing previous traffic. Capacity Planning reports project trends for rate, volume, and utilization for the following data on the selected interface:

- Overall traffic (IP Summary)
- Protocol traffic
- ToS traffic

You can specify several display and calculation options for the report:

- Time span of the historical (actual) data, which is shown with a white background on the view
- Time span of the projected data, which is shown with a gray background on the view
- Time range of the data that is used to calculate projections and (optionally) a time filter to exclude certain time periods from calculations

- Analysis type algorithm: Daily Percentile or Daily Average
- Threshold line, which is configured based on your selected percentage and selected bandwidth or speed

Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select Capacity Planning as the report type at the top of the page.
3. Select the report scope:
   - IP Summary: Overview of traffic on the selected interface
   - Protocols: Protocol traffic on the selected interface
   - ToS: ToS traffic on the selected interface

   The report page is updated.
4. (Optional) Change the reporting time frame and calculation options by using the Trend Settings options (see page 56).
5. (Optional) Change the data presentation type and the data measurement type by using the Presentation options (see page 64): Rate (default setting), Volume, or Utilization

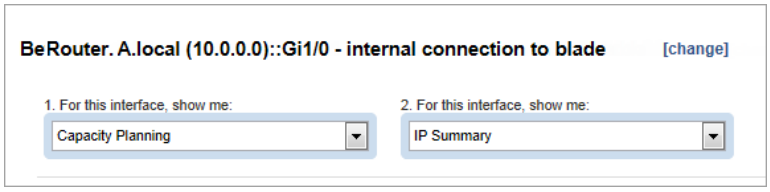
   Each option displays views of data that is inbound (In) and outbound (Out) on the interface.

Views on the Capacity Planning Report Page

You can configure the Capacity Planning report views to display historical data and calculate projections for three types of interface data on the selected interface:

- IP Summary - Overview of traffic
- Protocols - Protocol traffic
- ToS. - ToS

To change the data type, select a different option from the secondary menu at the top of the page.



The views that are shown on the report page are determined by two sets of options:

- Secondary report mode: IP Summary (default setting), Protocols, or ToS
- Presentation mode: Rate (default setting), Volume, or Utilization

IP Summary Report Page

The IP Summary report page displays the following view and table.

- IP Summary Trend - Total - Overall traffic inbound and outbound on the selected interface

  Two trend charts are included:

  - Rate presentation - Rate In and Rate Out trend charts show the data rates, expressed in a scale that is appropriate for the highest-rate value in the view (Y-Axis).
  - Volume presentation - Bytes In and Bytes Out trend charts show the data volume, expressed in a scale that is appropriate for the highest volume in the trend chart (Y-Axis).
  - Utilization presentation - Utilization In and Utilization Out trend charts show the utilization of interface capacity, which is measured in percentages (Y-Axis).

  The X-Axis shows date and time progression.

  The charts show color-coded lines:

  - Green line - Rate or volume of inbound data, or the utilization of inbound capacity
  - Blue line - Rate or volume of outbound data, or the utilization of outbound capacity
  - Red line - Threshold, which is configured by setting the Percentage value in the Trend Settings dialog (Calculations area)

  The historical data has a white background; the projected data has a gray background.

- IP Summary Table

  The IP Summary table contains the following columns:

  - Direction: Traffic direction with respect to the interface, either inbound (In) or outbound (Out)
  - Trend: Icon that shows whether the traffic is increasing or decreasing
  - Daily Change: Change over a day that is calculated for the rate (bps), volume (Bytes), or utilization (%)

- Days Until Threshold: Number of days until the traffic is expected to reach the known capacity of the interface
- Date of Threshold: Calendar date on which the traffic is expected to reach the known capacity of the interface

Protocols or ToS Report Page

The Protocol and ToS report pages display stacked trend charts of the historical traffic for a maximum of 12 protocols or ToS. A stacked trendline shows the predicted future traffic for each protocol or ToS.

The report page displays the following views and tables.

- Protocol Stacked Trend or ToS Stacked Trend (In and Out versions) - Inbound and outbound protocol traffic on the selected interface
  - Rate presentation - Data rates, expressed in a scale that is appropriate for the highest-rate value in the view (Y-Axis).
  - Volume presentation - Data volume, expressed in a scale that is appropriate for the highest volume in the view (Y-Axis).
  - Utilization presentation - Utilization of capacity for the selected interface, which is measured in percentages (Y-Axis).

  The X-Axis shows date and time progression.

  The red Threshold line shows the outbound threshold level, which is set in the Percentage field of the Trend Settings (Calculations) dialog.

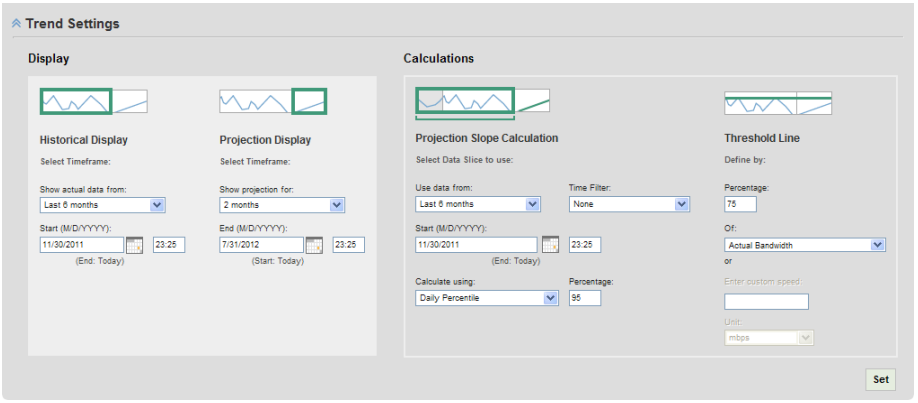
  The historical data has a white background; the projected data has a gray background.
- Protocol or ToS Table (In and Out versions)

  The tables contain the following columns:
  - Protocol Name: (Protocol table only) Name of the protocol, which may consist of its keyword and encapsulation (transport protocol and port number).
  - Type of Service: (ToS table only) ToS label, which may be a default label or a label your administrator has configured
  - Trend: Icon that shows whether the traffic is increasing or decreasing
  - Growth %: Percentage of traffic increase
  - Current %: Percentage of the total traffic that the protocol or ToS is using at the end date of the historical analysis (the current date)
  - Projected %: Percentage of the total traffic that the protocol or ToS is using at the end date of the traffic projection

  The Trend and Daily Change columns are defined in the IP Summary table description.

Trend Settings for Capacity Planning Reports

When you open a Capacity Planning report, the Trend Settings controls are at the top of the page. Display options are on the left and Calculations options are on the right. Use these settings to control the data display and projection calculations in the report.



Trend Settings Display Options

Use the Display options to specify the historical time period and the projection time period displayed in the report. This setting does not determine the data that is used to make projection calculations.

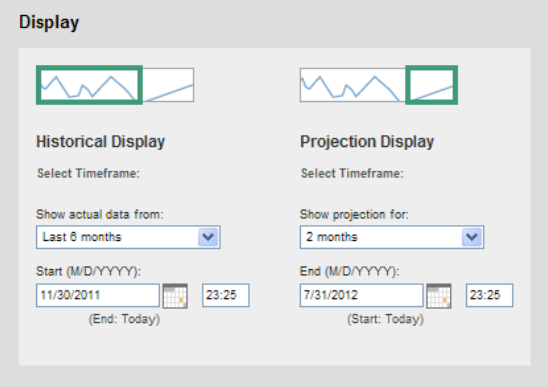
Follow these steps:

1. In the Historical Display section, select a time period from the 'Show actual data from' list.

   You can select a time period that is relative to today's date, such as Last 7 days, Last 1 month, Last 2 months, and Last 3 months. Alternatively, you can select Custom to specify a specific date.

   Note: The report displays the data starting at this time but does not necessarily use this time as the starting point to calculate the projection. For example, if you want the projection to calculate from six months of historical data but want to display only seven days of that data. In this scenario, you would select Last 7 days in this menu.

2. Accept the default start date or specify a custom start date in any of the following ways:
   - Click the calendar icon and choose a date from the calendar pop-up.
   - Enter a date value in the Start box in the DD/MM/YYYY format.
   - Enter a custom start time in the box on the right. Use the 24-hour time format.



3. Accept the default time period or select a time period from the 'Show projection for' list in the Projection Display section.

   You can select a time period relative to the Historical Display end date (such as 1 month) or you can select Custom to specify a date.

4. Accept the default end date or specify a custom end date for the projection in any of the following ways:
   - Click the calendar icon and choose a date from the calendar pop-up.
   - Enter a date value in the End box in the DD/MM/YYYY format.
   - Enter a custom end time in the box on the right. Use the 24-hour time format.

5. Click Set.

   The report views below the Trend Settings regenerate and reflect your changes.

   Note: If you make further changes, click Set again.

Trend Settings Calculations Options

Use the Calculations options to specify the data, calculation method, and threshold for calculating the projection data. These time period settings do not affect the projection data displayed in the report.

Follow these steps:

1. In the Projection Slope Calculation section, use the 'Use data from' list to select the historical time period you want use to calculate the projection data.

   You can select a time period that is relative to the current date, such as Last 7 days, Last 1 month, Last 2 months, or Last months. Alternatively, you can select Custom to select a specific start date.

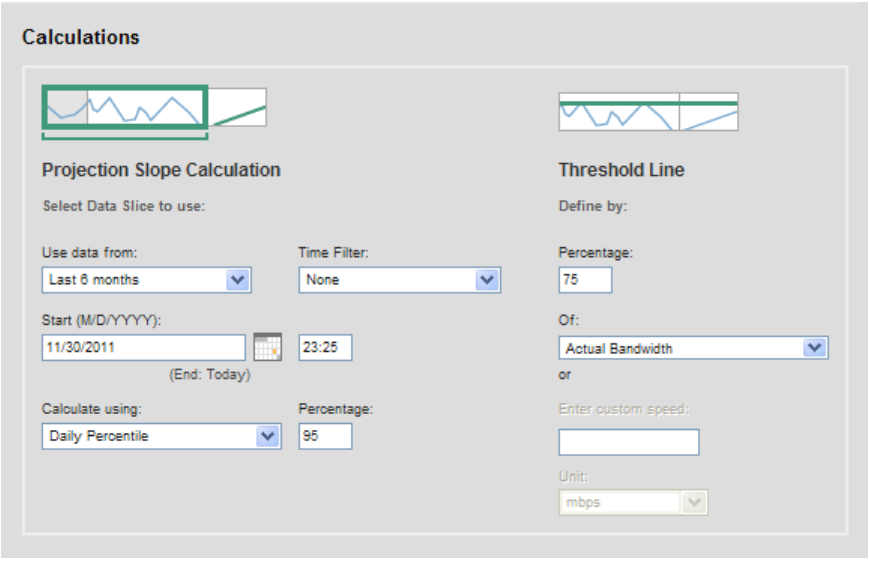
   Note: The report uses this starting time for calculations but does not necessarily use this time to display historical data in the report. For example, if you want the projection to calculate from 6 months of historical data but want to display only seven days of that data. In this scenario, you select 'Last 6 months' in this menu.

2. Use the Time Filters list to select a filter for restricting the data.

   Note: User accounts that are assigned the Power User or the Administrator role can create custom time filters. For information about creating time filters, see the *CA Network Flow Analysis Administrator Guide.*

3. Accept the default start date or specify a custom start date in any of the following ways:

   - Click the calendar icon and choose a date from the calendar pop-up.
   - Enter a date value in the Start box in the DD/MM/YYYY format.
   - Enter a custom start time in the box on the right. Use 24-hour time format.



4. Select a calculation method from the 'Calculate using' list and enter a value in the Percentage box.

   You can select Daily Percentile or Daily Average. To use the Daily Percentile method, enter a value in the Percentage field.

5. Enter a value in the Percentage box and select a measurement from the Of list in the Threshold Line section.

   The default measurement is Actual Bandwidth.

6. Click Set.

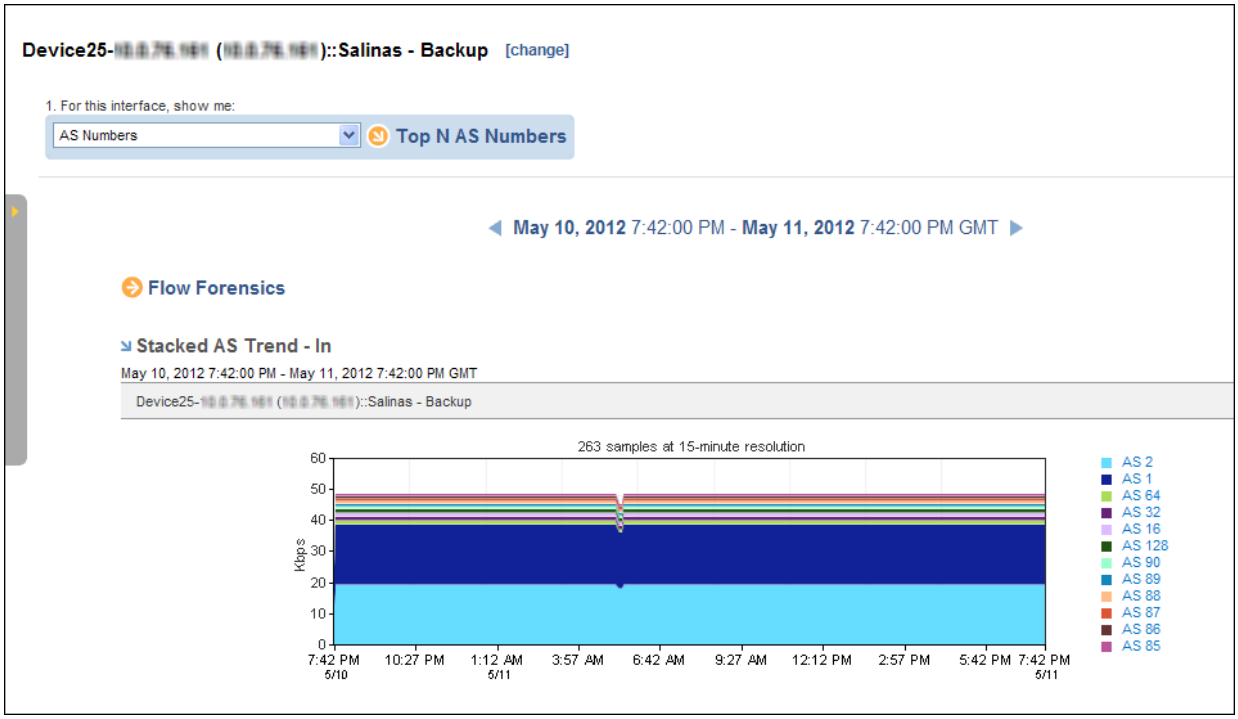
   The Trend report views regenerate and reflect your changes.

   Note: If you make further changes, click Set again.

Top N Autonomous System Numbers Report

The Top N AS report provides AS (Autonomous System) Next Hop data. The Next Hop data provides high-level summaries of total volume and rate statistics for each AS number on a particular interface. This type of reporting is valuable for managing network routes efficiently. The information helps service providers control costs by comparing traffic usage through transit networks versus traffic through networks with peer agreements.

This topic describes how to display a Top N AS report.



Follow these steps:

1. Display an interface report in either of the following ways:
   - Locate and click an interface on the Interfaces page.
   - Click an interface link in an existing view--for example, on the Enterprise Overview page.
2. Select AS Numbers as the report type at the top.
3. Make sure the Top N AS Numbers link appears next to the report type setting.

   The report page is updated.
4. (Optional) Change the data presentation type and the data measurement type by using the Presentation options (see page 64).
   - Stacked Trend Chart (default setting) of Rate, Volume, or Utilization data
   - Trend Chart of Rate, Volume, or Utilization data
   - Pie Chart
   - Summary Table of Rate, Volume, or Utilization data

   Each option displays views of data that is inbound (In) and outbound (Out) on the interface and data that is coming from (From) the previous hop and going to (To) the next hop.
5. (Optional) Change the reporting period: Open the Timeframe dialog by clicking the timeframe link (see page 61).

   The reporting period is the most recent 24-hour period by default.

Work with Interface Reports and Data Views

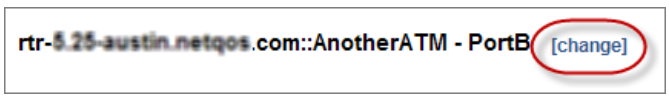
Each Interface report includes specific view types that display the data for the selected interface or group of interfaces. When you open an Interface report, the data is displayed in the report views uses the default Presentation options and settings.

Change the Interface for a Report

If you click an interface link on the Interface page, you drill down to an interface report. You can use the [change] link to view a report for a different interface.

Follow these steps:

1. Click the [change] option next to the interface name at the top of the report.



The Interface Index (see page 34) opens.

2. Locate the interface that interests you in either of the following ways:
   - Expand the parent router and select an interface from the list of details.
   - Use the Search field to locate an interface (see page 17).
3. Click the link in the Interface column.

   The Interface Index closes. You return to the Interfaces report page, which displays data for the selected interface.

Set the Time Period for a Report

The Enterprise Overview displays data for the previous 24-hour period. Interface reports also display data for the previous 24 hours by default. You can change the reporting period by using the time period controls at the top of the report page.

Note: The Capacity Planning report uses two different time periods for calculations and reporting data. Information about configuring time periods for capacity planning trends is in the topic Trend Settings for the Capacity Planning Report (see page 56).

When you view Interfaces report pages, you can change the time period for the displayed data. For example, if you notice an issue in a 1-day report, you might want to change the time period to be the last seven days. Expanding the time period can reveal whether the issue occurs daily.

The current time period is shown at the top of most Interfaces report pages. These interface reports reflect 1-minute resolution data. For a 24-hour time period, the report shows the data points in the previous 24 hours, including the final full 1-minute data point. For example, if you generate or refresh the report on May 11, 2012 at 16:11 GMT, the time period for the report is May 10, 2012 16:10:00 through May 11, 2012 16:10:00.

Note: Each user account has an assigned time zone, which determines how time is labeled in reports. For example, if a user who has a time zone of Central Standard Time (CST) views a report with data for 8:00 to 9:00 A.M., the data for 8:00 to 9:00 A.M. CST appears in the report. An Administrator can modify this setting for the user account. For more information about user account administration, see the *CA Network Flow Analysis Administrator Guide.*

The time period at the top of the report page is a link to the options you use to change the reporting time period.

Scroll the Time Period Interval

You can keep the current time span length for the interface report (such as 24 hours, one week, one month, or custom), but can shift the time period backward or forward. For example, you can scroll the time period back to show data for the week before the week now on display.

To scroll the time period back by one increment, click the Back icon .

To scroll the time period forward by one increment, click the Forward icon .

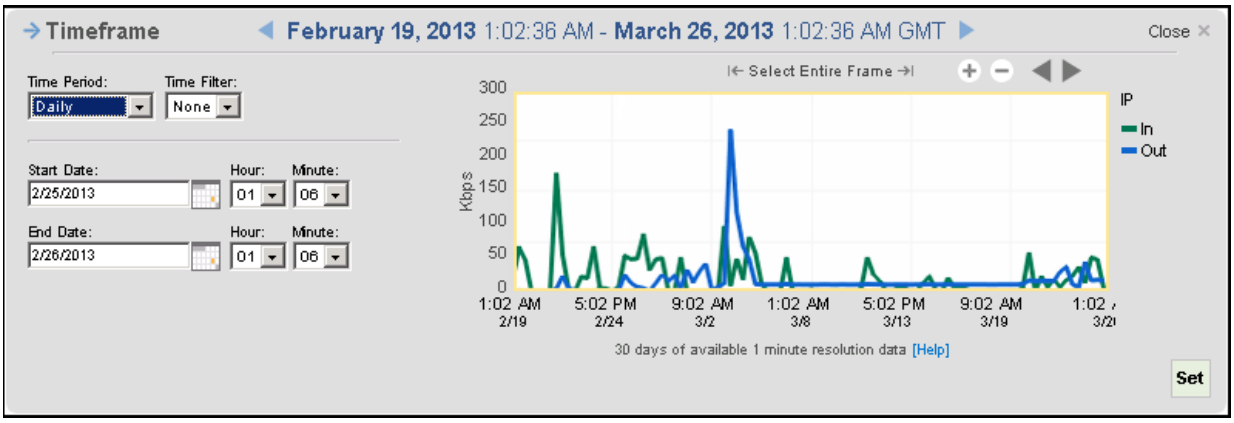
Specify a Built-In Time Period

You can specify a different time period for Interface reports by using one of the built-in options. The built-in time periods let you quickly expand or restrict the reporting time period relative to the current date and time. For example, you can extend the time period to find out if an observed event happens as part of a repeated pattern.

Follow these steps:

1. Click the time period link at the top of the Interfaces report page.

   The Timeframe options expand.



   Note: The time period link is on all top-level Interfaces report pages except Growth and Capacity Planning, which have other time options. In addition, if you drill down to a report page to investigate details, the drilldown report page does not include a time period link.

2. Select a time period for the report from the Time Period list.

   The time period is relative to the current date and time. A Daily time period produces a report about the 24 hours that precede the current date and time. A Weekly time period produces a report the week that precedes the current date and time.

3. Select a time filter from the Time Filter list.

   The available time filters are set up by the Administrator for CA Network Flow Analysis. Time filters limit the time span for reported data, for example to include only regular business hours.

4. Click Set.

   The active time period displayed in the Timeframe pane changes to give you a preview of the data that is included. The preview helps you verify that you are capturing any specific trends that are of interest.

5. Click Close at the top-right corner of the pane.

   The options are hidden.

Specify a Custom Start and End Time

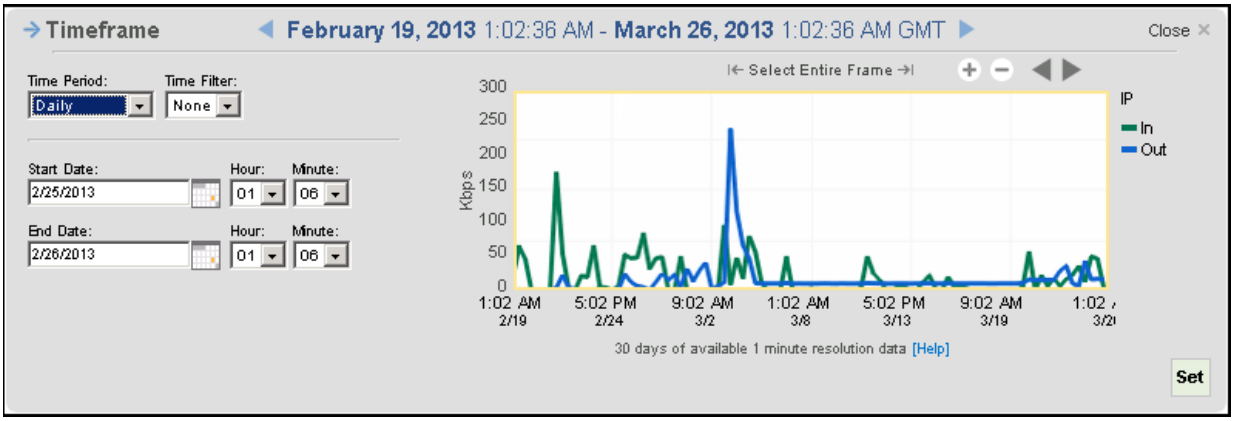
You can customize the time period for the current report. You can select a specific start date, end date, and time of day for collecting report data, such as the following times:

- Specific hour.
- Specific day.
- Unique week time period by specifying a day within the Saturday-to-Sunday 7-day time period that you want.
- Unique one-month time period by selecting the month start and end dates.
- Unique quarter-year time period by selecting the quarter start and end dates.
- Unique one-year time period by selecting the year start and end dates.

Follow these steps:

1. Click the time period at the top of the report page.

   The Timeframe pane expands to display the time period options.



2. Select Custom from the Time Period list. The end date and time are set to the current time by default.

3. Select the start date from the Start Date day, month, and year lists, or click the calendar icon to locate and select a date.
4. Select a start time from the Start Date Hour and Minute lists. The current time (hour:minutes) is selected by default. Hours are shown in 24-hour format.
5. Select an end date from the End Date day, month, and year lists, or click the calendar icon to locate and select a date.
6. Select an end time from the End Date Hour and Minute lists or click the calendar icon to locate and select a date. The current time (hour:minutes) is selected by default.
7. Click Set.

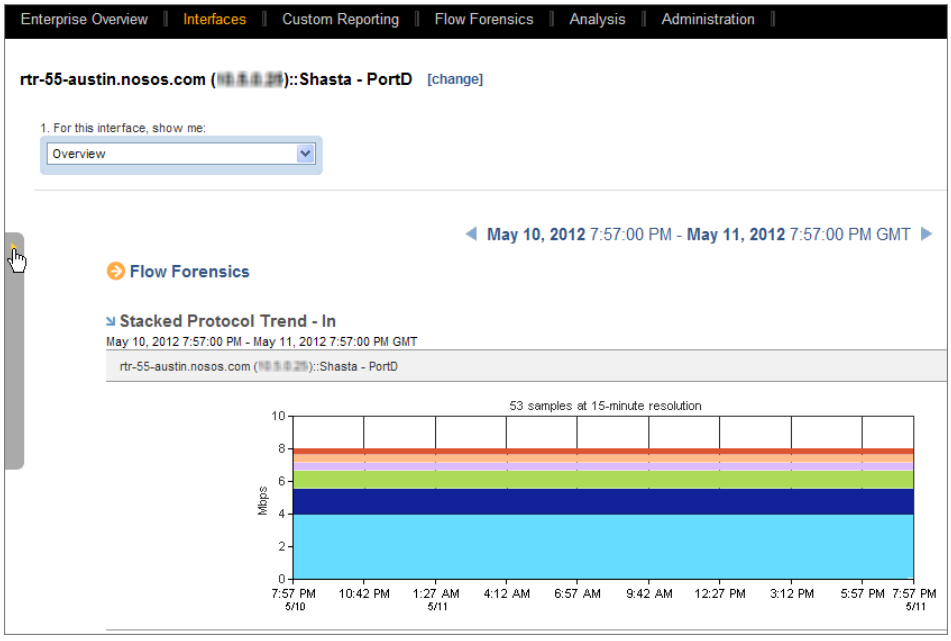
   The preview in the Timeframe pane updates to reflect your changes. This view helps you make sure you are capturing the needed data.
8. Click Close at the top-right corner of the pane.

   The options are hidden.

Set the Presentation Options

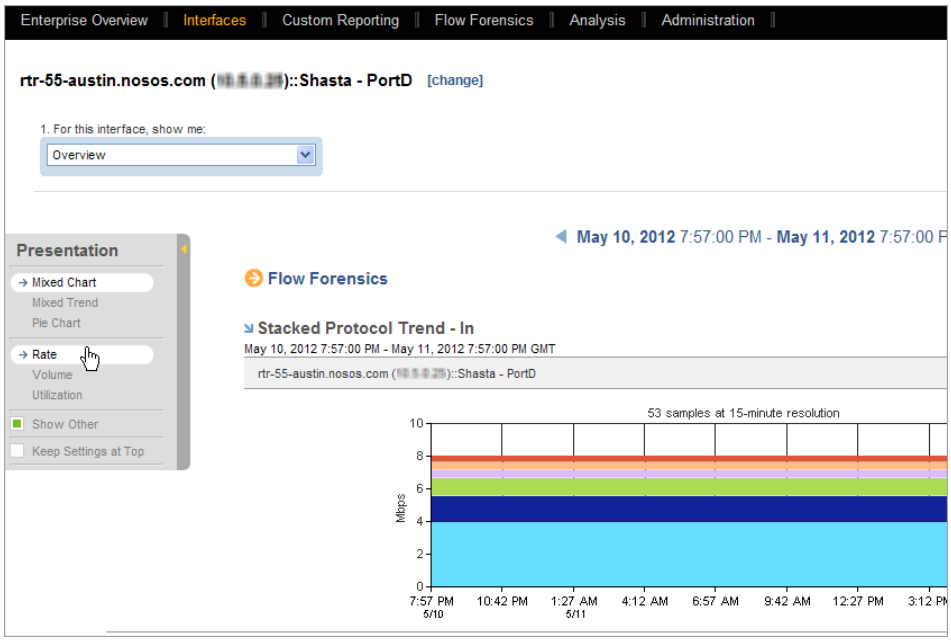
You can use the Presentation menu to choose the way data is presented in a drilldown Interface report.

To open the Presentation menu, click the gray bar on the left edge of the page, as illustrated in the following example.



The Presentation menu opens and gives you access to the options that are appropriate for the selected report type. The display options in the top part of the menu may include a one of the following report types:

- Trend Chart (see page 77)
- Pie Chart (see page 79)
- Summary Table (see page 80)



The selected presentation format determines which metric options are available. For example, if you choose a trend plot as the display type, you can choose rate, volume, or utilization for the metric.

Keep Settings at Top: As you scroll up or down the page, the Presentation menu moves to remain in view by default. To position the Presentation menu in a fixed position at the top of the page, select Keep Settings at Top.

Set the Display Option

Display options determine the presentation of the data in the report views. Each Interface report has a default display type, but you can use the Presentation options to change the display type. The display types that are available depend on the report.

- Stacked Trend Charts (see page 76)
  - Top N Protocols
  - Top N ToS
- Trend Charts (see page 77)
  - Top N Protocols
  - Top N ToS
  - Top N Hosts
  - Top N Conversations
  - Flows
- Mixed Chart (see page 82)
  - Overview
  - Capacity Planning
- Mixed Trend (see page 82)

  Overview
- Pie Charts (see page 79)
  - Overview
  - Top N Protocols
  - Top N ToS
  - Top N Hosts
  - Top N Conversations
- Summary Tables (see page 80)
  - Top N Protocols
  - Top N ToS
  - Top N Hosts
  - Top N Conversations
- Growth (see page 75)

  Growth Report
- Calendar Charts (see page 81)

  Utilization

Set the Rate, Volume, Utilization Option

Interface reports support the display of rate, volume, and utilization metrics. The metrics available for the report depend upon the type of data included in the report, and sometimes the selected display option.

Show Other Option

When you display a Top-N report for protocols, hosts, and conversations, you can include data for items other than the top ten. To include the other items, select the Show Other check box in the Presentation options. The data for the other protocols, hosts, or conversations is then rolled up and assigned a label of Other.

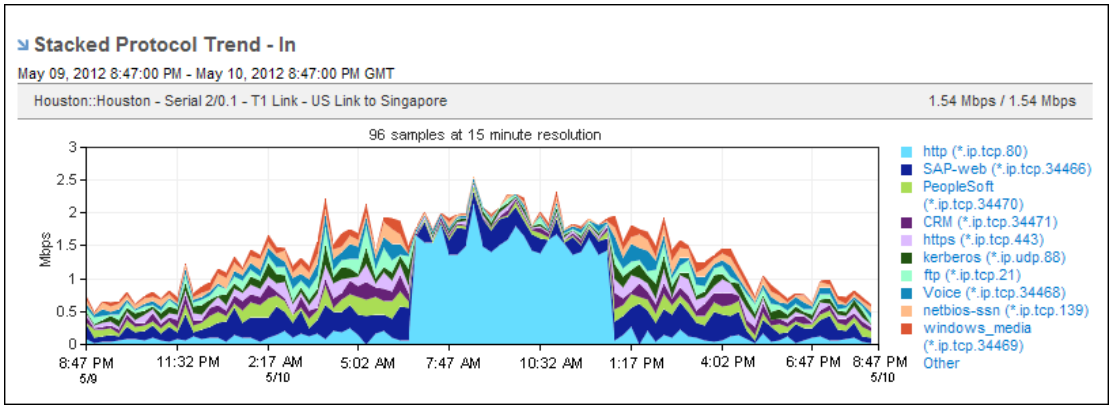
Analyze Interface Report Data

The Interface reports included in CA Network Flow Analysis include numerous view types that are designed to help you identify and analyze your network traffic. These real-time report views provide the previous hour of performance data by default in a 1-minute granularity view. By using this data, operations center personnel can determine possible causes for new issues and can troubleshoot the issues quickly.

Protocol Trend Views

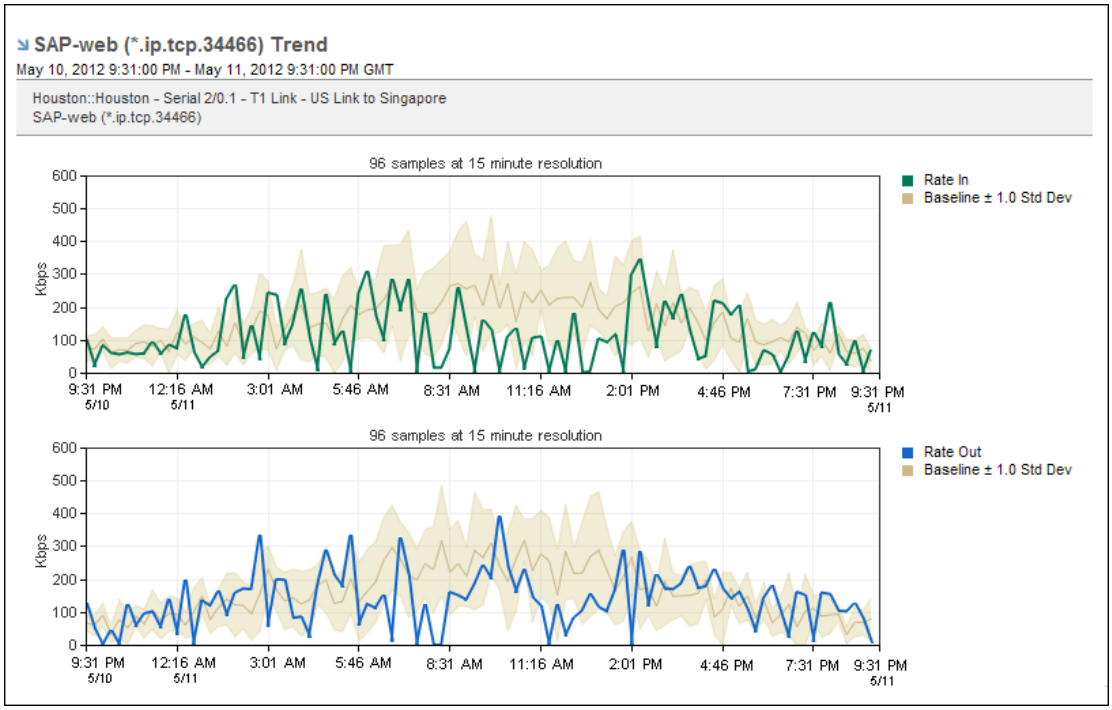
The data in Stacked Protocol Trend views helps you determine which type of traffic is consuming bandwidth on the interface. These views also show the way bandwidth consumption changed over the selected time period.

Click the name of a protocol in the legend to display a protocol report with interface data specific to that protocol.



The Stacked Protocol Trend views display data for the top ten protocols on the interface. To display data for protocols other than the top ten protocols, select Show Other in the Presentation menu. Data for protocols other than the top ten is rolled up and assigned a label of Other.

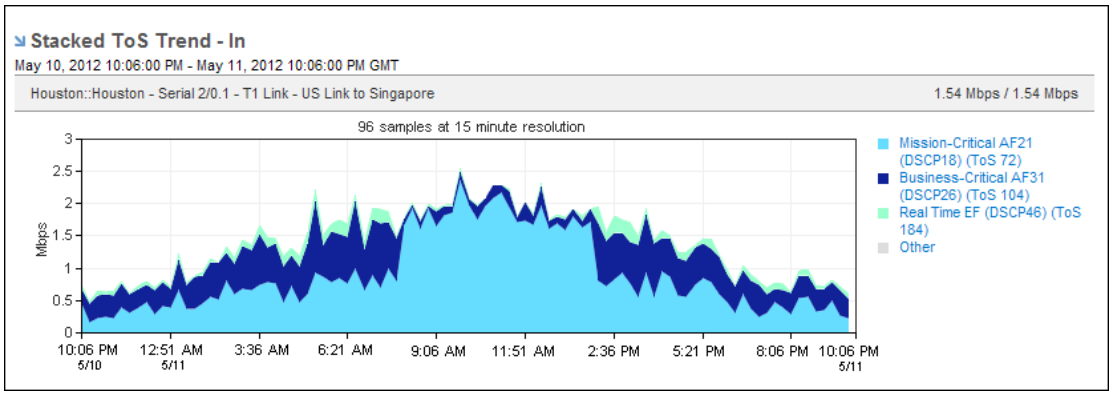
Change the presentation display to a trend chart to display each protocol as an individual trend plot. A trend chart is useful for comparing the protocol data patterns against a baseline.



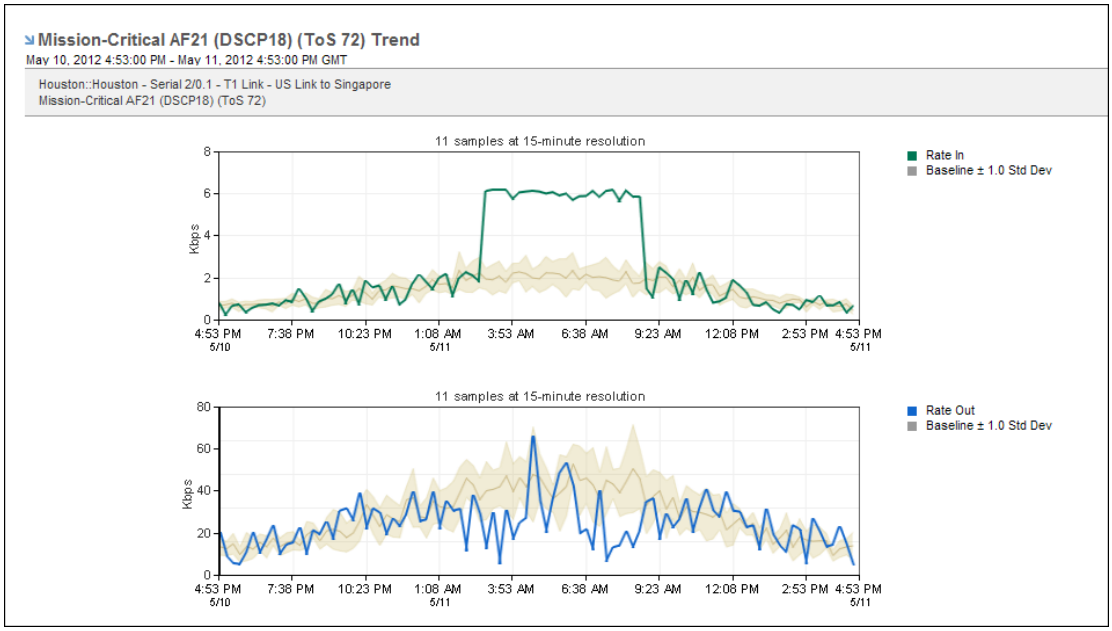
ToS Trend Views

The data in Stacked ToS Trend views helps you determine the amount of traffic on the interface by ToS designation and its change over the selected time period.

Click the name of a ToS in the legend to display the ToS report with interface data specific to that ToS.

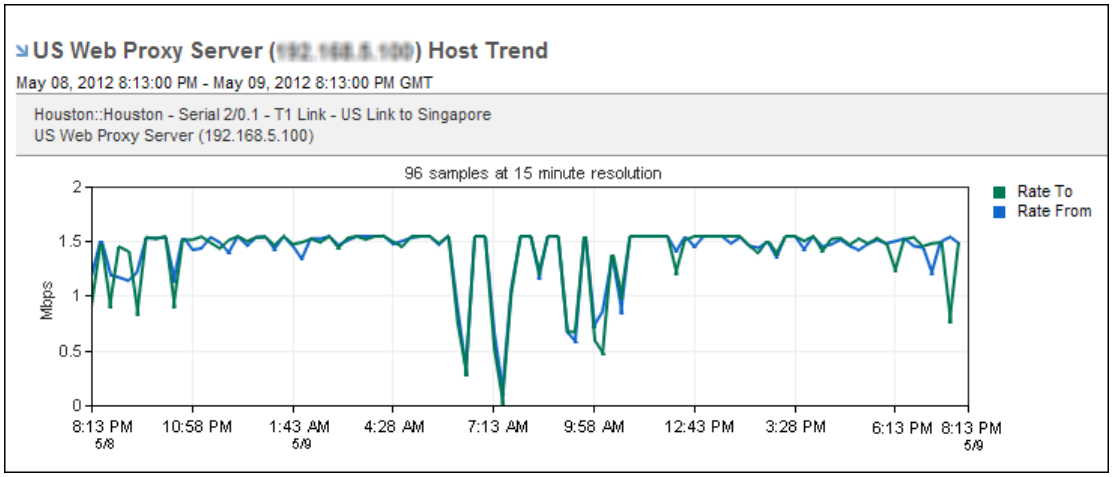


Change the presentation display to a trend chart to display each ToS as an individual trend plot. A trend chart is useful for comparing the ToS data patterns against a baseline.



Host Trend Views

Host data views are displayed as summary views (pie chart or summary table) by default. You can view individual trend plots for each of the hosts on the selected interface. To view individual trend plots, select the Trend Chart display type in the Presentation options for the Top-N Hosts report.

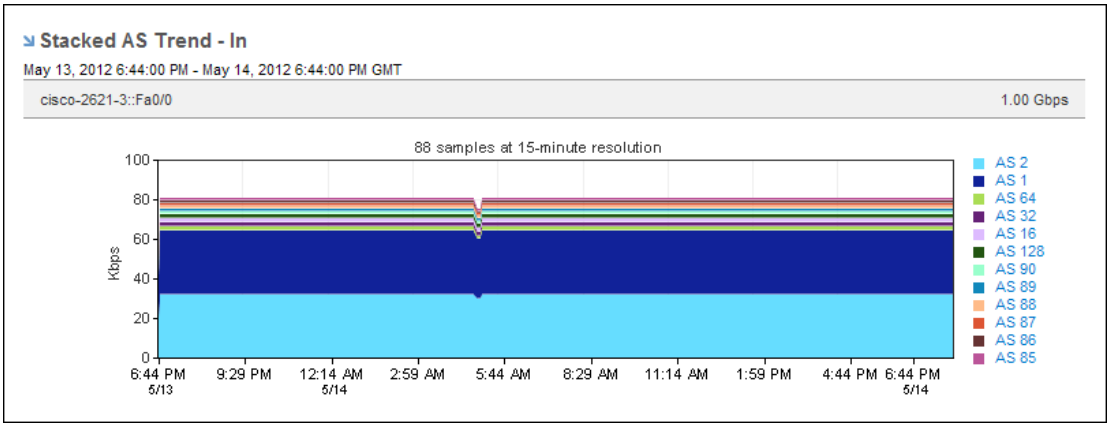


Host trend charts plot a line for each direction of the host traffic on the interface.

AS Number Trend Views

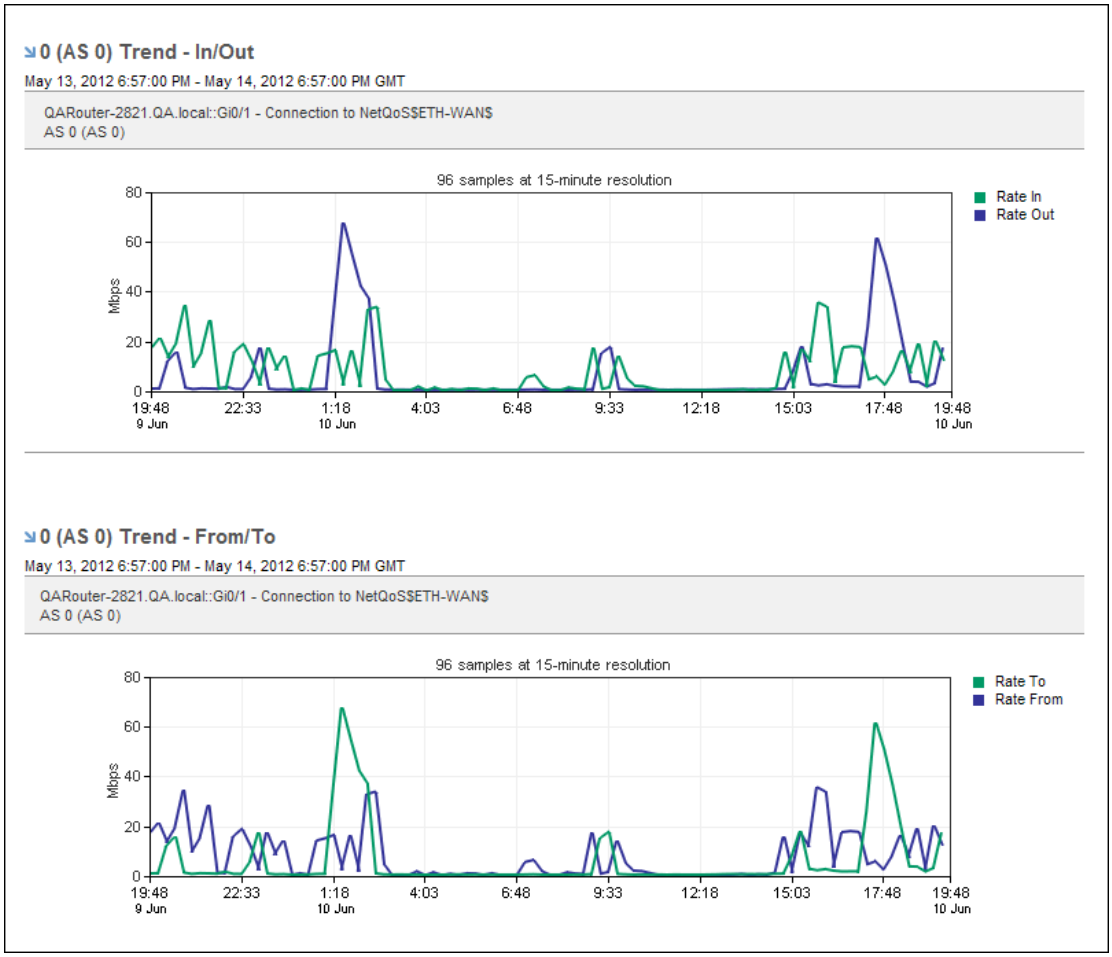
The data in the Stacked AS Trend views helps you determine the usage of numbered routes in a network. Use this AS (Autonomous System) Next Hop data to troubleshoot issues.

Click the name of an AS number in the legend to display an AS Next Hop Summary Table specific to that AS number.



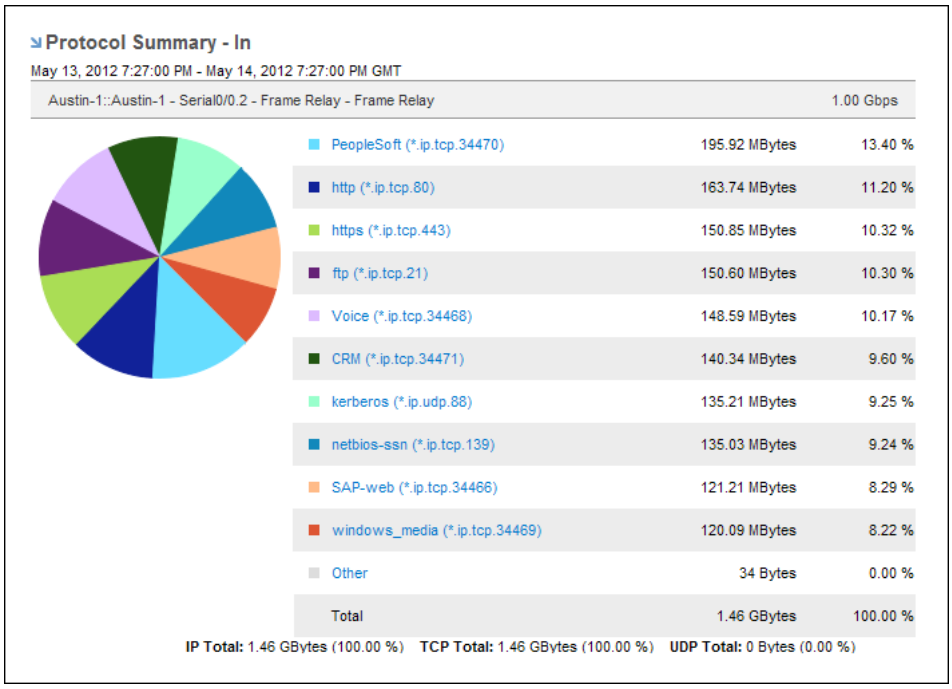
The Stacked AS Trend views display data for the top 10 AS numbers on the interface. To display data for AS numbers other than the top ten, select Show Other in the Presentation menu. Data for AS numbers other than the top ten is rolled up and assigned a label of Other.

Change the presentation display to a trend chart to display each AS number as an individual trend plot. A trend chart is useful for comparing the inbound and outbound AS number data patterns.



Protocol Summary Views

The Protocol Summary views can help you determine which protocols produce the most traffic over the interface during the selected time period. These views are an overview and provide a good starting point for troubleshooting issues.



Protocol Summary - In

May 13, 2012 7:27:00 PM - May 14, 2012 7:27:00 PM GMT

Austin-1::Austin-1 - Serial0/0.2 - Frame Relay - Frame Relay		1.00 Gbps
PeopleSoft (*.ip.tcp.34470)	195.92 MBytes	13.40 %
http (*.ip.tcp.80)	163.74 MBytes	11.20 %
https (*.ip.tcp.443)	150.85 MBytes	10.32 %
ftp (*.ip.tcp.21)	150.60 MBytes	10.30 %
Voice (*.ip.tcp.34468)	148.59 MBytes	10.17 %
CRM (*.ip.tcp.34471)	140.34 MBytes	9.60 %
kerberos (*.ip.udp.88)	135.21 MBytes	9.25 %
netbios-ssn (*.ip.tcp.139)	135.03 MBytes	9.24 %
SAP-web (*.ip.tcp.34466)	121.21 MBytes	8.29 %
windows_media (*.ip.tcp.34469)	120.09 MBytes	8.22 %
Other	34 Bytes	0.00 %
Total	1.46 GBytes	100.00 %

IP Total: 1.46 GBytes (100.00 %) **TCP Total:** 1.46 GBytes (100.00 %) **UDP Total:** 0 Bytes (0.00 %)

Protocol Summary views are included on Interface pages for specific interfaces when the selected report type is Overview or Protocols, the protocol range is Top N Protocols, and the Presentation mode is Pie Chart.

You also can include Protocol Summary views in Custom Reports.

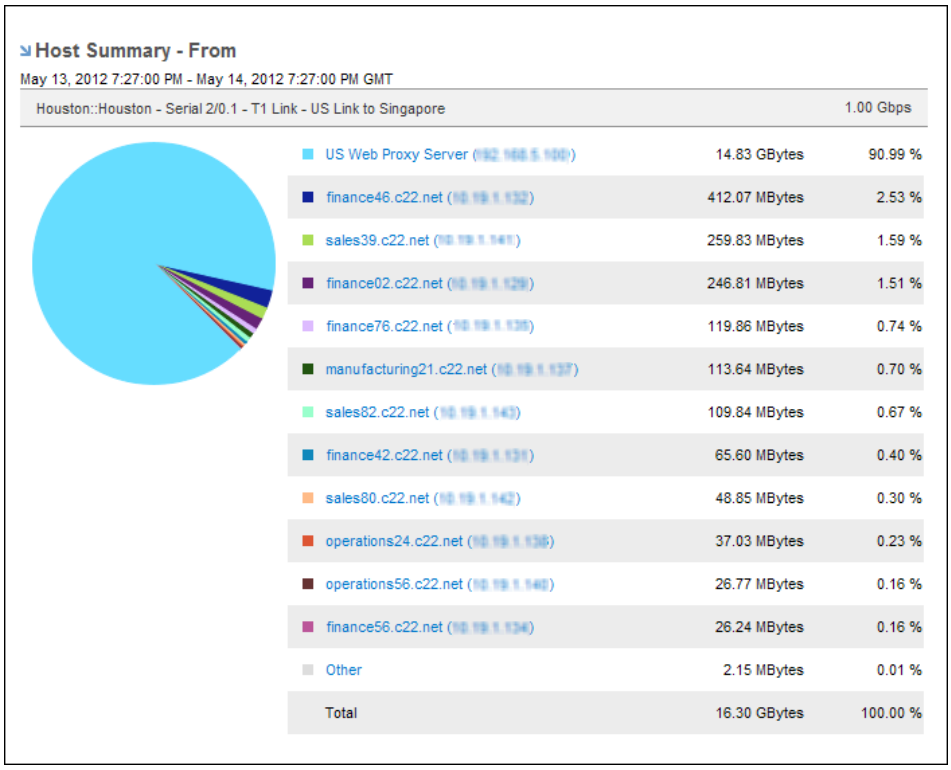
You can display Top N Protocols information on Interface pages in the following presentation modes:

- Pie charts of protocol summary data on Overview reports (inbound and outbound traffic) and Protocols report pages (inbound, outbound, and all traffic).
- Stacked trend charts of rate, volume, or utilization data on Overview and Protocols reports.
- Trend charts of rate, volume, or utilization data on Protocols reports.
- Summary tables of rate, volume, or utilization data on Protocols reports.

Host Summary Views

The Host Summary views can help determine which hosts have the highest traffic volume over the interface during a time period. Access to detailed host information helps pinpoint traffic sources and quickly determine whether traffic is normal. You may be able to resolve a problem quickly because you know which hosts are responsible.

Click the name of a host in a view to display the Hosts report with interface data that is specific to the host.



Host Summary views are included on Interface pages for specific interfaces when the selected report type is Overview or Hosts, the host range is Top N Hosts, and the Presentation mode is Pie Chart or Mixed Chart.

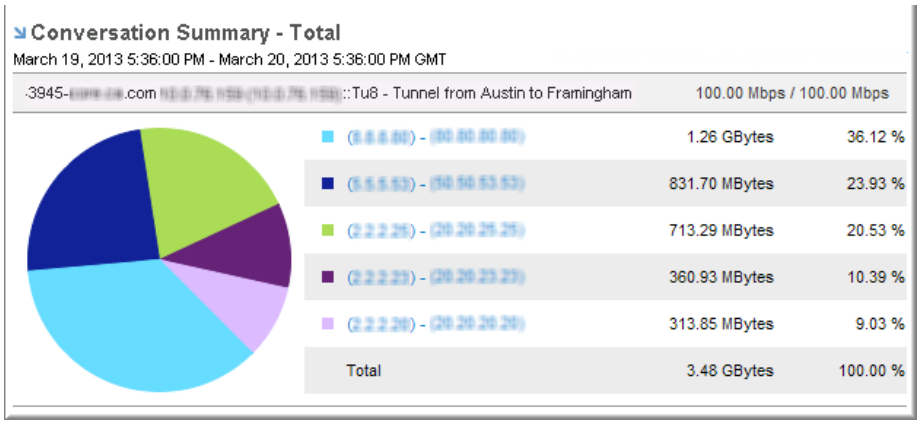
You also can include Host Summary views in Custom Reports.

You can display Top N Hosts information on Interface pages in the following presentation modes:

- Pie charts of host summary data on Overview reports (traffic from the host and to the host) and Hosts report pages (traffic from the host, traffic to the host, and all traffic).
- Trend charts of rate, volume, or utilization host data on Overview or Hosts reports.
- Summary tables of rate, volume, or utilization host data on Hosts reports. The data in a summary table provides additional data for the hosts, including Maximum To/From and Average To/From values.

Conversation Summary Views

The data displayed in the Conversation Summary views is designed to help you determine the conversations with the most volume of traffic over the interface during the selected time period. Use this information to troubleshoot issues and determine if there is a saturation issue or an area of poor performance.

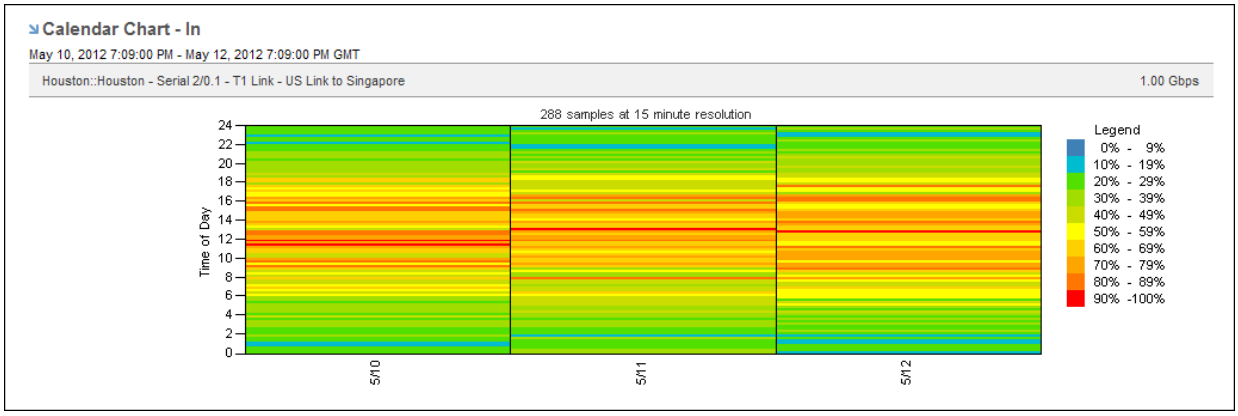


Click the name of a conversation in the view to display the Conversations report with interface data specific to that conversation.

These views display data for the top ten conversations on the interface by default. To display data for other conversations, select Show Other in the Presentation menu. Data for conversations other than the top ten is rolled up and assigned a label of Other.

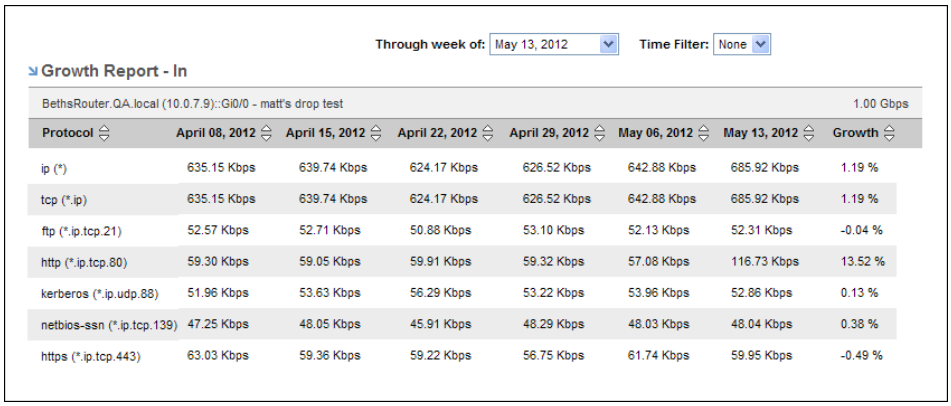
Utilization Calendar Charts

The Calendar Chart helps you detect utilization issues on an interface, determine when the problem started, and pinpoint the time of day the problem occurs. In the example chart, you can see that the utilization level for this interface is often at or above 70 percent. The high utilization level means that the performance of the applications sending data over this link is likely to be degraded at those times. Calendar Charts can also reveal patterns from day to day and from week to week so that you can determine whether a problem regularly occurs at a particular time.



Growth Reports

The Growth Report includes a specialized summary table. The table helps to identify applications that consume increasing amounts of bandwidth over time. You also can use the table data to determine whether future growth requires additional capacity. Display data for the previous six weeks or the previous six months and apply any available time filters. You can choose the units to display (such as bits per second) and whether to include inbound traffic, outbound traffic, or all traffic.



Protocol	April 08, 2012	April 15, 2012	April 22, 2012	April 29, 2012	May 06, 2012	May 13, 2012	Growth
ip (*)	635.15 Kbps	639.74 Kbps	624.17 Kbps	626.52 Kbps	642.88 Kbps	685.92 Kbps	1.19 %
tcp (*.ip)	635.15 Kbps	639.74 Kbps	624.17 Kbps	626.52 Kbps	642.88 Kbps	685.92 Kbps	1.19 %
ftp (*.ip.tcp.21)	52.57 Kbps	52.71 Kbps	50.88 Kbps	53.10 Kbps	52.13 Kbps	52.31 Kbps	-0.04 %
http (*.ip.tcp.80)	59.30 Kbps	59.05 Kbps	59.91 Kbps	59.32 Kbps	57.08 Kbps	116.73 Kbps	13.52 %
kerberos (*.ip.udp.88)	51.96 Kbps	53.63 Kbps	56.29 Kbps	53.22 Kbps	53.96 Kbps	52.86 Kbps	0.13 %
netbios-ssn (*.ip.tcp.139)	47.25 Kbps	48.05 Kbps	45.91 Kbps	48.29 Kbps	48.03 Kbps	48.04 Kbps	0.38 %
https (*.ip.tcp.443)	63.03 Kbps	59.36 Kbps	59.22 Kbps	56.75 Kbps	61.74 Kbps	59.95 Kbps	-0.49 %

By default, the table is sorted by the total rate of the most recent week. You can sort according to any column by clicking a column heading. You also can change from descending to ascending order by clicking the triangle next to the column heading.

Display Charts and Graphs

When you view information about a specific interface, host, conversation, or protocol, several types of report presentations are available for displaying the data such as charts, graphs, and tables. Each report type is suited to particular data types and situations.

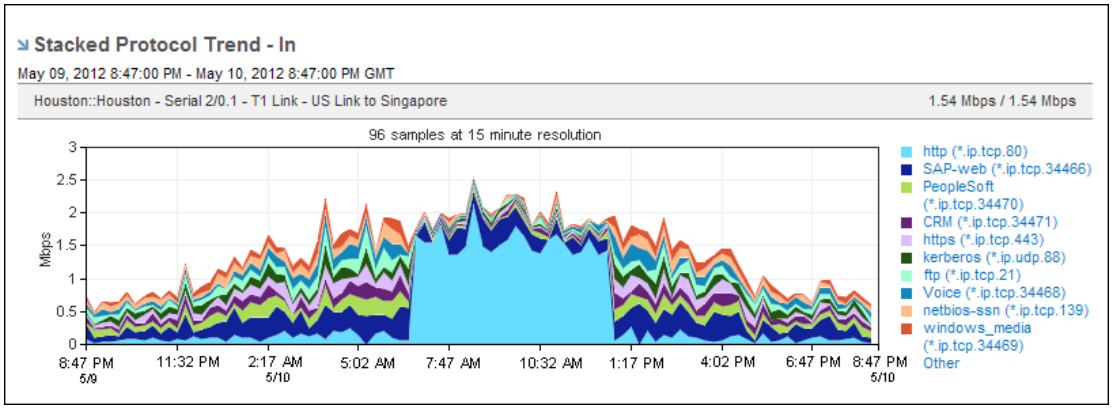
This section contains the following topics:

Stacked Trend Charts (see page 76)
Trend Charts (see page 77)
Pie Charts (see page 79)
Summary Tables (see page 80)
Calendar Charts (see page 81)
Mixed Display Options (see page 82)

Stacked Trend Charts

The stacked trend plots for Protocol and ToS summary data are excellent for establishing the types of applications that use the most bandwidth for a particular interface. Stacked trend plots also help you compare the use of each application with others.

The legend on the right of the stacked trend chart lists the protocols or ToS values so you can see the amount of data that is transferred for each category. In the example, notice the surge of inbound web (http) traffic.



The example report duration is daily. You might want to change the duration to monthly to determine whether the surge is a one-time occurrence or occurs regularly at a particular time. By default, views and reports show the most recent 24 hours of data. To change the time period or apply a time filter, use the Timeframe options.

See Also:

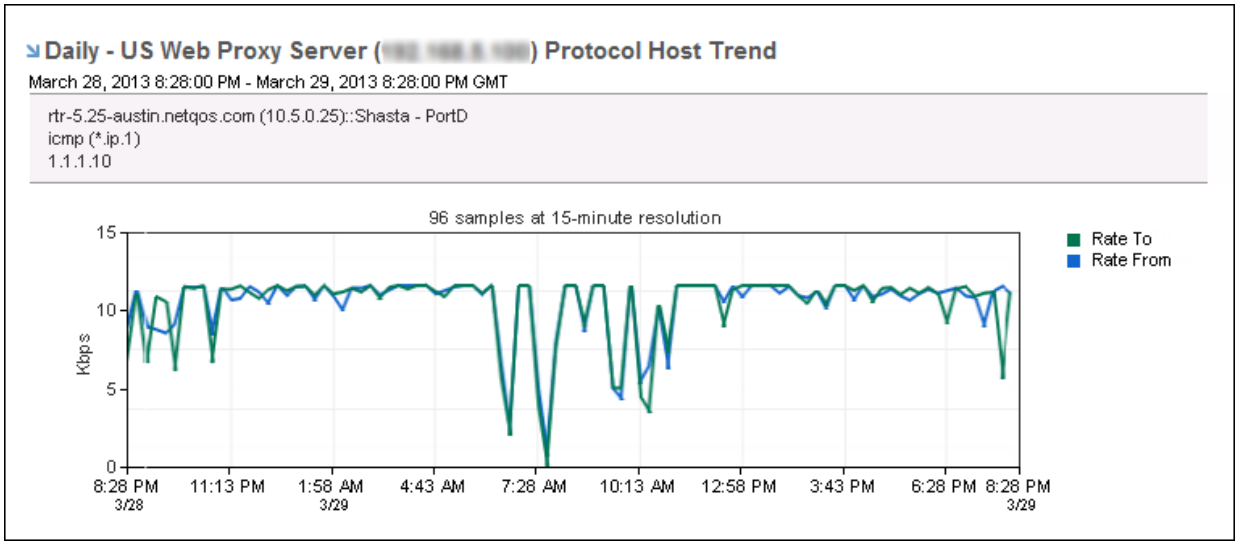
Set the Time Period for a Report (see page 61)

Trend Charts

The trend chart presentation format is available for interface data that is filtered by Protocol, ToS, Hosts, and Conversations. When you choose the trend chart presentation for a Protocol Summary, trend plots are shown for each of the top protocols.

Use trend charts to see traffic spikes and dips and to determine whether those patterns are consistent with your expectations for the interface. Click the name of a protocol, host, or conversation to view a more detailed trend chart.

By default, views and reports show the most recent 24 hours of data. To change the time period or apply a time filter, use the Timeframe options.



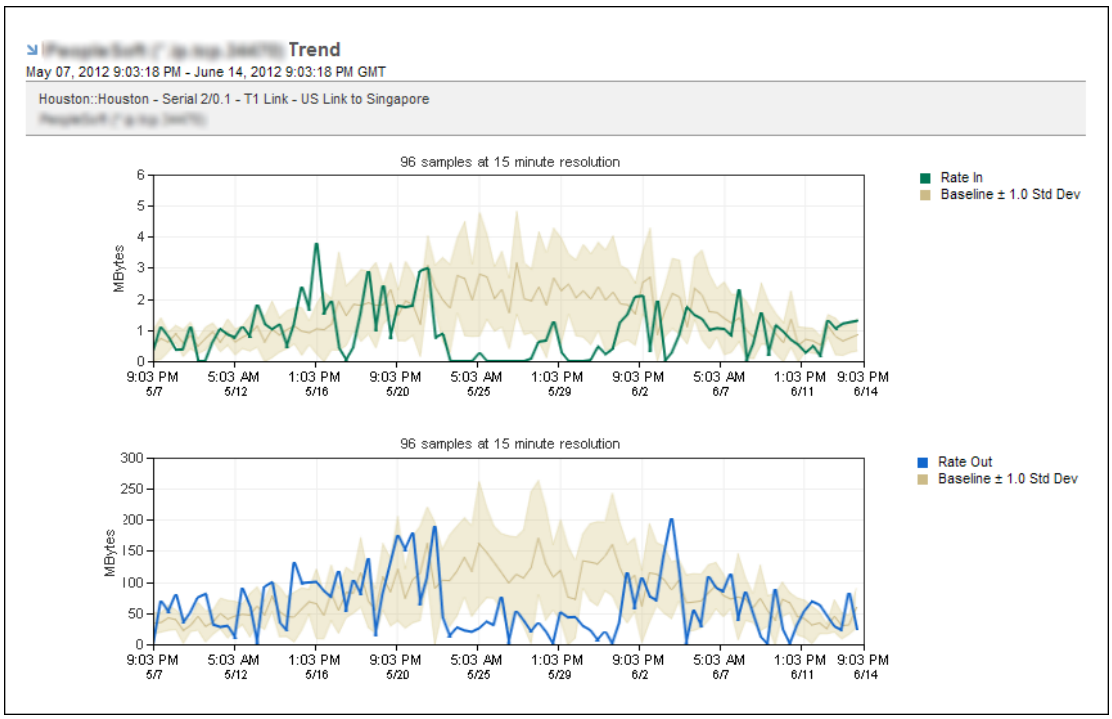
The preceding example shows a trend chart on the Interface page with the following settings:

- Report type: Protocols
- Protocol range: Specific protocol
- Report subtype: Hosts
- Hosts range: Top N Hosts
- Presentation type: Trend Chart
- Measurement type: Rate

Baselines

Protocol data views also support baselines for trend plots of some protocol, ToS and flow views. To display baselines, choose from the following settings:

- Protocols report type, Top N Protocols range, Trend Chart presentation type, Show Baselines option selected.
- ToS report type, Top N ToS range, Trend Chart presentation type, Show Baselines option selected.
- Flows report type, Show Baselines option selected.



The preceding example shows trend plots on the Interfaces page with the following settings:

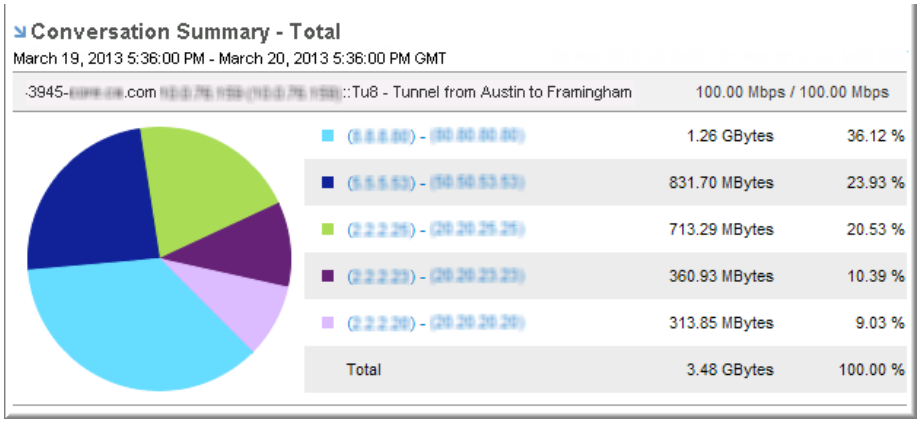
- Report type: Protocols
- Protocol range: Top N Protocols or a specific protocol with Overview as the report subtype
- Presentation type: Trend Chart or Mixed Chart
- Measurement type: Rate
- Show Baselines: Selected

See Also:

Set the Time Period for a Report (see page 61)

Pie Charts

Pie charts provide a visual comparison of the protocols, ToS, hosts, or conversations on the interface, making it easy to see which ones use the most or least amount of bandwidth. Pie charts also include a listing of numeric data.



By default, views and reports show the most recent 24 hours of data. To change the time period or apply a time filter, use the Timeframe options.

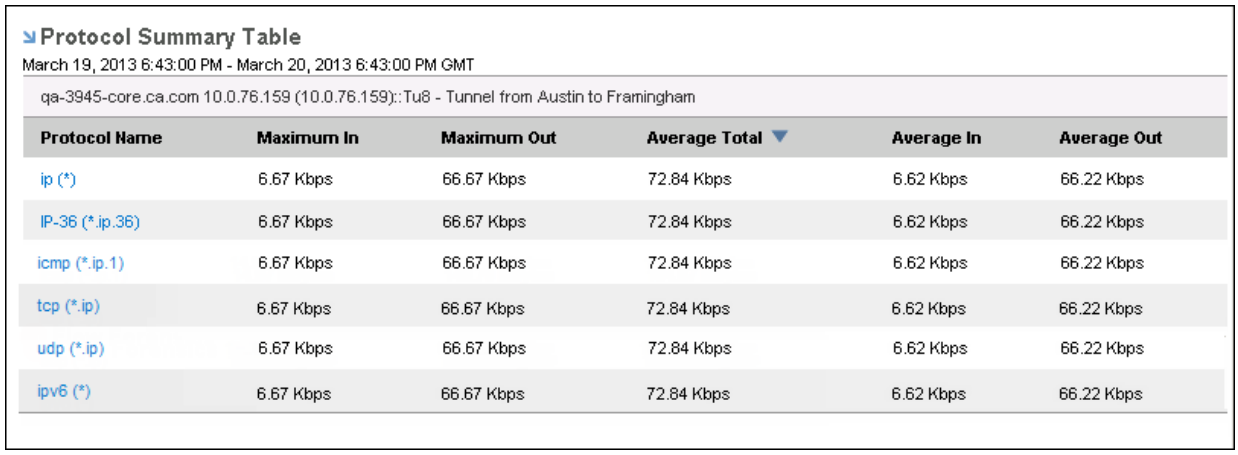
See Also:

Set the Time Period for a Report (see page 61)

Summary Tables

A summary table is a good presentation choice when you want Protocol or ToS summary data that can be easily sorted and saved to CSV format for use in a spreadsheet program. Summary tables are available for the following Top N report types on Interface pages: Protocols, ToS, Hosts, Conversations, and AS Numbers.

In the following example, the Protocol Summary Table lists protocols from the highest to lowest flow volume. You can change the sort order of the list by clicking a column name. Click again to change the order from ascending to descending. The sort column is marked with an arrow.



Protocol Summary Table

March 19, 2013 6:43:00 PM - March 20, 2013 6:43:00 PM GMT

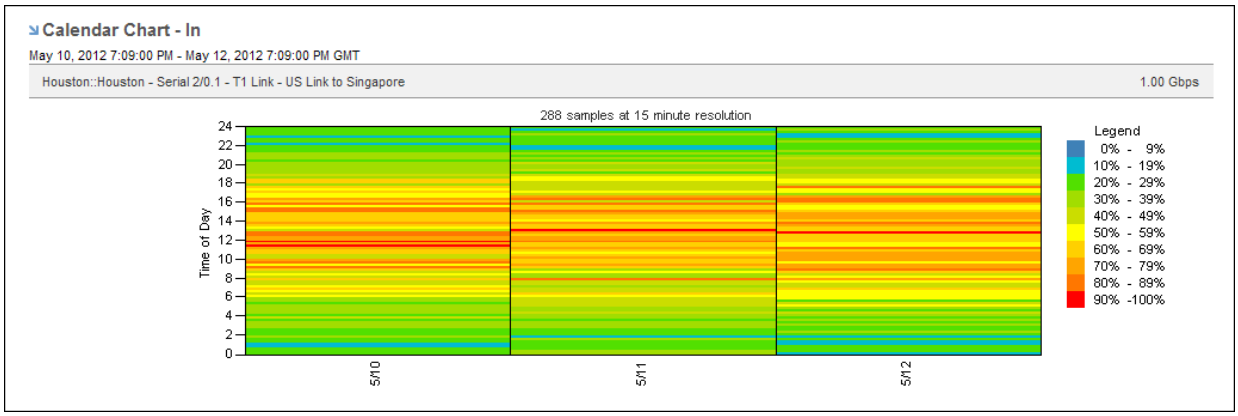
qa-3945-core.ca.com 10.0.76.159 (10.0.76.159)::Tu8 - Tunnel from Austin to Framingham

Protocol Name	Maximum In	Maximum Out	Average Total ▼	Average In	Average Out
ip (*)	6.67 Kbps	66.67 Kbps	72.84 Kbps	6.62 Kbps	66.22 Kbps
IP-36 (*.ip.36)	6.67 Kbps	66.67 Kbps	72.84 Kbps	6.62 Kbps	66.22 Kbps
icmp (*.ip.1)	6.67 Kbps	66.67 Kbps	72.84 Kbps	6.62 Kbps	66.22 Kbps
tcp (*.ip)	6.67 Kbps	66.67 Kbps	72.84 Kbps	6.62 Kbps	66.22 Kbps
udp (*.ip)	6.67 Kbps	66.67 Kbps	72.84 Kbps	6.62 Kbps	66.22 Kbps
ipv6 (*)	6.67 Kbps	66.67 Kbps	72.84 Kbps	6.62 Kbps	66.22 Kbps

Calendar Charts

When you choose to view Utilization summary data for an interface, the data is displayed as a calendar chart. You can show inbound, outbound, or total traffic in the chart, choose the month to display, and apply any available time filters.

Excessive utilization of an interface is shown as a block of red extending across the column for the day and rows indicating the time of day. Low utilization is shown in green. Varying shades of each color show the severity degree. The color for each severity range corresponds to a range of utilization values (calculated as percentages of total capacity). The legend explains how the colors are used in the calendar chart.



The calendar chart helps you detect utilization problems with the selected interface, determine when the problem started, and pinpoint the time of day the problem occurs. In the example, the interface utilization level is often at or above 70 percent. The high utilization level means that the performance of the applications sending data over this link is likely to be degraded at those times. Calendar charts can also reveal patterns from day to day and week to week so that you can determine whether a problem occurs regularly at a particular time.

Mixed Display Options

The Interface Overview report has additional presentation display types to accommodate a wider array of data--protocol, ToS, host, and conversation data. By using one of the mixed presentation types, you can view the report with the most useful presentation for each report view.

Mixed Chart

When the Mixed Chart is selected in the Presentation options, the report page displays both stacked trend and pie charts. Protocol and ToS data is presented using stacked trend charts. Host and conversation data is presented using pie charts.

Mixed Trend

When the Mixed Trend is selected in the Presentation options, the report page displays both stacked trend and trend charts. Protocol and ToS data is presented using stacked trend charts. Host and conversation data is presented using standard trend charts.

Chapter 4: Custom Reports

Custom Reports can answer specific technical and business questions in your environment, such as the following questions:

- Which applications are used most heavily in the regional offices?
- What is the total volume of traffic for global operations?
- Does the new data center have the capacity to handle additional servers?

To get started, select Custom Reporting from the NFA console menu.

The Create New Report page opens, which lists the existing reports. If you have the required permissions, the page contains functions for creating, managing, and running Custom Reports. You can generate updated versions of reports, add new report definitions, and change report settings.

The Create New Report page includes the following functions:

Saved Report Folders:

- *New:* Create a report folder.
- *Rename:* Change the name of a report folder.

Reports:

- *New:* Create a Custom Report definition.
- *Run:* Regenerate the data for one or more Custom Reports.
- *Move to Folder:* Change the parent folder for one or more report definitions.
- *Cancel:* Stop one or more reports from running.

This section contains the following topics:

Report Types and Usage (see page 84)
Set Up Custom Reports (see page 85)
Manage Custom Reports (see page 107)

Report Types and Usage

Custom Reports can show a variety of data, including the following types of information:

- *Interface:* View the total volume of traffic that is generated across particular interfaces.
- *Protocol:* Discover which applications are used by various business groups.
- *ToS:* View the distribution of applications by type of service (ToS).
- *Host:* View the activity or usage levels for applications on a server.
- *Conversation:* View the top conversations across interfaces or for a particular protocol.

Report on Network Utilization

Create a custom interface report to select the included interfaces so that you can report on network traffic by:

- Location, such as global, regional, country, state, and individual offices
- Business unit or department, such as Accounting, Marketing, and Sales
- Specific interface groups, such as EMEA, WAN, ATM interfaces, and Ethernet interfaces

Report on Application Distribution

Create a custom protocol report to focus on the applications and protocols in use in your organization. You can generate protocol distribution reports to:

- Show the applications that are used in each region.
- Understand which applications are used the most frequently.
- Determine whether any applications can be removed from the network or de-prioritized.
- Verify that rogue applications are not active on the network.

Report on ToS Distribution

Create a custom ToS report to identify the ToS categories for the most heavily utilized applications in your environment. You can generate ToS reports to:

- Understand which ToS is most widely used in your environment.
- Show the ToS categories in use in each regional location.

Report on Server Activity

Create a custom host report to identify the amount of traffic sent to and from particular servers in your organization. You can generate host reports to:

- Verify that application servers are utilized properly.
- Determine whether a server is vulnerable to any security risks.
- Determine whether a specific data center can handle additional servers.

Set Up Custom Reports

Depending on your user account settings, you may be able to perform a number of actions for Custom Reports:

- View existing reports that have been run.
- Run existing report definitions on demand.
- Set up a schedule for running and sending reports by email (Typically for Administrators and Power Users only).
- Create a Custom Report by stepping through the Custom Report wizard.
- Create a Custom Report by using an existing report as a starting point.
- Make changes to the following parts of an existing report definition:
  - Report name, parent folder, and description
  - Report summary types: interface, ToS, protocol, host, and conversation
  - Presentation views used for the summary data
  - Reporting period, data resolution, and time filter
  - Report recurrence schedule and email recipients
- Set the following elements to be included or excluded as report data sources:
  - Interfaces or interface groups
  - Protocols and ToS values
  - A host and subnet
  - A conversation
  - A subnet mask for aggregating data

This section contains the following topics:

Create a Custom Report (see page 86)
Review Settings for Custom Reports (see page 90)
Customize Which Interfaces Are in Custom Reports (see page 91)
Specify Custom Report Filters (see page 95)
Define Custom Report Periods and Schedules (see page 103)
View Custom Reports (see page 106)

Create a Custom Report

Use the Custom Report wizard to create a Custom Report step by step. The wizard guides you to select many options, such as the specific items on which to report, the presentation views, the reporting period, and, optionally, a schedule for running the report automatically.

Follow these steps:

1. Select Custom Reporting from the NFA console menu.
2. Click Create New Report.

   The Custom Report wizard opens and shows the options Create a new custom report and Copy an existing report.
3. Click 'Create a new custom report,' and click Next.

   Note: Alternatively, you can select 'Copy an existing report option' and modify an existing report.

   The Select Interfaces page opens.
4. Click one of the following options to select interfaces or interface groups for the report:

   - Add Interface Filter: Select one or more individual interfaces from the Interface Index.
   - Add Interface Group Filter: Select one or more interface groups from the Interface Group Selection list.

   The selected interfaces are added to the interface list.

   See Also: Select Interfaces and Interface Groups (see page 91)
5. Accept the default value or set the Inclusion value for each interface or interface group: 'Include' sets the program to use report data from the interface or group. 'Exclude' sets the program to bypass data from the interface or group.
6. Click Next.

   The Specify Filters & Rollup page opens.

7. (Optional) Specify the settings on the Specify Filters & Rollup page: Specify filters for gathering or excluding report data, then set the Inclusion value for each filter to Include or Exclude:
   - Add Protocol Filter: Select individual protocols from the Protocol Index.
   - Add Protocol Group Filter: Select protocol groups from the Protocol Group Index.
   - Add ToS Filter: Select individual ToS values from the ToS Index.
   - Add ToS Group Filter: Select ToS groups from the ToS Group Index.
   - Add Host Filter: Specify a host IP address and mask.
   - Add Conversation Filter: Identify the IP addresses and mask for each party in the conversation pair.

   See Also: Specify Custom Report Filters (see page 95)
8. Accept the default value or set the Inclusion value for each filter you specified:
   - Include: For each filter listed, use only the data of the listed type. For example, use data from the listed protocol group, but not from other protocol groups.
   - Exclude: For each filter listed, do not use the data of the listed type. For example, do not use data from the listed protocol group, but do use data from other protocol groups.
9. Select at least one type of summary data to make available for display in the report. Your selections make various report sections available in a later wizard page, but do not require you to include them. Select one or more check boxes in the Summary Types section:
   - Interface Summary: For example, view the volume of traffic for particular interfaces.
   - ToS Summary: For example, view the distribution of applications by type of service (ToS).
   - Protocol Summary: For example, view which applications are used by each business group.
   - Host Summary: For example, view the application activity or use levels for a server.
   - Conversation Summary: For example, view a list of the top conversations across interfaces for a particular protocol.
10. (Optional) Specify a mask for rolling up data by subnet, if you specified a host or conversation filter: Click the 'Rollup data using this mask' check box, then select a mask from the list.
11. Click Next.

    The Configure Layout page opens.

12. (Optional) Add one or more report sections to the report page layout:
    - Select a value from the Summary Type list.

      Note: The list of available summary types is limited to the summary types you specified on the previous page.
    - Select a value from the Presentation list and the Measurements list (if you selected the presentation type as Table, Trend Chart, or Stacked Trend Chart).
    - Click Add.

    The new section is added at the end of the report.
13. (Optional) Delete one or more report sections from the report page layout by clicking the X icon next to the section name.
14. (Optional) Re-order the report sections in any of the following ways:
    - Drag and drop the section.
    - Click the Top icon to move the section to the beginning of the report.
    - Delete sections and add them again in the correct order.
15. Click Next.

    The Specify Schedule page opens.
16. Select the type of reporting period from the Period list in the Specify Schedule page:
    - Duration: Limits the reporting period to an amount of time, ending at the time the report runs. Enter the number of time units in the Last box.

      Select a unit of time from the list (days, weeks, months, or years).

      You can set up a schedule for a Duration report or you can run the report on demand.
    - Start and end: Specify a Start date and End date either by using the calendar icons or by selecting hour and time values from the lists. Hour values are expressed in 24-hour format.
17. Enter the number of time units in the Resolution box. Select a value from the list for Start and End.

    A Start-and-End report runs on demand and cannot be set up to run on a schedule.
18. Accept the default setting or enter the number of time units in the Resolution box. Select a unit of time from the list (minutes, hours, days, weeks, months, or years).
19. (Optional) Select a time filter from the list, if your Administrator has created a time filter that is appropriate for your report.

20. (Optional) Select the Schedule check box and specify the following options:
    - Schedule: Select the type from the Schedule list (Daily, Weekly, Monthly, Quarterly, Yearly).
    - Daily: Select the day or days of the week, time of day, and time zone for report generation.
    - Weekly: Select the day of the week, time of day, and time zone for report generation.
    - Monthly: Select either the date or the week in the month and day of the week. Select the time of day, and time zone for report generation.
    - Quarterly: Select a month that ends the first reporting quarter, time of day, and time zone.
    - Yearly: Select a month that ends the first reporting year, time of day, and time zone.
21. (Optional) Enter the email addresses of all the report recipients in the format name@domain. Separate multiple addresses with a comma or semi-colon.

    The options in the Recurrence section are available only if you select 'duration' as the reporting period type.

    See Also: Define Custom Report Periods and Schedules (see page 103)
22. Click Next.

    The Enter Name page opens.
23. Identify the report and its location and click Next:
    - Folder: Accept the default folder or select a different folder to contain the new report.
    - Name: Give the new report a name, which appears in the Reports list.
    - Description: (Optional) Add a description to help identify the report. For example, use the description to identify scheduled reports and to indicate distinguishing features of Duration reports.

    The Summary & Submit page opens.
24. Review the information in the Report Definition Summary.
    - *Save:* Save the report definition and return to the Custom Reporting page.
    - *Save and Queue Report:* Queue the report to run and return to the Custom Reporting page.

Review Settings for Custom Reports

You can review the Report Definition Summary of a Custom Report to ensure that the report definitions are appropriate. From the Report Definition Summary page, you can access the Custom Report Wizard pages and can modify the report.

Follow these steps:

1. Click the name of the report you want to modify in the Reports list on the main Custom Reporting page.

   Note: Select a report that is not currently in execution--a report that does not have the status Running.

2. Display the Report Definition Summary page of the Custom Report wizard, if it is not already open. The steps for displaying the Report Definition Summary are dependent on the status of the report you select:

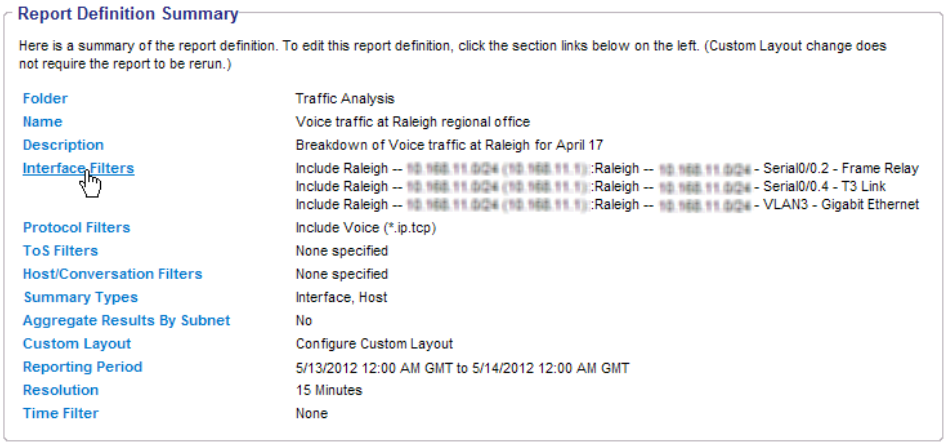
   - Complete: The report runs and opens. Click the Edit button on the left side of the Report Settings section to display the Report Definition Summary.
   - Defined: The Report Definition Summary opens automatically.

3. Review the current report settings and click the name of the section you want to modify.

   For example, click Interface Filters, Protocol Filters, or ToS Filters to add new filters or change existing filter settings.

4. The associated page opens, giving you access to the options that you can change.

   Also See: Set Up Custom Reports (see page 85)



5. When the changes are complete, click Queue Report to regenerate the report with the new settings.

   The Reports list opens and the modified report shows a status of Queued. When the report has been regenerated and is ready to be viewed, the status displays as Complete.

   When you modify a scheduled report, it is queued to be generated at the next scheduled runtime.

Customize Which Interfaces Are in Custom Reports

To define a Custom Report, you must specify at least one interface or interface group to supply data for the report. In the Select Interfaces page of the Custom Report wizard, you can select interfaces from the Interface Index or you can select interfaces by group. When you select an interface group, all interfaces in the group and any child groups are included in the report.

You can save the Custom Report definitions you create and edit existing reports as your reporting needs change. You can delete interfaces or temporarily exclude interfaces from the report.

Select Interfaces and Interface Groups

Before you specify other settings for a new Custom Report, you must add at least one interface or interface group. The Select Interfaces page provides options for specifying individual interfaces and interface groups, which you can use to create useful reports quickly.

Note: Custom groups are defined and managed in CA Performance Center. If CA Network Flow Analysis is not registered as a data source for CA Performance Center, the only available interface groups are the default groups that are defined by type.

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report that you want to change in editable mode: Click the name of the report. If the report has been run previously, it will run again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.

   Note: You can edit a report that appears in the Reports list as long as it has a status other than Running.

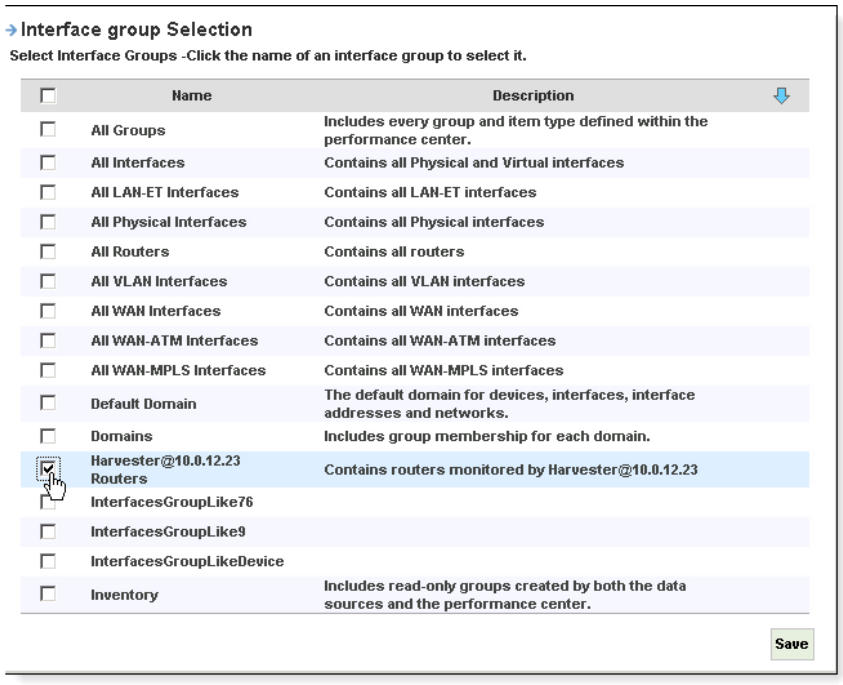
3. (Optional) Click Add Interface Filter and select one or more interfaces to include in the report. You can add individual interfaces, interface groups, or both. You must specify some kind of interface filter, however.

   The Select Interfaces page of the Custom Report wizard opens.

   - Expand the interface list for the desired router, then select the check box for each interface you want to include in the report.
   - Click Submit to add all selected interfaces to the list and close the Interface Index.

4. (Optional) Click Add Interface Group Filter and select one or more interface groups to include in the report. You can add individual interfaces, interface groups, or both. You must specify some kind of interface filter, however.

   The Interface Group Selection page opens.



   - Select check boxes for the groups to add from the Interface Group Selection list.
   - Click the blue arrow near the upper right corner to jump to the bottom of the list, then click Save.

   You return to the Select Interfaces page of the Custom Report wizard. The Select Interfaces list now includes the interfaces and interface groups you selected.

5. Check the list of interfaces and interface groups and their Inclusion values.

   Note: Items that have a value of Include are in the report. You can temporarily remove an interface or interface group from the report by setting the Inclusion value for that item to Exclude.

6. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.

   Note: To save the report definition, you must have at least one interface set to be included.

7. (Optional) Return to the report list by clicking one of these buttons:

   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the current report to run and return to the Custom Reporting page.

Delete Interfaces and Interface Groups

You can delete filters from Custom Report definitions as needed. When you delete interfaces or interface groups from a report definition, those interfaces are not included in the report data.

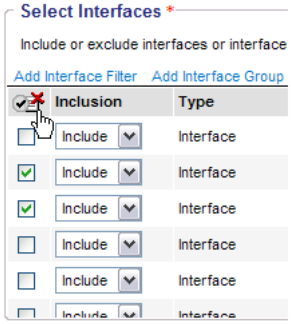
Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.

3. Click Interface Filters to open the Select Interfaces page of the Custom Report wizard.
4. Select the check box in the interface list next to each interface you want to delete.

5. Click the Remove Selected Filters icon that is located above the check boxes.



6. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.

   Note: If you select a scheduled Custom Report that uses a deleted interface or interface group, the "Unknown interface group" message is displayed. If all the associated interfaces or interface groups are deleted, the report will not run.

7. (Optional) Click one of the following buttons to return to the report list:

   - Return to Listing: Return to the report list on the Custom Reporting page.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Exclude Interfaces or Interface Groups Temporarily

To remove interfaces from a report temporarily, set the Include value for the interfaces to Exclude. For example, suppose that part of your network is temporarily offline and the offline interfaces distort the report data. You can exclude the interfaces, then change the value back to 'Include' when the interfaces are online again.

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.

3. Click Interface Filters to open the Select Interfaces page of the Custom Report wizard.
4. In the Select Interfaces list, set the Inclusion option to Exclude.
5. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.

6. (Optional) Check your changes in the summary, then click one of the following buttons to return to the report list:
   - Return to Listing: Return to the report list on the Custom Reporting page.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Specify Custom Report Filters

Use Custom Report filters to determine the type of data to include, such as protocol, ToS, host, and conversation data.

This section contains the following topics:

Available Report Summary Types for Selected Filters (see page 96)
Rules for Utilization Measurements (see page 96)
Add, Delete, or Change Protocol Filters (see page 97)
Add or Modify ToS Filters (see page 98)
Add or Modify Host and Conversation Filters (see page 99)
Delete Custom Report Filters (see page 102)
Exclude Custom Report Filters (see page 102)

Available Report Summary Types for Selected Filters

You can use various filters to limit the data in a Custom Report, but not all filter combinations are valid. For example, you can filter report data to show either hosts or conversations, but not both.

Valid filter combinations are shown in the list that follows. The filter or combination of filters you apply to a report determine which summary types are available, which are also included in the list:

- *No filters:* Interface, ToS, Protocol, Host, and Conversation summaries
- *Protocol filters:* Interface, ToS, Protocol, Host, and Conversation summaries
- *ToS filters:* Interface, ToS, Protocol, Host, and Conversation summaries
- *Protocol and ToS filters:* Interface, ToS, and Protocol summaries
- *Protocol and host filters:* Interface, Protocol, Host, and Conversation summaries
- *Protocol and conversation filters:* Interface, Protocol, Host, and Conversation summaries
- *ToS and conversation filters:* Interface, ToS, Host, and Conversation summaries
- *ToS and host filters:* Interface, ToS, Host, and Conversation summaries
- *Conversation filters:* Interface, ToS, Protocol, Host, and Conversation summaries
- *Host filters:* Interface, ToS, Protocol, Host, and Conversation summaries

Rules for Utilization Measurements

The following rules apply to utilization measurements:

- Inbound and outbound interface speeds must be set.
- Utilization is applicable only for interface, ToS, and protocol views and for data that has no host or conversation filter applied.
- Protocol or ToS utilization is limited to a single interface.
- Total utilization is not available.

Add, Delete, or Change Protocol Filters

You can add a protocol filter to include report data for the protocols defined in your CA Network Flow Analysis installation.

You can add a protocol group filter to restrict reported data to one or more protocol groups. Protocol groups are useful for streamlining Custom Report definitions. For example, protocol groups can help users easily report on network traffic that custom applications generate. The Administrator can create a group for each of the applications that includes the range of ports that are used for the application. Users can also choose from the default protocol groups that are provided automatically.

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.
3. Click Protocol Filters to open the Specify Filters & Rollup page of the Custom Report wizard.
4. (Optional) Select one or more individual protocols to include: Click Add Protocol Filter

   The Protocol Index dialog opens.

   - (Optional) Select the display mode for the protocols from the 'Select by' list:
     - Protocol Name: View the protocols groups by name, either divided into alphabetized lists or displayed together in the All list (Default setting).
     - Port Number: View the protocols in groups by port number. Click the arrows to expand the contents of individual port number groups or click Expand All to show the contents of all groups.
     - Show: Set the view to include TCP Ports, UDP Ports, or TCP & UDP Ports, when the 'Select by' is Port Number.
   - Locate and select the protocols in the protocol lists.

     To use a protocol that is not listed, add the protocol to the list: Click Add Protocol, then use the Add Protocol dialog to specify the new protocol name, port, type, and description.

     For more information about adding protocols, see the *CA Network Flow Analysis Administrator Guide.*
   - Click Submit. To locate the Submit button quickly, click the blue arrow to jump to the bottom of the page.

5. (Optional) Select one or more protocol groups to include: Click Add Protocol Group Filter

   The Protocol Group Index dialog opens.

   - Select check boxes for the protocol groups to add from the list.
   - Click Submit. To locate the Submit button quickly, click the blue arrow to jump to the bottom of the page.

   You return to the Select Filters & Rollup page of the Custom Report wizard.

6. Check the list of filters and their Inclusion values.

   Items that have a value of 'Include' are in the report. You can remove data for a protocol or protocol group temporarily by setting the Inclusion value for the item to 'Exclude.'

7. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.

8. (Optional) Return to the report list by clicking one of these buttons:

   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Add or Modify ToS Filters

You can add ToS filters or ToS group filters to restrict report data. You can filter for individual ToS values, use any ToS groups your Administrator has created, or use the default ToS group, All ToS.

ToS groups are useful for creating Custom Reports for specific classes of applications. For example, suppose that you want to watch applications that your IT department has classified as Gold Class applications. To facilitate reports on Gold Class applications, the Administrator creates a ToS group that includes the ToS values for those applications.

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.

3. Click ToS Filters.
4. The Specify Filters & Rollup page of the Custom Report wizard opens.

5. (Optional) Select one or more individual ToS values to include: Click Add ToS Filter

   The Protocol Index dialog opens.

   - Select the check box for each ToS value you want to include.
   - Click Submit. To locate the Submit button quickly, click the blue arrow to jump to the bottom of the page.

6. (Optional) Select one or more ToS groups to include: Click Add ToS Group Filter

   The ToS Group Index dialog opens.

   - Select check boxes for the ToS groups you want to add.
   - Click Save.

   You return to the Select Filters & Rollup page of the Custom Report wizard.

7. Check the list of filters and their Inclusion values.

   Items that have a value of 'Include' are in the report. You can remove data for a ToS value or ToS group temporarily by setting the Inclusion value for that item to 'Exclude.'

8. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.

9. (Optional) Return to the report list by clicking one of these buttons:

   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Add or Modify Host and Conversation Filters

You can add host or conversation filters to limit the report data to specific hosts or conversations, but you cannot add both host and conversation filters. You can apply a single type of filter or you can use one of the following valid filter combinations:

- Protocols/Protocol Groups + ToS/ToS Groups
- Protocols/Protocol Groups + Hosts
- Protocols/Protocol Groups + Conversations
- ToS/ToS Groups + Hosts
- ToS/ToS Groups + Conversations

Additional information about the presentation data you can produce with various filter combinations is in the topic Specify Custom Report Filters (see page 95).

Add or Modify Host Filters

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.
3. Click Host/Conversation Filters to open the Specify Filters & Rollup page of the Custom Report wizard.
4. Click Add Host Filter.

   The Apply Host Filter dialog opens.
5. Specify the following values, then click Submit.
   - Host/Network IP: Enter the IP address of the host network whose data will be included.
   - Mask: Select a mask from the list.

   For example, enter 192.168.1.0 with a mask of 255.255.255.0 to include data from all hosts on the class C network 192.168.1.0. The report will not include any data from hosts at other network addresses.

   You return to the Select Filters & Rollup page of the Custom Report wizard.
6. Check the list of filters and their Inclusion values.

   If you specify a single host filter with a value of 'Include,' the report contains data only for that host. If you set a host filter to have a value of Exclude, the report contains data for all other hosts in the selected set of interfaces.
7. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.
8. (Optional) Return to the report list by clicking one of these buttons:
   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Add or Modify Conversation Filters

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.
3. Click Host/Conversation Filters to open the Specify Filters & Rollup page of the Custom Report wizard.
4. Click Add Conversation Filter.

   The Apply Conversation Filter dialog opens.
5. Specify the following values for each host in the conversation pair, then click Submit.

   - Host/Network IP: Enter the IP address of each host network in the conversation pair in the Host/Network IP boxes.
   - Select a mask from the list to the right of the Host/Network IP value.

   For example, specify the two hosts in the conversation by entering 192.168.1.1 with a mask of 255.255.255.225 and 192.168.1.0 with a mask of 255.255.255.0. The report will include conversation data between all hosts on the 192.168.1.1 network and the 192.168.1.0 network.

   You return to the Select Filters & Rollup page of the Custom Report wizard.
6. Check the list of filters and their Inclusion values.

   If you specify a single conversation filter with a value of 'Include,' the report contains data only for that conversation. If you set the conversation filter to 'Exclude,' the report contains all data for other conversations in the selected set of interfaces.
7. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.
8. (Optional) Return to the report list by clicking one of these buttons:

   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Delete Custom Report Filters

You can delete filters from Custom Reports to reflect the deletion of protocols, hosts, or TOS values from your network. Any filter you delete is no longer used to define the report data.

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.
3. Click Host/Conversation Filters to open the Specify Filters & Rollup page of the Custom Report wizard.
4. Select the check box next to each filter that you want to delete.
5. Click the Remove Selected Filters icon at the top-left corner of the list.
6. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.
7. (Optional) Return to the report list by clicking one of these buttons:
   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Exclude Custom Report Filters

For each filter you define in a Custom Report, you can opt to include either:

- Only the data that matches the filter criteria
- All the data that does not match the filter criteria

To set the type of filtering action, you set the Inclusion value for each filter in the Specify Filters list. To display matching data, set the Inclusion value to Include (the default setting). To display data that does not match, set the Inclusion value to Exclude.

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.
3. Click Host/Conversation Filters to open the Specify Filters & Rollup page of the Custom Report wizard.
4. Locate the filter whose data you want to exclude and select Exclude from the Inclusion list.
5. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.
6. (Optional) Return to the report list by clicking one of these buttons:
   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Define Custom Report Periods and Schedules

When you define a Custom Report, you must specify the reporting time period and the resolution of the reporting data. You can define a specific, nonrecurring time period (for a start-and-end report) or you can choose a timespan that ends at the report runtime (for a duration report). You also have the option to set a duration report to regenerate on a recurring schedule and to have the automated reports sent out by email.

This section contains the following topics:

Specify a Reporting Period for Custom Reports (see page 104)
Specify Schedules for Auto-Generated Reports (see page 105)

Specify a Reporting Period for Custom Reports

The Custom Report Wizard provides a Specify Schedule page that defines the report time period. For a manually generated report, you can simply select a time period, resolution, and optional time filter. If you want to generate the report automatically at scheduled intervals, you can also use the Schedule option.

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.
3. Click Reporting Period to open the Specify Schedule page of the Custom Report wizard.

   Note: Custom Reports always display data using the Greenwich Mean Time (GMT) time zone. If a user has set the time to a specific time zone, the reports display the data using GMT.
4. Select the type of reporting period from the Period list on the Specify Schedule page:

   - Duration: Include data from the block of time that immediately precedes the report runtime. Enter a number of days, weeks, months, or years.

     You can set up a schedule for a duration report or you can run the report on demand. To run a scheduled report on demand, you can make a copy of the report and can disable the schedule in the copy.
   - Start and end: Include data from a specific, nonrecurring timespan. Use the calendars to specify a Start date and End date or select hour and time values from the lists.

     Hour values are expressed in 24-hour format.

     A start-and-end report runs on demand. You cannot set up a schedule for a start-and-end report.
5. Set the resolution (granularity for data collection) on the Specify Schedule page: Accept the default setting or enter the number of time units in the Resolution box. Select a unit of time from the list (minutes, hours, days, weeks, months, or years).

   The default resolution varies depending on the length of the reporting period. For example, if you specify a duration of one month for the period, the default resolution is 8 hours. If you specify a duration of one day, the default resolution is 15 minutes.

6. (Optional) Select a time filter from the list on the Specify Schedule page, if your Administrator has created an appropriate time filter.
7. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.
8. (Optional) Return to the report list by clicking one of these buttons:
   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

Specify Schedules for Auto-Generated Reports

Use the Schedule option to set the Custom Report to regenerate at specified times.

For example, suppose that you want to check network traffic during the monthly backups that occur on the last Sunday of each month. You schedule a report to be regenerated on the last Sunday of every month. Suppose that operating system updates occur on the 15th of every month. To check the network traffic during those updates, you schedule a report to be regenerated on the 15th of each month.

Note: The options in the Recurrence section are available only if you select 'duration' as the reporting period type.

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click Edit in the Report Settings section at the top of the report page.

   The Report Definition Summary page opens, which contains links to the Custom Report wizard pages.
3. Click Reporting Period to open the Specify Schedule page of the Custom Report wizard.
4. Click the Schedule check box and choose a recurrence interval from the list:
   - Daily: Select the day or days of the week the report will run.
   - Weekly: Select the day of the week the report will run.
   - Monthly: Select either a date or a week and day combination to specify the one day per month the report will run.
   - Quarterly: Select the month that ends the first quarter in which the report will run. Starting with the specified quarter, the report will run on the last day of each quarter.

- Yearly: Select the month that ends the first year the report will run. The report runs on the last day of the year.

For all schedule interval types, select the time of day and time zone for the report to run.

5. (Optional) Email Results To: Enter the email addresses of anyone who should receive the report by email. Use the format name@domain. Separate multiple addresses with a comma or semi-colon.
6. Click Save Changes.

   Your changes are saved and you return to the Report Definition Summary.
7. (Optional) Return to the report list by clicking one of these buttons:
   - Return to Listing: Return to the Custom Reporting page without queuing the report to run.
   - Queue Report: Queue the report to run and return to the Custom Reporting page.

View Custom Reports

When you have defined the Custom Reports that you need, you are ready to generate a new report and view it in the NFA console. You can run and view the following types of reports:

- Unscheduled duration reports on demand.
- The most recent versions of scheduled duration reports that have been generated automatically.
- The most recent versions of start-and-end reports

Follow these steps:

1. Select Custom Reporting from the NFA console menu if the Custom Reporting page is not already open.

   The Custom Reporting page contains two panes. The left pane lists the folders that store saved reports. The right pane lists the reports in the currently selected folder.
2. Click the name of the folder that contains the report you want to view.
3. Click the report name in the Reports list.

   The report runs. The results are displayed when report generation is complete.

4. (Optional) Change the type of presentation by selecting an option from the Report Type list.

   The default presentation type is Custom layout. The other available options are dependent on the filters that are defined for your report.

   When you select an option other than Custom Layout, a Presentation menu is added on the left side of the page. You can select from the presentation types and from the data types to modify your view. For example, you could change from a pie chart to a stacked trend chart that shows volume.

Also See:

Set the Presentation Options (see page 64)

Manage Custom Reports

Creating reports for your organization is an important part of using the capabilities of CA Network Flow Analysis. The report definitions are saved so you can generate an updated report at any time or you can use the report as a template for another report. As the number of report definitions grows, use the folder management system to keep the reports organized and accessible.

The report folders are listed in the left pane. The Custom Reports folder is a built-in folder, which is already present when you install CA Network Flow Analysis. Create additional folders to provide more extended organization for your reports.

The right pane displays a list of the reports stored in the currently selected folder. Use the links at the top and bottom of the panel to delete, run, or move any selected reports, to create a report, or to cancel the ongoing regeneration of reports.

Create a Report Folder

Create your own report folders to group reports. For example, you can use folder names to identify the purpose for a set of reports.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. Click **New** at the bottom of the **Saved Report Folders** pane.

   A pop-up dialog opens.

3. Enter a name for the new folder in the pop-up dialog.
4. Click **OK**.

   The dialog closes and the new folder appears in the **Saved Report Folders** pane.

Rename a Report Folder

You can change the name of a report folder, including the name of the default report folder.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. In the **Saved Report Folders** pane, select the check box next to the report folder that you want to rename.
3. Click **Rename**.

   A pop-up dialog opens.
4. Enter a new name for the folder in the pop-up dialog.
5. Click **OK**.

   The dialog closes. The new report folder name appears in the **Saved Report Folders** pane.

Move a Report to Another Folder

You can add folders and move report definitions among the folders to make the report definitions easier to find or to help identify them.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. In the **Reports** pane, select the check box next to all the reports that you want to move.
3. Click **Move to Folder**.

   A pop-up dialog opens.
4. Select a destination folder from the list.
5. Click **OK**.

   The dialog closes. The reports are now in their new location, and are visible when you click that folder name in the **Saved Report Folders** pane.

Delete Saved Report Definitions

When a saved report definition is no longer needed, you can delete it. You can delete one report definition at a time, or you can delete multiple definitions in a single folder simultaneously. Be sure that you do not delete a report definition that is useful as a template for creating other reports. Deleted report definitions cannot be restored.

Follow these steps:

1. In the Reports pane, select the check box next to all report definitions that you want to delete.
2. Click Delete.

   A confirmation box opens.
3. In the confirmation dialog box, click OK.

   The confirmation box closes. The list of saved report definitions is updated.

Delete Report Folders

You can delete unneeded report folders and their contents. Be sure that you do not delete useful report definitions or folders. Deleted folders and report definitions cannot be restored.

Follow these steps:

1. In the Saved Report Folders pane, select the check box next to all the report folders that you want to delete.
2. Click Delete.

   A confirmation box opens. If the folders contain report definitions, the confirmation box reminds you of the number of report definitions that will be deleted.
3. In the confirmation dialog box, click OK.

   The confirmation box closes. The list of saved report definitions is updated.

Chapter 5: Flow Forensics Reports

Flow Forensics reports let you drill down to raw data flows and see a level of detail that is not available in other reports. You can jump to detailed information about any of the fields in a data packet for any monitored interface.

You can run a Flow Forensics report to drill down and view raw flow data. The data is parsed into meaningful reports.

Use Flow Forensics to browse raw flow data for a specified time period. You can filter the results by using a number of fields. You can export the displayed data to a file in comma-separated value (CSV) format.

Flow Forensics reports let you report on all of the flow data that is collected in your environment. You can analyze every protocol, host, and conversation on your network. Other report types are designed to show the most active interfaces, protocols, hosts, and conversations or to show individual instances of these items.

Flow Forensics reports can provide a comprehensive analysis of all traffic for the following categories, for example:

- Protocols that are active for one or more specified hosts
- All protocols that are active on the network
- All hosts that access one or more specified hosts
- Volume of traffic to or from one or more specified hosts

This section contains the following topics:

Flow Forensics Report Types (see page 111)
Work with Flow Forensics Reports (see page 128)

Flow Forensics Report Types

The following topics describe the available Flow Forensics reports.

Address Report Group

The Address Flow Forensics reports have the following fields.

Report	Src Addr	Dest Addr	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)	# of Src Addr	# of Dest Addr	IP Protocol	Dest Port
Address Pairs	Y	Y	Y	Y	Y	Y	Y	Y	Y				
Destination Address Peer Count		Y				Y				Y			
Destination Addresses		Y	Y	Y	Y	Y	Y	Y	Y				
Source Address Peer Count	Y										Y		
Source Address Peer Count with Destination Port	Y					Y					Y	Y	Y
Source Addresses	Y		Y	Y	Y	Y	Y	Y	Y				

Address Pairs Report

Displays the following information about pairs of IP addresses that exchanged traffic:

- IP addresses of the source host and destination host in the conversation
- Data volume and rate, shown in bytes (or kilobytes, megabytes) and packets

Percentage of total traffic that the data represents, shown in bytes (or kilobytes, megabytes) and packets

Destination Address Peer Count Report

Displays the following information about each traffic destination:

- Destination address
- Number of unique source addresses that exchanged traffic with the destination host
- Flow count

Destination Addresses Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count of each traffic destination.

Source Address Peer Count Report

Displays the following information about each traffic source:

- Source address
- Number of destination addresses that received traffic from the source host
- Flow count

Source Address Peer Count with Destination Port Report

Displays the following information about each traffic source:

- Source address
- Destination port
- IP protocol
- Number of destination addresses that received traffic from the source host
- Flow count

Source Addresses Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count of each source address.

Application Response Time Report Group

The Application Response Time reports show Cisco's Application Response Time (ART) metrics. ART metrics are available for IPFIX flows from routers that have Cisco ART metrics enabled.

Meaningful data is shown in the Application Response Time reports under the following conditions:

- The routers and interfaces in the report are configured to export IPFIX flow.
- The exported flow includes the appropriate fields.

  If a router is not configured to return data for the appropriate fields, a zero (0) appears in the corresponding table cells. Non-NBAR2 traffic shows a zero for all of the values except the router IP address and application name.

  The Application column values show the NBAR2 application name followed by the application ID. The application name is included if it is defined by the standard (not custom) NBAR2 engine. Otherwise the Application value may consist of only the application ID.

The Application Response Time reports have the following fields.

Report	Router Addr	Application	Transactions	Avg Total Transaction Time	Late Responses	Retransmissions	Client Address	Server Address	New Connections	Avg Client Network Delay	Avg Server Network Delay	Avg Response Time	Avg Application Delay
Application Metrics	Y	Y	Y	Y	Y	Y							
Client Side Metrics	Y	Y					Y	Y	Y	Y			
Server Side Metrics	Y	Y							Y		Y	Y	Y

Application Metrics Report

Displays a summary of ART metrics for IPFIX flow that includes NBAR2 data. The report table includes a row for each unique combination of the following values:

- IP address of the router that sent the data
- NBAR2 application name
- Number of transactions
- Number of late responses
- Number of times that lost packets were retransmitted
- Average of the total transaction time, which is calculated from the flow record data

Client Side Metrics Report

Displays client-side ART metrics for IPFIX flow that includes NBAR2 data. Each row shows the values for a unique combination of the following values:

- IP address of the router that sent the data
- NBAR2 application name
- IP addresses of the client and server
- Number of new connections
- Average client network delay

Server Side Metrics Report

Displays server-side ART metrics for IPFIX flow that includes NBAR2 data. Each row shows the values for a unique combination of the following values:

- IP address of the router that sent the data
- NBAR2 application name
- Number of new connections
- Average server network delay
- Average response time (includes the network time from the client to the server and the server response time)
- Average application delay

ICMP Report Group

The ICMP Flow Forensics reports have the following fields.

Report	Src Addr	Dest Addr	Dest Network	# of Src Addr	# of Dest Addr	ICMP	Pkts	Flows
Bad IP Headers	Y							Y
Fragmentation Required and DF Flag Set		Y		Y				Y
ICMP Traffic Summary						Y		Y
Ping Conversation Pairs	Y	Y					Y	Y
Ping Destinations		Y					Y	Y
Ping Sources	Y						Y	Y
Traceroute Requests by Destination		Y		Y				Y
Traceroute Requests by Source	Y				Y			Y
Traceroute Requests Pairs	Y	Y						Y
TTL Expired in Transit	Y	Y						Y
Unreachable Destination by Source	Y						Y	Y
Unreachable Destination Networks			Y				Y	Y

Report	Src Addr	Dest Addr	Dest Network	# of Src Addr	# of Dest Addr	ICMP	Pkts	Flows
Unreachable Destinations	Y		Y				Y	Y

Bad IP Headers Report

Displays the source address and flow count of each bad IP header--each IP header that failed the checksum.

Fragmentation Required and DF Flag Set Report

Displays the following information about packets that require fragmentation--packets that had unreachable hosts or that were flagged Fragmentation Needed and Don't Fragment:

- Destination address
- Number of source addresses that sent this type of data to the destination address
- Number of flows that contained packets of this type

ICMP Traffic Summary Report

Summarizes the Internet Control Message Protocol (ICMP) types and codes that occurred. The report contains the following information:

- ICMP description, type, and code
- Volume of inbound packets for each ICMP
- Flow count for each ICMP

Ping Conversation Pairs Report

Displays the following information about ping requests:

- Source address
- Destination address
- Volume of inbound packets
- Flow count

Ping Destinations Report

Displays the following information about ping request destinations:

- Destination address that received the request
- Volume of inbound packets
- Flow count

Ping Sources Report

Displays the following information about ping request sources:

- Source address that generated the request
- Volume of inbound packets
- Flow count

Traceroute Requests by Destination Report

Displays the following information about traceroute request destinations:

- Destination address of the traceroute request
- Number of source addresses that sent traceroute requests to the destination
- Flow count

Traceroute Requests by Source Report

Displays the following information about traceroute request sources:

- Source address of each traceroute request
- Number of destination addresses that received traceroute requests from the source
- Flow count

Traceroute Requests Pairs Report

Displays the following information about each traceroute address pair:

- Source address of the traceroute request
- Destination address of the traceroute request
- Flow count

TTL Expired in Transit Report

Displays the following information about data that met or exceeded the Time To Live (TTL) threshold:

- Source address
- Destination address
- Flow count

Unreachable Destination by Source Report

Displays the following information about sources that tried to connect with unreachable destinations:

- Source address
- Volume of inbound packets
- Flow count

Unreachable Destination Networks Report

Displays the following information about unreachable destinations:

- Destination network and subnet mask
- Number of inbound packets
- Flow count

Unreachable Destinations Report

Displays the following information about sources and unreachable destinations:

- Source address
- Destination network and subnet mask
- Volume of inbound packets
- Flow count

MAC Report Group

The MAC Flow Forensics reports have the following fields.

Report	Dest MAC	Source MAC	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
Destination MAC	Y		Y	Y	Y	Y	Y	Y	Y
MAC Pairs	Y	Y	Y	Y	Y	Y	Y	Y	Y
Source MAC		Y	Y	Y	Y	Y	Y	Y	Y

Destination MAC Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count on each destination Media Access Control (MAC) address.

MAC Pairs Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count on each pair of source and destination MAC addresses.

Source MAC Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count on each source MAC address.

MPLS Reports

The MPLS Labels Flow Forensics report has the following fields.

Report	Router Addr	Label Addr	Label Type	Top Label	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
MPLS Labels	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

MPLS Labels Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count of traffic that had a unique combination of the following values:

- Router address
- Multiprotocol Label Switching (MPLS) address
- MPLS label type
- MPLS top label

Network Reports Group

The Network Flow Forensics reports have the following fields.

Report	Src A S	Dest A S	Src Network	Dest Network	Src Addr	Dest Addr	ToS	Next Hop	TCP Reset Count	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
Autonomous System Pairs	Y	Y								Y	Y	Y	Y	Y	Y	Y
Autonomous System Pairs (with Destination Network)	Y	Y		Y						Y	Y	Y	Y	Y	Y	Y
Destination Autonomous Systems		Y								Y	Y	Y	Y	Y	Y	Y
Destination Networks				Y						Y	Y	Y	Y	Y	Y	Y
Network Pairs			Y	Y						Y	Y	Y	Y	Y	Y	Y
Network Pairs (with ToS)			Y	Y			Y			Y	Y	Y	Y	Y	Y	Y

Report	Src A S	Dest A S	Src Network	Dest Network	Src Addr	Dest Addr	ToS	Next Hop	TCP Reset Count	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
Next Hops								Y		Y	Y	Y	Y	Y	Y	Y
Source Autonomous Systems	Y									Y	Y	Y	Y	Y	Y	Y
Source Networks	Y									Y	Y	Y	Y	Y	Y	Y
TCP Resets					Y	Y			Y							

Autonomous System Pairs Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic between a pair of source and destination autonomous systems.

Autonomous System Pairs (with Destination Network) Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic that had a unique combination of the following values:

- Source AS
- Destination AS
- Destination network and subnet mask

Destination Autonomous Systems Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic on each destination autonomous system.

Destination Networks Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count of traffic on each destination network and subnet.

Network Pairs Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic on each pair of source and destination network subnets.

Network Pairs (with ToS) Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic on each network pair that had a unique combination of the following values:

- Source network and subnet mask
- Destination network and subnet mask
- ToS

Next Hops Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic for each next-hop address.

Source Autonomous Systems Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic on each source autonomous system.

Source Networks Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic on each source network and subnet.

TCP Resets Report

Displays the TCP reset count of traffic on each source and destination address pair.

QOS Report Group

The QoS (Quality of Service) Flow Forensics reports have the following fields.

Report	DSCP	ToS	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
Differentiated Services	Y		Y	Y	Y	Y	Y	Y	Y
Type of Service		Y	Y	Y	Y	Y	Y	Y	Y

Differentiated Services Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the traffic flow count for each DiffServ code point (DSCP) value.

Types of Service Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the traffic flow count for each Type of Service (ToS).

Session Report Group

The Session Flow Forensics reports have the following fields.

Report	Router Addr	Interface In	IP Protocol	Src Addr	Src Addr (IPv6)	Src Port	Interface Out	Dest Addr	Dest Addr (IPv6)	Dest Port	ToS	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Flow Duration	Pkts	Rate (Pkts)	% Total (Pkts)	Engine	Application
Client-Server Sessions			Y					Y		Y		Y	Y	Y	Y		Y	Y	Y		
Conversation Sessions	Y	Y	Y	Y				Y		Y	Y	Y	Y	Y	Y	Y			Y		
Conversation Sessions (NBAR2)	Y	Y	Y	Y		Y		Y		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Conversations			Y	Y		Y		Y		Y		Y	Y	Y	Y		Y	Y	Y		
Conversations (IPv6)			Y		Y	Y			Y	Y		Y	Y	Y	Y		Y	Y	Y		
Conversations (with Interfaces)	Y	Y	Y	Y		Y	Y	Y		Y		Y	Y	Y	Y		Y	Y	Y		
Destination Applications			Y							Y		Y	Y	Y	Y		Y	Y	Y		
Destination Endpoints			Y					Y		Y		Y	Y	Y			Y	Y	Y		
Protocols			Y									Y	Y	Y	Y		Y	Y	Y		
Server-Client Sessions			Y	Y		Y		Y				Y	Y	Y	Y		Y	Y	Y		
Source Applications			Y			Y						Y	Y	Y	Y		Y	Y	Y		
Source Endpoints			Y	Y		Y						Y	Y	Y	Y		Y	Y	Y		

Client-Server Sessions

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of each session that had a unique combination of the following values:

- Source and destination address.
- Destination port.
- IP protocol.

Conversation Sessions Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count and cumulative flow duration of each conversation session that had a unique combination of the following values:

- Router address
- Inbound interface
- Source address and port
- Destination address and port
- ToS
- IP protocol

Conversation Sessions (NBAR2) Report

Displays conversation session traffic and identifies any NBAR2 (Next Generation Network-Based Application Recognition) data that is included. The report table includes a row for each unique combination of the following values:

- IP address of the router that sent the data
- Name of the interface that received the data
- IP protocol for the data
- IP addresses and ports of the source host and destination host in the conversation
- Type of service
- Volume, rate and percentage of total traffic that the data represents, shown bytes (or megabytes, kilobytes) and packets
- Flow count
- Total duration of the flows in the row
- NBAR2 Engine name and ID
  Standard NBAR2 data has "layer7 (13)" in the Engine column.
- NBAR2 Application name and ID

If a router is not configured to return NBAR2 data, a zero (0) appears in its rows under the Engine and Application columns. If other columns contain a zero for the router rows, the router may not be configured to return the fields for those values.

The Application column values show the NBAR2 application name followed by the application ID. The application name is included if it is defined by the standard (not custom) NBAR2 engine. Otherwise the Application value may consist of only the application ID.

Conversations Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic for each IPv4 address pair that had a unique combination of the following values:

- Source address and port
- Destination address and port
- IP protocol

Conversations (IPv6) Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic for each IPv6 address pair that had a unique combination of the following values:

- Source address and port
- Destination address and port
- IP protocol

Conversations (with Interfaces)

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of each conversation that had a unique combination of the following values:

- Router address
- Inbound and outbound interface
- Source address and port
- Destination address and port
- IP protocol

Destination Applications Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic that had a unique combination of the following values:

- Destination port
- IP protocol

Destination Endpoints Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic that had a unique combination of the following values:

- Destination address
- Destination port
- IP protocol

Protocols Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of traffic that had a unique IP protocol.

Server-Client Sessions Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of each traffic session that had a unique combination of the following values:

- Source address and port
- Destination address and port
- IP protocol

Source Applications Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of each traffic session that had a unique combination of the following values:

- Source port
- IP protocol

Source Endpoints Report

Displays the volume, rate, and percent of total inbound bytes and packets. Also displays the flow count of each traffic session that had a unique combination of the following values:

- Source address
- Source port
- IP protocol

TCP Reports

The TCP Flags Flow Forensics report has the following fields.

Report	TcpFlags	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
TCP Flags	Y	Y	Y	Y	Y	Y	Y	Y

TCP Flags Report

Displays volume, rate, and percent of total inbound bytes/packets, as well as the flow count of traffic for each TCP flag.

VLAN Report Group

The VLAN Flow Forensics reports have the following fields.

Report	Destination VLAN	Source VLAN	Bytes	Rate (Bits)	% Total (Bytes)	Flows	Pkts	Rate (Pkts)	% Total (Pkts)
Destination VLANs	Y		Y	Y	Y	Y	Y	Y	Y
Source VLANs		Y	Y	Y	Y	Y	Y	Y	Y
VLAN Pairs	Y	Y	Y	Y	Y	Y	Y	Y	Y

Destination VLANs Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count of traffic on each destination VLAN.

Source VLANs Report

Displays the volume, rate, and percent of total inbound bytes/packets, as well as the flow count of traffic on each source VLAN.

VLAN Pairs Report

Displays the volume, rate, and percent of total bytes in/packets in, as well as the flow count of traffic on each source and destination VLAN pair.

WAAS Segment Report Group

WAAS Segment Report

Displays a report that identifies the WAAS (Wide Area Application Services) segment number and pass-through reason. Having the pass-through reason helps you determine why flow is not optimized.

The report shows meaningful data if the reporting routers have WAAS configured and if Cisco Performance Agent monitors the WAAS traffic. Other traffic does not return any meaningful values except for the router IP address.

The Application column values show the NBAR2 application name followed by the application ID. The application name is included if it is defined by the standard (not custom) NBAR2 engine. Otherwise the Application value may consist of only the application ID.

The WAAS Segment Flow Forensics report has the following fields.

Report	Router Addr	Application	Client Address	Server Address	WAAS Segment	
WAAS Segment	Y	Y	Y	Y	Y	Y

The report table includes a row for each unique combination of the following values:

- IP address of the router that sent the data
- Application name (NBAR2 application name and ID)
- IP addresses of the client and server
- WAAS segment: Type of WAAS data source
- WAAS passthrough reason

Work with Flow Forensics Reports

Open the Flow Forensics page and create Flow Forensics reports to see details about raw data flows for troubleshooting. Use the saved report definitions to generate an updated report at any time. You can also use a report definition as a basis for another Flow Forensics report.

As the number of reports grows, use the folder management system to keep the reports organized and accessible.

This section contains the following topics:

Open the Flow Forensics Page (see page 128)
Create a Flow Forensics Report (see page 128)
View a Flow Forensics Report (see page 133)
Create a Report Folder (see page 133)
Rename a Report Folder (see page 134)
Move a Report to Another Folder (see page 134)

Open the Flow Forensics Page

When you click the Flow Forensics tab, the Saved Report Folders pane is displayed on the left and the existing reports are displayed on the right.

You can perform the following tasks in the Saved Report Folders pane: create folders, rename folders, and delete custom folders. You cannot delete the default Flow Forensics Reports folder, which is built in to CA Network Flow Analysis. Create additional folders to provide more extended organization for your Flow Forensics reports.

The right pane displays the Flow Forensics report definitions in the currently selected folder. Use the links at the top and bottom of the pane to delete or run selected reports, as well as to create or move reports.

Create a Flow Forensics Report

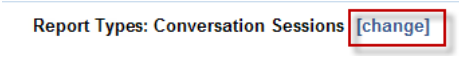
Complete the following steps to create a Flow Forensics report.

Follow these steps:

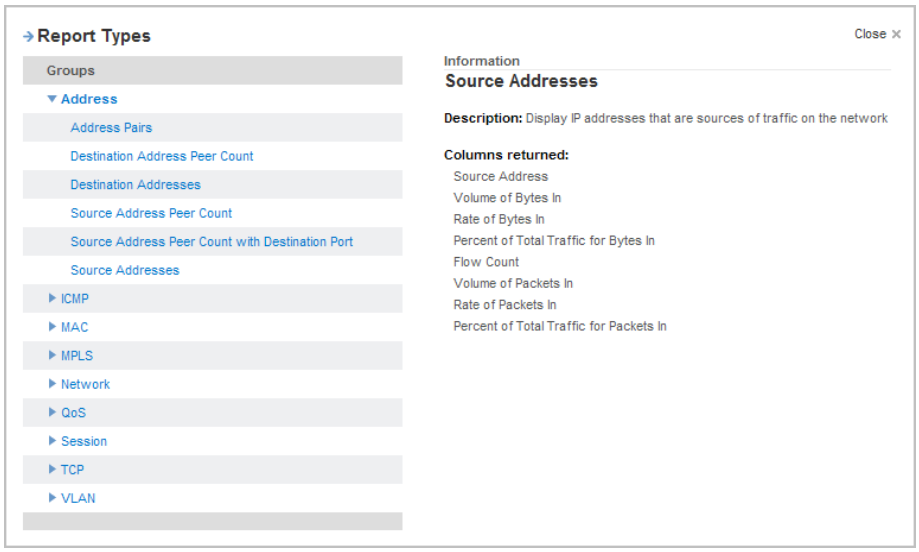
1. Select Flow Forensics from the NFA console menu if the Flow Forensics page is not already open.
2. Click Create New Report.

   The Report Settings page opens and displays options for the default report type, Conversation Sessions.

3. (Optional) Change the report type:
   - Click [change] next to the Report Types label to select a different report type.



   The Report Types dialog opens.



   - Click the heading for the report group that interests you.

     The report list expands for the selected group.

   - Select the report type from the expanded list.

     You return to the Report Settings page, which shows a name and label for the new report type.

   Also See: Flow Forensics Report Types (see page 111)

4. (Optional) Identify the report and set the folder for saving it by entering values in the following fields:
   - Name: Report name that appears on
   - Description: Add a description for the report.
   - Folder: Select a parent folder for the report.
5. (Optional) Change the filters that are used in the report definition:
   - Remove Filters: Click the X next to the filter name in the Added Filters list to delete a filter from the report definition.
   - Add Filters: Use the Add Filters options to filter the displayed data.

Example: To exclude the FTP protocol, complete the following steps:

a. Select RA: Protocol Filter.

b. Select NotEqual.

c. Click Protocol Index.

d. Select the ftp protocol.

The following list describes the available filters.

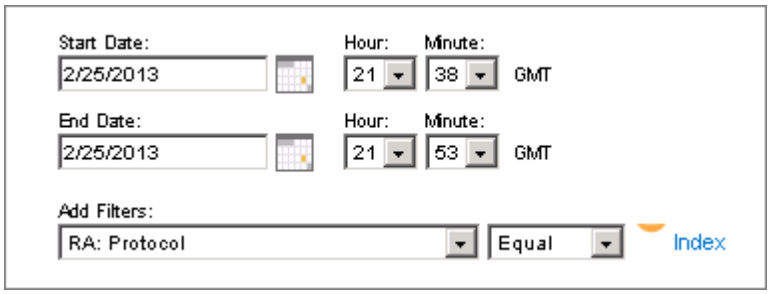
Note: Certain filters may not be available for all reports.

- *RA: Protocol:* Filters for the actual protocol, including Application mapping rules, as defined in CA Network Flow Analysis Administration (Flow Forensics report filter)
- *RA: Interface:* Filters for the actual interface, excluding aggregate and custom virtual interfaces, as defined in CA Network Flow Analysis Administration (Flow Forensics report filter)
- *RA Type-of-service:* Filters for the CA Network Flow Analysis type of service as defined in CA Network Flow Analysis Administration (Flow Forensics report filter)
- *Destination Address:* Filters for the IP address of one or multiple destination hosts (Flow Forensics report filter)
- *Destination Autonomous System:* Filters for the autonomous number for the destination network (Flow Forensics report filter)
- *Destination MAC Address:* Filters for the destination MAC address (Flow Forensics report filter)
- *Destination Mask:* Filters for the IP mask of a destination network (Flow Forensics report filter)
- *Destination Port:* Filters for the destination port number (0 through 65,535) (Flow Forensics report filter)
- *Destination VLAN:* Filters for the destination address of the VLAN (Flow Forensics report filter)
- *Flow Count:* Filters for the number of flows (Flow Forensics report filter)
- *Flow Duration:* Filters for the duration of the flows (Flow Forensics report filter)
- *ICMP:* Filters for information about ICMP (Flow Forensics report filter)
- *MPLS Top Label:* Filters for the top label of MPLS (Flow Forensics report filter)
- *MPLS Top Label IP Address:* Filters for the IP address of the MPLS top label (Flow Forensics report filter)
- *MPLS Top Label Type:* Filters for the type of MPLS top label type (Flow Forensics report filter)

- *Next Hop:* Filters for the IP address of next destination hop (Flow Forensics report filter)
- *Percent of Total Traffic for Bytes In:* Filters for the percentage of bytes in total traffic (Flow Forensics report filter)
- *Percent of Total Traffic for Packets In:* Filters for the percentage if packets in total traffic (Flow Forensics report filter)
- *Protocol:* Filters for the actual IP Protocol Number (6=tcp,17=udp) (Flow Forensics report filter)
- *Protocol and Destination Port:* Filters for the actual IP Protocol Number (6=tcp,17=udp) and the Destination port number (0 through 65,535) (Flow Forensics report filter)
- *Protocol and Source or Destination Port:* Filters for the actual IP Protocol Number (6=tcp,17=udp) and the Source or Destination port number (0 through 65,535) (Flow Forensics report filter)
- *Protocol and Source Port:* Filters for the actual IP Protocol Number (6=tcp,17=udp) and the IP address of a source host (Flow Forensics report filter)
- *Router Address:* Filters for the IP address of the router (Flow Forensics report filter)
- *Router Address and Interface In:* Filters for the router address and router interface (in) index number (Flow Forensics report filter)
- *Router Address and Interface In or Out:* Filters for the router address and router interface (in or out) index number (Flow Forensics report filter)
- *Router Address and Interface Out:* Filters for the router address and router interface (out) index number (Flow Forensics report filter)
- *Source Address:* Filters for the IP address of one or multiple source hosts (Flow Forensics report filter)
- *Source Autonomous System:* Filters for the autonomous number for the source network (Flow Forensics report filter)
- *Source MAC Address:* Filters for the source MAC address (Flow Forensics report filter)
- *Source Mask:* Filters for the IP mask of a source network (Flow Forensics report filter)
- *Source or Destination Address:* Filters for the IP address of a source host or a destination host (Flow Forensics report filter)
- *Source or Destination MAC Address:* Filters for the source or destination of the MAC address (Flow Forensics report filter)

- *Source or Destination Mask:* Filters for the IP mask of a source network or a destination network (Flow Forensics report filter)
- *Source or Destination Port:* Filters for the source port number or the destination port number (Flow Forensics report filter)
- *Source or Destination VLAN:* Filters for the source or destination of the VLAN (Flow Forensics report filter)
- *Source Port:* Filters for the source port number (Flow Forensics report filter)
- *Source VLAN:* Filters for the source VLAN (Flow Forensics report filter)
- *TCP Flags:* Filters for the Transmission Control Protocol (TCP) flags (Flow Forensics report filter)
- *Type-of-service:* Filters for the IP type of service number (0 through 255) (Flow Forensics report filter)
- *Volume of Bytes In:* Filters for the volume of bytes in (Flow Forensics report filter)
- *Volume of Packets In:* Filters for the volume of packets in (Flow Forensics report filter)

6. (Optional) Change the timespan for collecting report data: Select Start Date and End Date values.



7. Run or save the report:
   - Save: Save the report so it is available for later use, but is not executed immediately.

     The report is saved and the Saved icon is added to the Report Settings page.
   - Run: Save, queue, and run the report.

     The Report Queued message appears. When the report finishes execution, the message closes and the report appears.

     Click Back to Folders to return to the Flow Forensic Reports folders before execution is complete.

View a Flow Forensics Report

Complete the following steps to view an existing Flow Forensics report.

Follow these steps:

1. Select Flow Forensics from the NFA console menu if the Flow Forensics page is not already open.
2. Click the parent folder that contains the report.

   The list of reports in the folder opens.
3. Click the check box next to the report that you want to view.
4. Click Run.

   A verification message opens.
5. Click OK.
6. Refresh the view until the report status is Complete.

   The report results are displayed.

Create a Report Folder

Create your own report folders to group reports. For example, you can use folder names to identify the purpose for a set of reports.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. Click **New** at the bottom of the **Saved Report Folders** pane.

   A pop-up dialog opens.
3. Enter a name for the new folder in the pop-up dialog.
4. Click **OK**.

   The dialog closes and the new folder appears in the **Saved Report Folders** pane.

Rename a Report Folder

You can change the name of a report folder, including the name of the default report folder.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. In the **Saved Report Folders** pane, select the check box next to the report folder that you want to rename.
3. Click **Rename**.

   A pop-up dialog opens.
4. Enter a new name for the folder in the pop-up dialog.
5. Click **OK**.

   The dialog closes. The new report folder name appears in the **Saved Report Folders** pane.

Move a Report to Another Folder

You can add folders and move report definitions among the folders to make the report definitions easier to find or to help identify them.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. In the **Reports** pane, select the check box next to all the reports that you want to move.
3. Click **Move to Folder**.

   A pop-up dialog opens.
4. Select a destination folder from the list.
5. Click **OK**.

   The dialog closes. The reports are now in their new location, and are visible when you click that folder name in the **Saved Report Folders** pane.

Chapter 6: Analysis Reports

You can troubleshoot problems as they occur by using Analysis reports to identify issues before users in your environment are adversely affected.

The troubleshooting capabilities of CA Network Flow Analysis are not limited to the features discussed in these topics.

This section contains the following topics:

Set Up Analyses (see page 135)
Manage Analysis Reports (see page 143)

Set Up Analyses

An Analysis report is designed to compare collected network data to a threshold so you can identify potential bottlenecks, anomalies, and viruses. Analysis reports help you identify potential problems before they become serious issues. You can schedule these reports to run regularly, which means you can continually analyze your network traffic for potential issues.

To open the Analysis page, click Analysis in the NFA console menu.

The Analysis page includes the following options:

New

Create an Analysis report.

Run

Execute one or more reports at the same time.

Move to Folder

Transfer one or more reports to a different directory.

Cancel

Immediately stop the execution of one or more reports that are running.

When you create Analyses, you specify protocol, ToS, host, and conversation filters to use. The following list shows the valid filters and combinations of filters:

- No filters
- Protocol filters
- ToS filters
- Protocol and ToS filters

- Protocol and host filters
- Protocol and conversation filters
- ToS and conversation filters
- ToS and host filters
- Conversation filters
- Host filters

Create an Analysis Report

No Analysis reports are installed by default. A report folder named Analyses exists by default, which you cannot delete. You can store your saved Analysis reports in this folder or you can create other folders to organize your Analysis reports.

Follow these steps:

1. Select Analysis from the NFA console menu if the Analysis page is not already open.
2. Select Create New Report.

   The Analysis Wizard opens and displays options for creating an analysis definition or modifying a copy of an existing analysis definition.
3. Select one of the options and click Next.
   - Create a new analysis

     Define an entirely new Analysis report.
   - Copy an existing analysis

     Select an existing report to copy and use as a basis for the new report.

   If you select "Create a new analysis," the Select Interfaces page of the Analysis wizard opens.
4. Select interfaces or interface groups for the report.
   a. Click one of the following options:
   - Add Interface Filter

     Select one or more individual interfaces from the Interface Index.
   - Add Interface Group Filter

     Select one or more interface groups from the Interface Group Selection list.

     The selected interfaces are added to the interface list.

a. Accept the default value or set the Inclusion value for each interface or interface group:

   - 'Include' sets the program to use report data from the interface or group.
   - 'Exclude' sets the program to eliminate data from the interface or group.

b. Click Next.

   The Specify Filters & Threshold page opens.

5. Specify the settings on the Specify Filters & Threshold page:

   a. (Optional) Specify filters for gathering or excluding report data, then set the Inclusion value for each filter to Include or Exclude:

      - Add Protocol Filter

        Select individual protocols from the Protocol Index.

      - Add Protocol Group Filter

        Select protocol groups from the Protocol Group Index.

      - Add ToS Filter

        Select individual ToS values from the ToS Index.

      - Add ToS Group Filter

        Select ToS groups from the ToS Group Index.

      - Add Host Filter

        Specify a host IP address and mask.

      - Add Conversation Filter

        Identify the IP addresses and mask for each party in the conversation pair.

   b. Accept the default value or set the Inclusion value for each filter you specified:

      - Include

        For each filter listed, use only the data of the listed type. For example, use data from the listed protocol group, but not from other protocol groups.

      - Exclude

        For each filter listed, do not use the data of the listed type. For example, do not use data from the listed protocol group, but do use data from other protocol groups.

   c. Set the Threshold Settings values to specify the threshold that is used for the Analysis report.

   d. Click Next.

   For example, to report on overutilized interfaces you might specify a threshold to examine total traffic that goes above 70 percent utilization.

6. Click Next.

   The Specify Schedule page opens.

7. Select the type of reporting period from the Period list on the Specify Schedule page:

   - Duration

     Limits the reporting period to an amount of time, ending at the time the report runs. Enter the number of time units in the Last box. Select a unit of time from the list (days, weeks, months, or years).

     You can set up a schedule for a Duration report or you can run the report on demand.

   - Start and end

     a. Use one of the following methods to specify a Start date and End date:

        Select the calendar icons and click dates to specify the Start and End of the report period.

        Select hour and time values from the lists. Hour values are expressed in 24-hour format.

     b. Enter the number of time units in the Resolution box. Select a value from the list for Start and End.

        A Start-and-End report runs on demand. You cannot set up a schedule for a Start-and-End report.

8. Accept the default Resolution setting on the Specify Schedule page or enter the number of time units in the Resolution box. Select a unit of time from the list (minutes, hours, days, weeks, months, or years).

9. (Optional) Select a time filter from the list on the Specify Schedule page, if your Administrator has created a time filter that is appropriate for your report.

10. (Optional) Select the Schedule check box on the Specify Schedule page and specify the following options:

    a. Schedule: Select the type from the Schedule list (Daily, Weekly, Monthly, Quarterly, Yearly).

       - Daily: Select the day or days of the week, time of day, and time zone for report generation.
       - Weekly: Select the day of the week, time of day, and time zone for report generation.
       - Monthly: Select either the date or the week in the month and day of the week. Select the time of day, and time zone for report generation.

- Quarterly: Select a month that ends the first reporting quarter, time of day, and time zone.
- Yearly: Select a month that ends the first reporting year, time of day, and time zone.

b. (Optional) Email Results To: Enter the email addresses of all the report recipients in the format name@domain. Separate multiple addresses with a comma or semi-colon.

The options in the Recurrence section are available only if you select 'duration' as the reporting period type.

11. Click Next.

    The Enter Name page opens.

12. Identify the report and its location and click Next:

    - Folder

      Accept the default folder or select a different folder to contain the new report.

    - Name

      Give the new report a name that will appear in the Reports list.

    - Description

      (Optional) Add a description to help identify the report. For example, you may to use the description to identify scheduled reports and to indicate distinguishing features of Duration reports.

    Additional information about managing Analysis reports is in the topic Manage Analysis Reports (see page 143).

    The Summary & Submit page opens.

13. Review the information in the Report Definition Summary.

    - Save

      Save the report definition and return to the Custom Reporting page.

    - Save and Queue Report

      Queue the report to run and return to the Custom Reporting page.

    - Back

      Return to previous pages in the wizard to redefine the report.

View an Analysis Report

When you have defined the Analysis reports that you need, you are ready to generate a new report and to view it in the NFA console. You can run and view the following types of reports:

- Unscheduled duration reports on demand.
- The most recent versions of scheduled duration reports that have been generated automatically.
- The most recent versions of start-and-end reports.

Follow these steps:

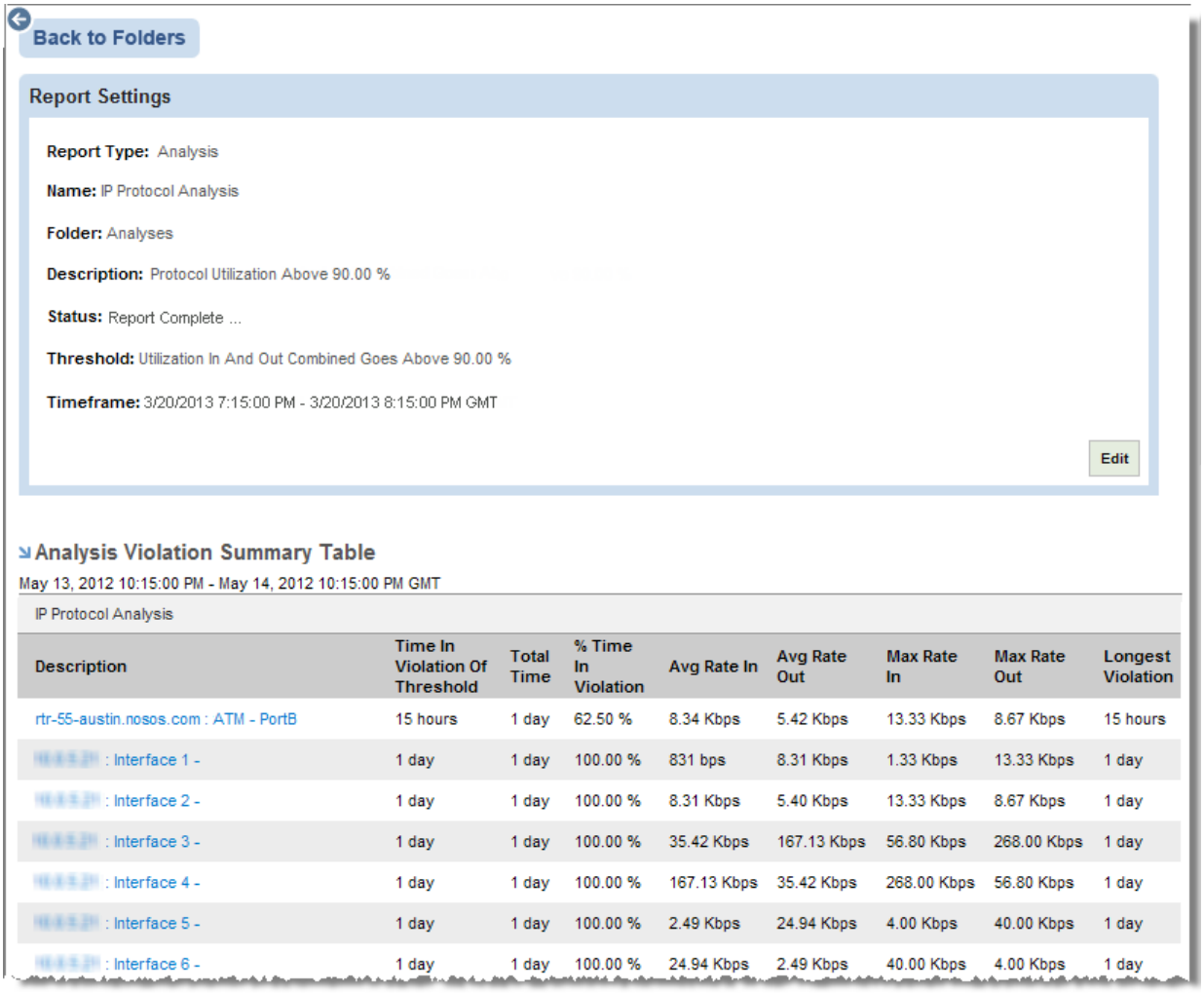
1. Select Analysis from the NFA console menu if the Analysis page is not already open.

   The Analysis page contains two panes. The left pane lists the folders that are used to store saved report definitions. The right pane lists the reports in the currently selected folder.

2. Click the name of the folder that contains the report you want to view.

3. Click the report name in the Reports list.

   The report runs. The results are displayed when report generation is complete.



Back to Folders

Report Settings

Report Type: Analysis

Name: IP Protocol Analysis

Folder: Analyses

Description: Protocol Utilization Above 90.00 %

Status: Report Complete ...

Threshold: Utilization In And Out Combined Goes Above 90.00 %

Timeframe: 3/20/2013 7:15:00 PM - 3/20/2013 8:15:00 PM GMT

Edit

Analysis Violation Summary Table

May 13, 2012 10:15:00 PM - May 14, 2012 10:15:00 PM GMT

IP Protocol Analysis

Description	Time In Violation Of Threshold	Total Time	% Time In Violation	Avg Rate In	Avg Rate Out	Max Rate In	Max Rate Out	Longest Violation
rtr-55-austin.nosos.com : ATM - PortB	15 hours	1 day	62.50 %	8.34 Kbps	5.42 Kbps	13.33 Kbps	8.67 Kbps	15 hours
[redacted] : Interface 1 -	1 day	1 day	100.00 %	831 bps	8.31 Kbps	1.33 Kbps	13.33 Kbps	1 day
[redacted] : Interface 2 -	1 day	1 day	100.00 %	8.31 Kbps	5.40 Kbps	13.33 Kbps	8.67 Kbps	1 day
[redacted] : Interface 3 -	1 day	1 day	100.00 %	35.42 Kbps	167.13 Kbps	56.80 Kbps	268.00 Kbps	1 day
[redacted] : Interface 4 -	1 day	1 day	100.00 %	167.13 Kbps	35.42 Kbps	268.00 Kbps	56.80 Kbps	1 day
[redacted] : Interface 5 -	1 day	1 day	100.00 %	2.49 Kbps	24.94 Kbps	4.00 Kbps	40.00 Kbps	1 day
[redacted] : Interface 6 -	1 day	1 day	100.00 %	24.94 Kbps	2.49 Kbps	40.00 Kbps	4.00 Kbps	1 day

You can click an interface name to display more information about that interface. For example, you may be able to view a calendar chart that shows the time and duration of a violation.

Edit an Analysis Report

When you view an Analysis report, you may want to review the Report Definition Summary to ensure that the report definitions are correct. This summary provides access to the Analysis wizard pages in case you want to change any settings.

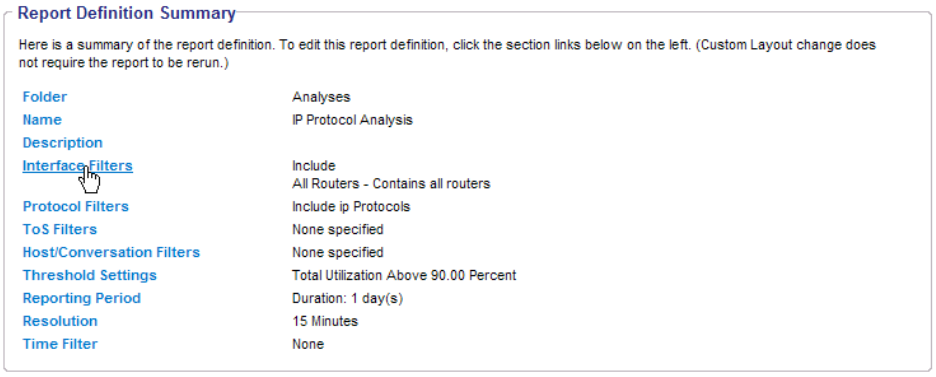
Follow these steps:

1. In the Report Settings section at the top of the report page, click Edit.

   The Report Definition Summary is displayed.

2. Review the current settings for the Analysis report.

3. Click the name of a category to open the associated page for making changes.



4. When you have made all the desired changes, click Queue Report to regenerate the report with the new settings.

   You return to the Reports list, which shows the modified report with a status of Queued. When the report has been regenerated and is ready to be viewed, the status displays as Complete.

   A scheduled report will be queued and will be generated at the next scheduled runtime.

Also See:

Create an Analysis Report (see page 136)

Manage Analysis Reports

Creating Analysis reports for your organization helps to troubleshoot various issues. Analysis report definitions are saved so you can generate an updated report at any time or can use the report definition as a template to create another report. As the number of reports grows, use the folder management system to keep the report definitions easy to find.

The report folders are listed on the left. The Analysis Reports folder is a built-in folder, which you can rename, but cannot delete. Create additional folders to provide more extended organization for your Analysis reports.

The right pane displays the names of the Analysis reports in the currently selected folder. Use the links at the top and bottom of the pane to delete or run selected reports, and to create or move report definitions.

This section contains the following topics:

Create a Report Folder (see page 143)
Rename a Report Folder (see page 144)
Move a Report to Another Folder (see page 144)

Create a Report Folder

Create your own report folders to group reports. For example, you can use folder names to identify the purpose for a set of reports.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. Click **New** at the bottom of the **Saved Report Folders** pane.

   A pop-up dialog opens.
3. Enter a name for the new folder in the pop-up dialog.
4. Click **OK**.

   The dialog closes and the new folder appears in the **Saved Report Folders** pane.

Rename a Report Folder

You can change the name of a report folder, including the name of the default report folder.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. In the **Saved Report Folders** pane, select the check box next to the report folder that you want to rename.
3. Click **Rename**.

   A pop-up dialog opens.
4. Enter a new name for the folder in the pop-up dialog.
5. Click **OK**.

   The dialog closes. The new report folder name appears in the **Saved Report Folders** pane.

Move a Report to Another Folder

You can add folders and move report definitions among the folders to make the report definitions easier to find or to help identify them.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. In the **Reports** pane, select the check box next to all the reports that you want to move.
3. Click **Move to Folder**.

   A pop-up dialog opens.
4. Select a destination folder from the list.
5. Click **OK**.

   The dialog closes. The reports are now in their new location, and are visible when you click that folder name in the **Saved Report Folders** pane.

Chapter 7: Site to Site Reports

Site to Site reports enable you to view volumes of data between two or more sites. A site may be defined as a collection of subnets that can also be discontiguous.

Use Site to Site reports to compare bytes in, rate in, bytes out, and rate out between pairs of sites. You can export the displayed data to a file in comma-separated value (CSV) format.

The reports may be configured for:

- Sites involved in the report (including creation of site definitions)
- Report schedule (scheduled or on demand)
- Time period
- Selecting data granularity (1-minute or 15-minute data)

You can use saved report definitions to generate an updated report at any time. As the number of reports grows, use the folder management system to keep the reports organized and accessible.

This section contains the following topics:

Open the Site to Site Page (see page 145)
Create a Site to Site Report (see page 146)
Define Site to Site Report Periods and Schedules (see page 148)
View a Site to Site Report (see page 150)
Create a Report Folder (see page 151)
Rename a Report Folder (see page 151)
Move a Report to Another Folder (see page 152)

Open the Site to Site Page

When you click the **Site to Site** tab, the **Saved Report Folders** pane is displayed on the left and any existing reports are displayed on the right.

You can perform the following tasks in the **Saved Report Folders** pane: create folders, rename folders, and delete custom folders. You cannot delete the default **Site to Site Reports** folder, which is built in to CA Network Flow Analysis. Create additional folders to provide more extended organization for your Site to Site reports.

The right pane displays the Site to Site report definitions in the currently selected folder. Use the links at the top and bottom of the pane to delete or run selected reports, as well as to create or move reports.

Create a Site to Site Report

Use the Site to Site wizard to create a site to site report step by step. The wizard guides you to select many options, such as the sites involved in the report, the report schedule, the data resolution (1-minute or 15-minute), and the reporting period.

Follow these steps:

1. Select **Site to Site** from the NFA console menu.
2. Click **Create New Report**.

   The Site to Site Report Wizard opens and shows the options **Create a new Site to Site report** and **Copy an existing report**.
3. Click **Create a new Site to Site report** and click **Next**.

   Note: Alternatively, you can select the **Copy an existing report** option and modify an existing report.

   The **Select Sites** page opens.
4. Select at least two sites for the report. You can either select an existing site or sites, or create a new site definition.

   To create a new site definition:

   a. Click **Create Site**.

   b. Enter **Site Name**, **Site Description** (optional), **Network Name**, and **Subnet**.

   c. (Optional) Click **Add Another Network** to add additional networks to the site definition.

   d. Click **Save**.

   The selected sites are added to the site list.
5. Click **Next**.

   The **Specify Schedule** page opens.
6. Select the type of reporting period from the **Period** list in the **Specify Schedule** page:

   - **duration**: Limits the reporting period to an amount of time, ending at the time the report runs. Enter the number of time units in the **Last** box.

     Select a unit of time from the list (**days**, **weeks**, **months**, or **years**).

     You can set up a schedule for a duration report or you can run the report on demand.

   - **start & end**: Specify a **Start** date and **End** date either by using the calendar icons or by selecting hour and time values from the lists. Hour values are expressed in 24-hour format.

7. Select the data resolution (1-minute or 15-minute) in the **Resolution** box.

   Note: 1-minute data resolution is limited to no more than 30 days, based on the storage allocated to your NFA system. If a duration of more than 30 days is required, use 15-minute data to get more complete results.

8. (Optional) Select the **Schedule** check box and specify the following options:

   - Schedule: Select the type from the Schedule list (Daily, Weekly, Monthly, Quarterly, Yearly).
     - **Daily**: Select the day or days of the week, time of day, and time zone for report generation.
     - **Weekly**: Select the day of the week, time of day, and time zone for report generation.
     - **Monthly**: Select either the date or the week in the month and day of the week. Select the time of day, and time zone for report generation.
     - **Quarterly**: Select a month that ends the first reporting quarter, time of day, and time zone.
     - **Yearly**: Select a month that ends the first reporting year, time of day, and time zone.

   Note: The options in the **Recurrence** section are available only if you select 'duration' as the reporting period type.

9. (Optional) Enter the email addresses of all the report recipients in the format *name@domain*. Separate multiple addresses with a comma or semi-colon.

10. Click **Next**.

    The **Enter Name** page opens.

11. Identify the report and its location:

    - **Folder**: Accept the default folder or select a different folder to contain the new report.
    - **Name**: Give the new report a name, which appears in the **Reports** list.
    - **Description**: (Optional) Add a description to help identify the report. For example, use the description to identify scheduled reports and to indicate distinguishing features of Duration reports.

    Click **Next**. The **Summary & Submit** page opens.

12. Review the information in the **Report Definition Summary**.

    - **Save**: Save the report definition and return to the **Site to Site** page.
    - **Save and Queue Report**: Queue the report to run and return to the **Site to Site** page.

Define Site to Site Report Periods and Schedules

When you define a Site to Site Report, you must specify the reporting time period and the resolution of the reporting data. You can define a specific, nonrecurring time period (for a start-and-end report) or you can choose a timespan that ends at the report runtime (for a duration report). You also have the option to set a duration report to regenerate on a recurring schedule and to have the automated reports sent out by email.

This section contains the following topics:

Specify a Reporting Period for Site to Site Reports (see page 148)
Specify Schedules for Auto-Generated Reports (see page 149)

Specify a Reporting Period for Site to Site Reports

The Site to Site Wizard provides a **Specify Schedule** page that defines the report time period. For a manually generated report, you can simply select a time period, resolution, and optional time filter. If you want to generate the report automatically at scheduled intervals, you can also use the **Schedule** option.

Follow these steps:

1. Select **Site to Site** from the NFA console menu if the Site to Site page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click **Edit** in the **Report Settings** section at the top of the report page.

   The **Report Definition Summary** page opens, which contains links to the Site to Site wizard pages.
3. Click **Reporting Period** to open the **Specify Schedule** page of the Site to Site wizard.

   Note: Site to Site reports always display data using the Greenwich Mean Time (GMT) time zone. If a user has set the time to a specific time zone, the reports display the data using GMT.
4. Select the type of reporting period from the **Period** list on the **Specify Schedule** page:
   - Duration: Include data from the block of time that immediately precedes the report runtime. Enter a number of days, weeks, months, or years.

     You can set up a schedule for a duration report or you can run the report on demand. To run a scheduled report on demand, you can make a copy of the report and can disable the schedule in the copy.

- Start and end: Include data from a specific, nonrecurring timespan. Use the calendars to specify a Start date and End date or select hour and time values from the lists.

  Hour values are expressed in 24-hour format.

  A start-and-end report runs on demand. You cannot set up a schedule for a start-and-end report.

5. Set the resolution (granularity for data collection) on the **Specify Schedule** page: Accept the default setting or select a value in the **Resolution** box.
6. (Optional) Select a time filter from the list on the **Specify Schedule** page, if your Administrator has created an appropriate time filter.
7. Click **Save Changes**.

   Your changes are saved and you return to the **Report Definition Summary**.
8. (Optional) Return to the report list by clicking one of these buttons:
   - **Return to Listing**: Return to the Site to Site page without queuing the report to run.
   - **Queue Report**: Queue the report to run and return to the Site to Site page.

Specify Schedules for Auto-Generated Reports

Use the **Schedule** option to set the Site to Site report to regenerate at specified times.

For example, suppose that you want to check network traffic during the monthly backups that occur on the last Sunday of each month. You schedule a report to be regenerated on the last Sunday of every month. Suppose that operating system updates occur on the 15th of every month. To check the network traffic during those updates, you schedule a report to be regenerated on the 15th of each month.

Note: The options in the **Recurrence** section are available only if you select 'duration' as the reporting period type.

Follow these steps:

1. Select **Site to Site** from the NFA console menu if the Site to Site page is not already open.
2. Put the report in editable mode: Click the name of the report. If the report has been run previously, it runs again. In this case, click **Edit** in the **Report Settings** section at the top of the report page.

   The **Report Definition Summary** page opens, which contains links to the Site to Site wizard pages.
3. Click **Reporting Period** to open the **Specify Schedule** page of the Site to Site wizard.

4. Click the **Schedule** check box and choose a recurrence interval from the list:
   - **Daily**: Select the day or days of the week the report will run.
   - **Weekly**: Select the day of the week the report will run.
   - **Monthly**: Select either a date or a week and day combination to specify the one day per month the report will run.
   - **Quarterly**: Select the month that ends the first quarter in which the report will run. Starting with the specified quarter, the report will run on the last day of each quarter.
   - **Yearly**: Select the month that ends the first year the report will run. The report runs on the last day of the year.

   For all schedule interval types, select the time of day and time zone for the report to run.
5. (Optional) **Email Results To**: Enter the email addresses of anyone who should receive the report by email. Use the format *name@domain*. Separate multiple addresses with a comma or semi-colon.
6. Click **Save Changes**.

   Your changes are saved and you return to the Report Definition Summary.
7. (Optional) Return to the report list by clicking one of these buttons:
   - **Return to Listing**: Return to the **Site to Site** page without queuing the report to run.
   - **Queue Report**: Queue the report to run and return to the **Site to Site** page.

View a Site to Site Report

Complete the following steps to view an existing Site to Site report.

Follow these steps:

1. Select **Site to Site** from the NFA console menu if the Site to Site page is not already open.
2. Click the parent folder that contains the report.

   The list of reports in the folder opens.
3. Click the check box next to the report that you want to view.
4. Click **Run**.

   A verification message opens.
5. Click **OK**.

6. Refresh the view until the report status is Complete.

   The report results are displayed.

Create a Report Folder

Create your own report folders to group reports. For example, you can use folder names to identify the purpose for a set of reports.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. Click **New** at the bottom of the **Saved Report Folders** pane.

   A pop-up dialog opens.
3. Enter a name for the new folder in the pop-up dialog.
4. Click **OK**.

   The dialog closes and the new folder appears in the **Saved Report Folders** pane.

Rename a Report Folder

You can change the name of a report folder, including the name of the default report folder.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. In the **Saved Report Folders** pane, select the check box next to the report folder that you want to rename.
3. Click **Rename**.

   A pop-up dialog opens.
4. Enter a new name for the folder in the pop-up dialog.
5. Click **OK**.

   The dialog closes. The new report folder name appears in the **Saved Report Folders** pane.

Move a Report to Another Folder

You can add folders and move report definitions among the folders to make the report definitions easier to find or to help identify them.

Follow these steps:

1. Navigate to the page for the report type: **Custom Reporting**, **Flow Forensics**, **Analysis**, or **Site to Site**.
2. In the **Reports** pane, select the check box next to all the reports that you want to move.
3. Click **Move to Folder**.

   A pop-up dialog opens.
4. Select a destination folder from the list.
5. Click **OK**.

   The dialog closes. The reports are now in their new location, and are visible when you click that folder name in the **Saved Report Folders** pane.

Chapter 8: Views in Performance Center

You can view data from CA Network Flow Analysis in Performance Center Console dashboards and Interface pages. Some of the views can be found in both consoles, although the view format and options may be different.

The topics in this section describe the Performance Center views that have CA Network Flow Analysis data. The topics also describe the basics of working with the views.

This section contains the following topics:

Dashboards and Views (see page 153)
CA Network Flow Analysis Views in CA Performance Center (see page 156)
CA Anomaly Detector Views in Performance Center (see page 202)
Customizing Dashboards and Views (see page 212)
Sharing Data with Other Users (see page 227)
Organizing Dashboards in Menus (see page 234)

Dashboards and Views

Dashboards are dynamic report-building pages in the Performance Center Console. Dashboards are accessible from the Dashboards tab (CA PC) or Reports tab (NPC). Each dashboard is a collection of views that present data from registered data sources on a single web page. The layout, views, time interval, and group context of each dashboard can be customized.

Note: Your user account role rights determine the dashboards that you can see.

Reports are static output from an on-demand selection or an exported dashboard page. Reports that you export from a dashboard create a static data set from the data and information in the associated dashboard. On-demand reports capture a data set from a single managed item or group in the Inventory. You can print reports, send them by email, or export them in CSV or PDF format. For each format, the report captures a selected data set.

Dashboards are organized in menus. *Menus* in the Performance Center Console are lists of items in the Dashboards tab (CA PC) or Reports tab (NPC). Menus group similar dashboards or report pages together. By default, Administrators and Designers can customize menus and assign them to user account roles.

Performance Center has a set of built-in dashboards and menus, which are available for use immediately after your administrator registers the product as a data source. Users who have the required role rights can customize dashboards, menus, and views to create a custom system for individual operators.

The menus and dashboards that are available to you are displayed when you hover over or click the Dashboards or Reports tab.

Performance Center Dashboards

Performance Center dashboards display views of data from registered data sources such as CA Network Flow Analysis. *Views*, or *data views*, present statistical data, usually in a graph or table format. Each view represents a discrete set of collected data. Depending on your user account role rights, you can add and edit individual views or remove them from a dashboard page. In some cases, you can export the data to a file in CSV format.

View placement on dashboard pages is flexible. Users with the required role rights can customize dashboards. They can, for example, place views of application performance data beside views of volume data to help troubleshoot issues from a single page.

The predefined (factory) dashboards are organized into workflows. You can drill down from Top N views to more detailed metrics from a narrow context, such as an individual device. Workflows let you see data that may be related to the metric you are reviewing.

Administrators can create custom groups to display data for a specific set of sites, devices, or interfaces. You can apply groups to dashboards by using the group selector (the 'change' link at the top left). You can change the “context” of the dashboard to analyze data for specific groupings at the summary, device, or item level.

Views that show data for a group are CA Performance Center-generated views that contain rollups of data from data sources. Views that show data for a server or device, or detailed metrics from a narrow context often provide a drilldown path directly to the data source. The Single Sign-On feature lets you navigate seamlessly from a dashboard to a data source interface.

Types of Report Pages

Two categories of dashboards are available by default or through customization:

- *Summary pages* provide high-level information, such as averages from groups of managed items. Summary dashboards often provide a drilldown path to more detailed, related pages from a selected context.
- *Context pages* provide specific, focused performance or status data from a narrow context, such as a single router or server. These pages are available as drill-down links or tabs from Summary dashboards.

To drill in to a detailed view from a Summary dashboard, take one of the following steps:

- Right-click the item to select the context page that you want to see.
- Click the item to open the default context page.

Note: Your role rights must include the ability to Drill into Views.

Default sets of context pages are available for individual devices, interfaces, and servers. These pages include a set of customizable tabs that let you access more specific context data for a selected managed item. For example, the Router context includes tabs for Health, Utilization, and Error data.

Context Page Navigation

You can frequently access more information about individual managed items from dashboards. Most dashboards are composed of views of summary data, such as hourly rollups or averages from a group of items. If additional data is available from the data source, you can click linked items on the dashboard page to drill down into *context pages*.

Note: The role right to Drill into Views is required.

The views on context pages show filtered data from a narrow context, such as a view of data from a single managed item. Use the links to drill down into specific data and home in on the source of a performance problem.

In data views from some data sources, you can also right-click the name of an item in a table view to access a menu. For example, right-click the link that corresponds to an item name in the Inventory section. A menu lets you select a related context page, containing more granular data.

Finally, some context pages include tabs to additional pages of detailed data. Click a tab to see data that has been filtered by a selected managed item or type of item.

CA Network Flow Analysis Views in CA Performance Center

You can display CA Network Flow Analysis data in the CA Performance Center Console in several ways:

Built-in CA Performance Center Dashboards with Enterprise-Wide Data:

- **Infrastructure Overview dashboard**:
  - Interfaces Over Threshold (see page 165)
  - Routers with the Most Flow Traffic (see page 168)
  - Top Enterprise Hosts by Volume (see page 160)
  - Top Enterprise Protocols by Volume (see page 161)
  - Top Flows by Interface (see page 163)
  - Top IP Interface Utilization (Flow) (see page 162)
- **Management: Management Overview dashboard**:
  - Top Flows by Interface (see page 163)
  - Top IP Interface Utilization (Flow) (see page 162)
- **Management: Network Overview dashboard**:
  - Top Enterprise Hosts by Volume (see page 160)
  - Top Enterprise Protocols by Volume (see page 161)
- **Capacity Planning: Router/Switch Capacity Watch Lists dashboard**:
  - Routers with the Most Flow Traffic (see page 168)

Custom CA Performance Center Dashboard Views with Interface-Specific Data: Display interface-specific CA Network Flow Analysis data by adding the following views (see page 226):

- Calendar Heat Chart (Flow) (see page 169)
- Stacked Protocol Trend (see page 172)
- Stacked ToS Trend (see page 175)
- Top Conversations (Bar) (see page 183)
- Top Conversations (Pie) (see page 185)
- Top Conversations (Table) (see page 187)
- Top Hosts (Bar) (see page 189)
- Top Hosts (Pie) (see page 191)

- Top Hosts (Table) (see page 193)
- Top Protocols (Bar) (see page 196)
- Top Protocols (Pie) (see page 198)
- Top Protocols (Table) (see page 200)
- ToS Summary (Pie) (see page 178)
- ToS Summary (Table) (see page 180)

Built-In CA Performance Center Interface Page Views with CA Network Flow Analysis Data:

- **IP Performance tab**:
  - Stacked Protocol Trend (see page 172)
  - Top Conversations (Pie) (see page 185)
  - Top Hosts (Pie) (see page 191)
  - ToS Summary (Pie) (see page 178)
- **CBQoS tab**:
  - Stacked Protocol Trend (see page 172)
  - Stacked ToS Trend (see page 175)

CA Network Flow Analysis Views in CA NetQoS Performance Center

You can display CA Network Flow Analysis data in the CA NetQoS Performance Center Console in several ways:

Enterprise-Wide Data on Built-in Dashboards in the CA NetQoS Performance Center Console:

- **Enterprise Dashboard**:
  - Interfaces Over Threshold (see page 165)
  - Top Enterprise Hosts by Volume (see page 160)
  - Top Enterprise Protocols by Volume (see page 161)
- **Traffic Analysis**:
  - Interfaces Over Threshold (see page 165)
  - Top Enterprise Hosts by Volume (see page 160)
  - Top Enterprise Protocols by Volume (see page 161)
  - Top IP Interface Utilization (Flow) (see page 162)

- **Network Overview**:
  - Top Enterprise Hosts by Volume (see page 160)
  - Top Enterprise Protocols by Volume (see page 161)
- **Routers/Switches Overview**:
  - Interfaces Over Threshold (see page 165)

Custom Dashboard Views with CA Network Flow Analysis Data

Display CA Network Flow Analysis data on custom report pages by adding the following views:

- Interfaces Over Threshold (see page 165)
- Multi-Interface Stacked Protocol Trends (see page 172)
- Multi-Interface Stacked ToS Trends (see page 175)
- Multi-Interface Utilization Trends
- Routers With the Most Flow Traffic (see page 168)
- Top Enterprise Hosts By Volume (see page 160)
- Top Enterprise Protocols By Volume (see page 161)
- Top Flows by Interface (see page 163)
- Top IP Interface Utilization (Flow) (see page 162)

Interface Page Views with CA Network Flow Analysis Data in the CA NetQoS Performance Center Console:

- **Interface Capacity tab**:
  - Stacked Protocol Trend (see page 172)
  - Top Conversations (Pie) (see page 185)
  - Top Hosts (Pie) (see page 191)
- **Interface QoS tab**:
  - Stacked Protocol Trend (see page 172)
  - Stacked ToS Trend (see page 175)
  - Top Conversations (Pie Chart) (see page 185)
  - Top Hosts (Pie Chart) (see page 191)
  - Top Protocols (Pie Chart) (see page 198)
  - ToS Summary (Table) (see page 180)

Custom Interface Tab with CA Network Flow Analysis Data Views

Display CA Network Flow Analysis data on custom Interface pages by adding the following views:

- Calendar Chart (Flow) (see page 169)
- Multi-Protocol Baseline Trends
- Top Conversations (Bar Chart) (see page 183)
- Top Conversations (Pie Chart) (see page 185)
- Top Conversations (Table) (see page 187)
- Top Hosts (Bar Chart) (see page 189)
- Top Hosts (Pie Chart) (see page 191)
- Top Hosts (Table) (see page 193)
- Top Protocols (Bar Chart) (see page 196)
- Top Protocols (Pie Chart) (see page 198)
- Top Protocols (Table) (see page 200)
- ToS Summary (Pie Chart) (see page 178)
- ToS Summary (Table) (see page 180)
- Stacked Protocol Trend (see page 172)
- Stacked ToS Trend (see page 175)

Enterprise-Level Views

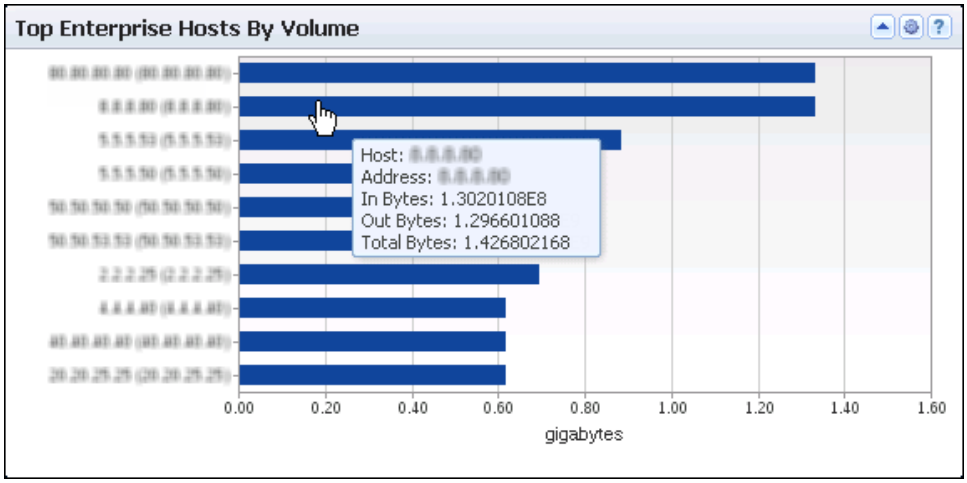
You can view enterprise-wide data from CA Network Flow Analysis in several Performance Center dashboard views, which are described in the topics that follow. The *top* interfaces, hosts, protocols, or ToS are the ones that have the highest traffic volume during the reporting period.

This section contains the following topics:

Top Enterprise Hosts by Volume (see page 160)
Top Enterprise Protocols by Volume (see page 161)
Top IP Interface Utilization (Flow) (see page 162)
Top Flows by Volume (see page 163)
Interfaces Over Threshold (see page 165)
Routers with the Most Flow Traffic (see page 168)

Top Enterprise Hosts by Volume

The Top Enterprise Hosts by Volume view in the Performance Center Console shows the enterprise hosts that have the highest traffic volume, as reported by CA Network Flow Analysis. The example graphic shows the view in the CA Performance Center Console.



The view shows a bar for each of a maximum of 10 hosts that have the highest traffic volume. The bar chart includes the following information:

Host

Identifies the host server by its name and IP address (Y-Axis). If an administrator has defined an alias for the device, the alias is displayed. Otherwise, the discovered device name is displayed.

Volume

Measures the total amount of data sent to or from the host, expressed in a scale that is appropriate for the highest-volume host (X-Axis).

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Infrastructure Overview, Network Overview, or Summary context custom dashboard (see page 220)
- (NPC) Enterprise, Traffic Analysis, Network Overview, and custom dashboards

Available Actions

You can perform several actions in this view, including the following ones:

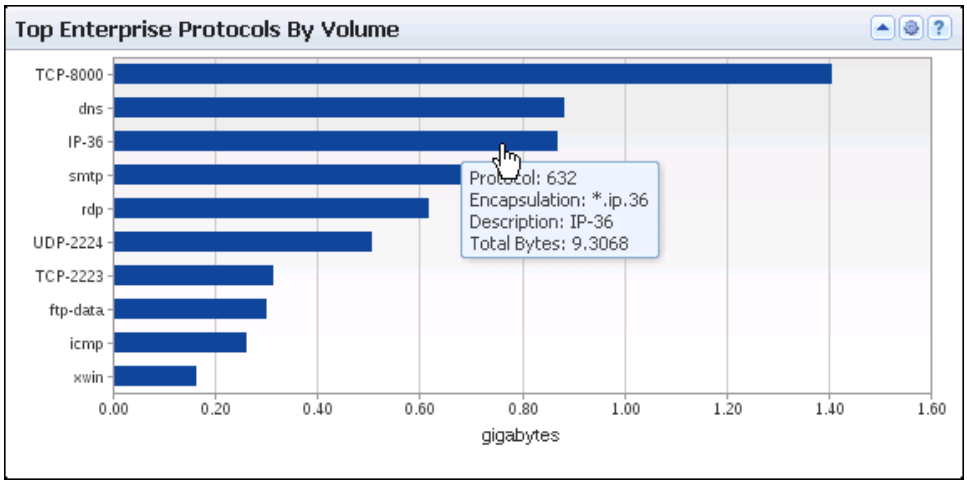
- Change the view name by editing the view settings (see page 215).
- Display details in a Tooltip by holding your cursor over a bar.
- Click a name or bar to open related views in the NFA console.

Find the Comparable View in the NFA Console

The Top Enterprise Hosts by Volume view is similar to the Top Hosts view on the Enterprise Overview page in the NFA console.

Top Enterprise Protocols by Volume

The Top Enterprise Protocols by Volume view in the Performance Center Console shows the protocols with the highest volume of network traffic across the enterprise. The example graphic shows the view in the CA Performance Center Console.



The view includes the following information for a maximum of 10 protocols that are associated with the highest traffic during the reporting period:

Protocol

Identifies the protocol by its keyword (Y-Axis).

Volume

Measures the total amount of data associated with the protocol expressed in a scale that is appropriate for the highest-volume protocol (X-Axis).

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Infrastructure Overview or Network Overview dashboard; Summary context view in a custom dashboard (see page 220)
- (NPC) Enterprise, Traffic Analysis, Network Overview, and custom dashboards

Available Actions

You can perform several actions in this view, including the following ones:

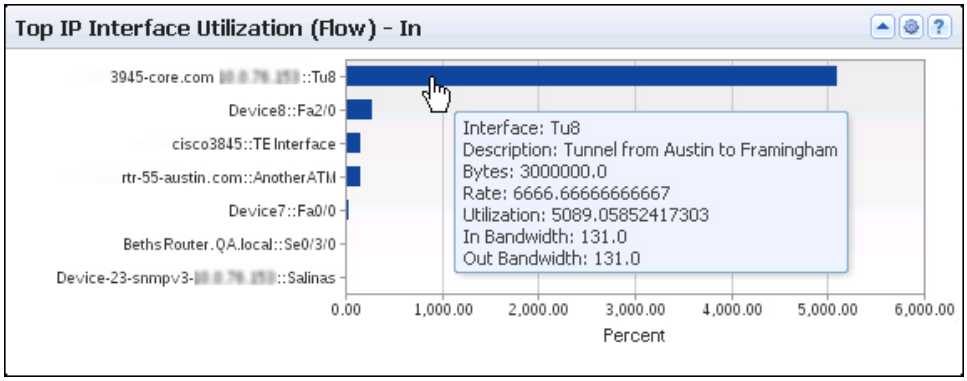
- Change the view name in the view settings (see page 215).
- Display details in a Tooltip by holding your cursor over a bar.
- Click a name or bar to open related views in the NFA console.

Find the Comparable View in the NFA Console

The Top Enterprise Protocols by Volume view in the Performance Center Console is similar to the Top Protocols view on the Enterprise Overview page in the NFA console.

Top IP Interface Utilization (Flow)

The Top IP Interface Utilization (Flow) views in the Performance Center Console show the high-utilization interfaces from across the enterprise. The example graphic shows the view in the CA Performance Center Console.



The view includes the following information for a maximum of 10 top interfaces during the reporting period:

Name

Identifies the interface by its device name/interface name (Y-Axis).

Percent (Utilization)

Measures the percentage of interface capacity that was used (X-Axis). The view shows the utilization of either inbound or outbound capacity.

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Infrastructure Overview and Management Overview dashboards; Summary-type view in a custom dashboard (see page 220)
- (NPC) Traffic Analysis and custom dashboards

Available Actions

You can perform several actions in this view, including the following ones:

- Change the data direction, view name, and context (the interfaces that are used) by editing the view settings (see page 215).
- (NPC) Change the utilization thresholds.
- Display details in a Tooltip by holding your cursor over a bar.
- Click a name or bar to open related information on the Interface context pages.

Find the Comparable View in the NFA Console

The Top IP Interface Utilization (Flows) view in the Performance Center Console is similar to the Interface Utilization view on the Enterprise Overview page in the NFA console.

Top Flows by Volume

The Top Flows by Volume views in the Performance Center Console show the interfaces across the enterprise that have the highest volume of inbound or outbound traffic.

The view shows the following information for a maximum of 10 top interfaces:

Name

Identifies the interface by its device name (such as its router name), followed by a colon (:) and the interface name (Y-Axis).

Volume

Measures the volume of flow data on the interface (X-Axis) expressed in a scale that is appropriate for the highest-volume interface.

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Infrastructure Overview and Management Overview dashboards; Summary context view in a custom dashboard (see page 220)
- (NPC) Custom dashboard

Available Actions

You can perform several actions in this view, including the following ones:

- Change the data direction or the view name by editing the view settings (see page 215).
- Display details in a Tooltip by holding your cursor over a bar. The Tooltip identifies the interface position among the top 10, with Interface 0 as the one with the highest traffic volume.
- Click a name or bar to open related information on the Interface context pages.

Find Flow Volume Data in the NFA Console

To see the flow volume of multiple top interfaces in the NFA console, create and run a Custom report. For example, you can view flow volume for the top interfaces in summary pie charts, summary tables, trend charts, and stacked trend charts. For instructions, see the topic "Set Up Custom Reports" in the *CA Network Flow Analysis Operator Guide.*

To see the flow volume of a single top interface in the NFA console, drill into details from the Enterprise Overview page:

1. Click an interface name or bar in one of the Top Interfaces views on the NFA console Enterprise Overview page.
2. Select Flows from the list labeled "For this interface, show me" on the Interface page that opens.
3. Click the gray bar on the left edge of the page to change the presentation mode.

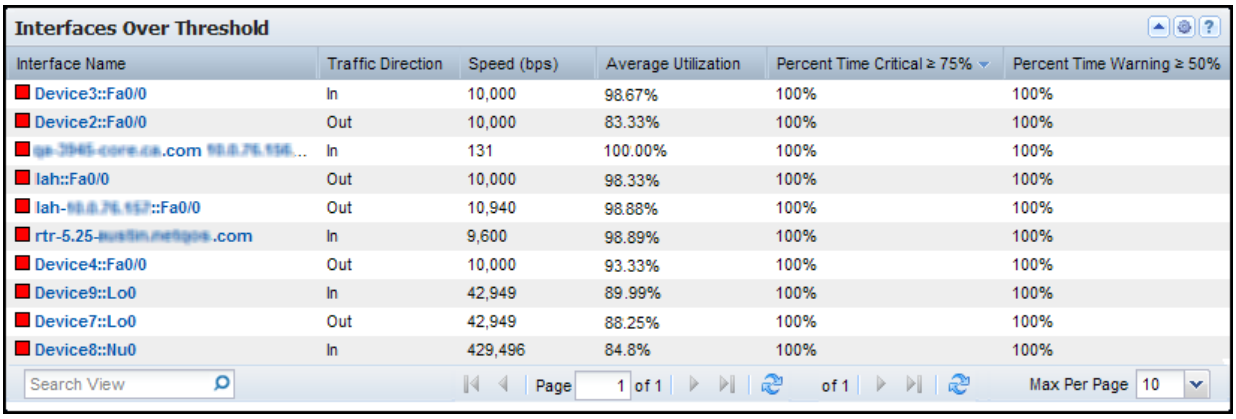
4. Click Volume in the Presentation menu that opens.

   The Flows views display a trend chart of inbound flow volume and outbound flow volume.

   To jump to the Performance Center Interface Pages data for the selected interface, click the arrow next to the Flows title and select CA PC/NPC Interface Performance.

Interfaces Over Threshold

The Interfaces Over Threshold view in the Performance Center Console lists the most heavily used interfaces throughout the enterprise. A table summary shows the interfaces with utilization that exceeds the configured thresholds. The example graphic shows the view in the CA Performance Center Console.



Interfaces Over Threshold

Interface Name	Traffic Direction	Speed (bps)	Average Utilization	Percent Time Critical ≥ 75%	Percent Time Warning ≥ 50%
Device3::Fa0/0	In	10,000	98.67%	100%	100%
Device2::Fa0/0	Out	10,000	83.33%	100%	100%
[redacted].com [redacted]	In	131	100.00%	100%	100%
lah::Fa0/0	Out	10,000	98.33%	100%	100%
lah-[redacted]::Fa0/0	Out	10,940	98.88%	100%	100%
rtr-5.25-[redacted].com	In	9,600	98.89%	100%	100%
Device4::Fa0/0	Out	10,000	93.33%	100%	100%
Device9::Lo0	In	42,949	89.99%	100%	100%
Device7::Lo0	Out	42,949	88.25%	100%	100%
Device8::Nu0	In	429,496	84.8%	100%	100%

Search View | Page 1 of 1 | of 1 | Max Per Page 10

The Interfaces Over Threshold view shows the interfaces whose traffic exceeded the configured thresholds during the reporting period. The view includes the following information for up to ten top interfaces:

Status

Identifies the interface status as Critical (Red - Meets or exceeds the user-defined Critical threshold) or Warning (Orange - Meets or exceeds the user-defined Warning threshold).

Interface Name

Identifies the interface by its name. (Depending on the application setting for the name format, the name may be prefixed by the device name.)

Traffic Direction

Shows whether the data was inbound or outbound on the interface.

Speed

(CA PC) Records the data speed that is defined for the interface.

Average Utilization

Measures the average percentage of interface capacity that was used.

Percent Time Critical

Shows the percentage of the reporting period the interface met or exceeded the Critical threshold.

Percent Time Warning

Shows the percentage of the reporting period the interface met or exceeded the Warning threshold.

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Infrastructure Overview dashboard; Summary context view in a custom dashboard (see page 220)
- (NPC) Enterprise, Traffic Analysis, Routers/Switches Overview, or custom dashboard

Available Actions

You can perform several actions in this view, including the following ones:

- Change the thresholds, view name, and utilization settings as described in this topic.
- (CA PC) Change the columns that are shown in the table: Click near a column border, click Columns, then choose the columns to display.
- Click an interface name to open the Interface context pages. You can review details or open additional views of interface data.

How to Change the View Settings

Follow these steps:

1. Open the dialog for editing the view:
   - (CA PC) Click the Edit icon  in the view title bar and click Edit.
   - (NPC) Click the arrow next to the title name and select Edit from the menu.

   The dialog opens.
2. (Optional) Edit the text in the Title field to change the name in the view title bar.

3. (Optional) Edit the thresholds by changing any of the following values in the Interfaces Over Threshold Settings section:

   - Critical - % Utilization: Specify the utilization percentage for flagging interfaces with a status of Critical, the highest level of concern. If the utilization for an interface has met or exceeded this percentage, it is marked with a red (Critical) status symbol.
   - Warning - % Utilization: Specify the utilization percentage for flagging interfaces with a status of Warning. If the utilization for an interface has met or exceeded this percentage, but has not met the Critical threshold, the interface is marked with an orange (Warning) status symbol.
   - Affected % of reporting period: Specify the percentage of the reporting period that a utilization percentage must be violated in order for the threshold to be met.

     For example, if the 'Affected % of reporting period' value is 25, the threshold is met for the interfaces that have a utilization level at or above the threshold level during 25% of the reporting period. With the default reporting period of 24 hours, the list includes interfaces at or above the threshold value for six hours or more during the previous 24 hours.

4. (Optional) (NPC) Define a new context to filter the interfaces that can appear in the view: Select the Filter by value and select a context type and setting in the Select Context dialog.

   Interfaces that are not in the selected group do not appear in the view, even if they violate a threshold. If you select a group, the defined context appears under the view title.

5. (Optional) Specify which users are affected by the settings: Select a value from the Apply Changes list:

   - For All Tenant Users: Saves the changes so that they are only available to users associated with your tenant (possibly the Default Tenant).
   - My User Account: Saves the changes to your user account as a default for this view.
   - My Current Session: Reverts the changes when you log out.

6. Click Save to save your changes, Cancel to exit without saving changes, or Use Defaults to restore the default values.

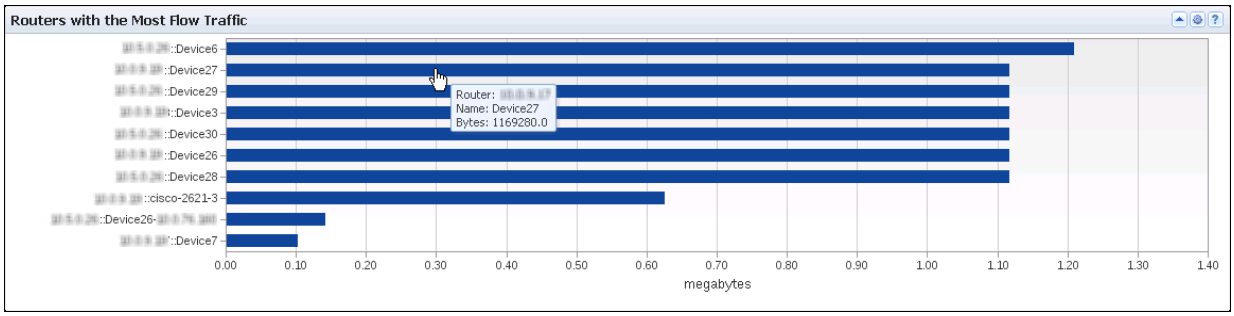
   The dialog closes and the view reflects your changes.

Find the Comparable View in the NFA Console

The Interfaces Over Threshold view in the Performance Center Console is similar to the Interface Utilization view on the Enterprise Overview page in the NFA console.

Routers with the Most Flow Traffic

The Routers with the Most Flow Traffic view in the Performance Center Console displays the routers in your network that have the highest traffic. Traffic use is measured for both inbound and outbound traffic during the reporting period, as reported by CA Network Flow Analysis. The example graphic shows the view in the CA Performance Center Console.



The view includes the following information for a maximum of 10 routers:

Name

Consists of the router IP address and device name (Y-Axis). If an administrator defined an alias for the device item, the alias is displayed. Otherwise, the discovered device name is displayed.

Volume

Measures the total amount of traffic for the router expressed in megabytes, for example (X-Axis).

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Infrastructure Overview and Router/Switch Capacity Watch Lists dashboards; Summary-type view in a custom dashboard (see page 220)
- (NPC) Custom dashboard

Available Actions

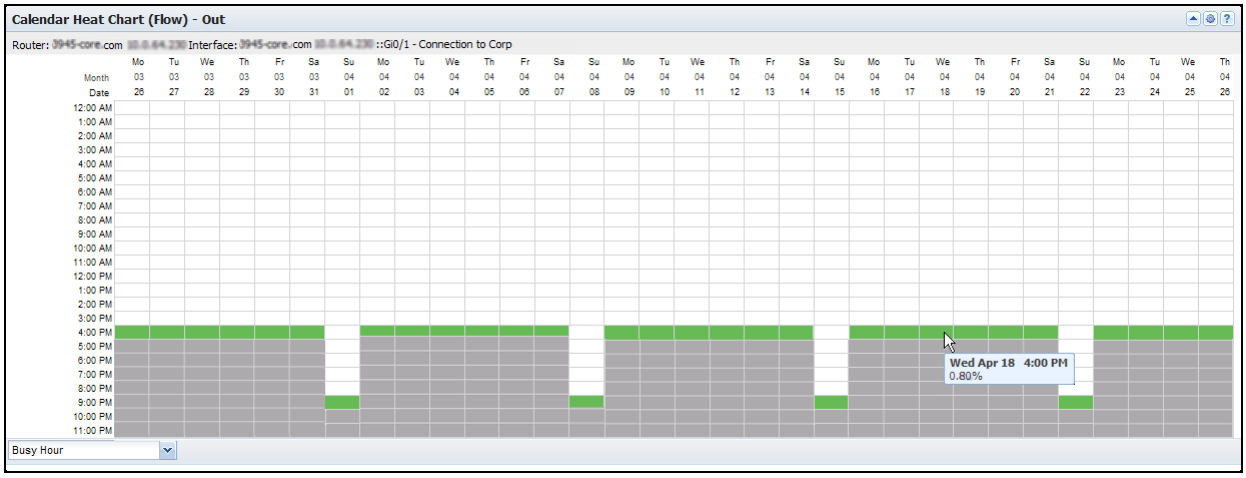
You can perform several actions in this view, including the following ones:

- Change the view name by editing the view settings (see page 215).
- (NPC) Change the context (the routers that can be used in the view).

- Display details in a Tooltip by holding your cursor over a bar.
- Click a router bar to view details in the Performance Center Router pages.

Calendar Chart (Flow)

The Calendar Heat Chart (Flow) view maps the utilization percentage of the selected interface over time. The example graphic shows the view in the CA Performance Center Console.



This view makes it easy to detect recurring data patterns. Finding a pattern can help you identify the source of high traffic rates and potential performance issues. You might discover that the high traffic rates you thought were intermittent actually follow a pattern. The view can show the hour of each day when utilization is the highest, for example.

Each color represents a severity range that is calculated as a percentage of total capacity. High utilization is shown in orange and red. Low utilization is shown in green and blue.

The view includes the following information:

Identifier

Consists of the router name, interface name, and interface description (under the view title). The interface description consists of the ifDescr value by default, so it may be slightly different than the interface description that is shown in the NFA console.

(NPC) The identifier line also includes the interface speed.

Month, Date, and Day of the Week

Denote the day that the traffic occurred (X-Axis columns).

Hour

Denotes the hour of the day that the traffic occurred (Y-Axis).

Opening the View

To see the Calendar Heat Chart view in the Performance Center Console, add it to a custom dashboard (see page 226).

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 220)
- (NPC) Interface Pages (with an interface selected): Custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the data direction and view name as described in this topic.
- (CA PC) Display details in a Tooltip by holding your cursor over a cell.
- (CA PC) Click Show All and choose a pattern-matching filter. For example, select Busy Hour to show only the data for the busiest hour of each day.

How to Change the View Settings

Follow these steps:

1. Open the dialog for editing the view:
   - (CA PC) Click the Edit icon  in the view title bar and click Edit.
   - (NPC) Click the arrow next to the title name and select Edit from the menu.

   The dialog opens.
2. (Optional) Edit any of the following settings in the Calendar Heat Chart (Flow) Settings section:
   - Title: Change the name that appears in the view title bar.
   - (CA PC) Time Display Format: Select the time format for the chart, either 12 hours or 24 hours.

- (CA PC) Zone Start: Set the starting value of each heat zone. The defaults are based on IT industry standards for performance. For example, the default Red Zone Start value is 70 percent utilization.

  Defaults: Green Zone Start = 0, Yellow Zone Start = 50, Orange Zone Start = 60, Red Zone Start = 70.

- (CA PC) Business Week Start: Select the day that starts the business week.

  Default: Monday.

- (CA PC) Direction Settings: Select the direction of traffic on the selected interface to include in the report:
  - Out: Outbound on the interface.
  - In: Inbound on the interface.
  - Total: Combination of inbound and outbound traffic.

3. (Optional) (CA PC) Change the context for the view data: Select a different interface from the Context Settings table.
4. (Optional) Specify which users are affected by the setting changes: Select a value from the Apply Changes list:
   - Default for All Users: Saves the changes to all user accounts as a default for this view.
   - For All Tenant Users: Saves the changes so that they are only available to users associated with your tenant.
   - My User Account: Saves the changes to your user account as a default for this view.
   - My Current Session: Reverts the changes when you log out.
5. Click Save to save your changes.

   The settings dialog closes. The view refreshes to reflect your updates.

Find the Comparable View in the NFA Console

To display Calendar Chart data for an interface in the NFA console, select an interface on the Interface page and select the following options:

- Report type: Utilization.
- Presentation menu option: Direction In or Direction Out.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Interface: Stacked Trend Charts

The Stacked Trend views show the top protocol or ToS values that are used for traffic on the currently selected interface. The views are described in the topics that follow.

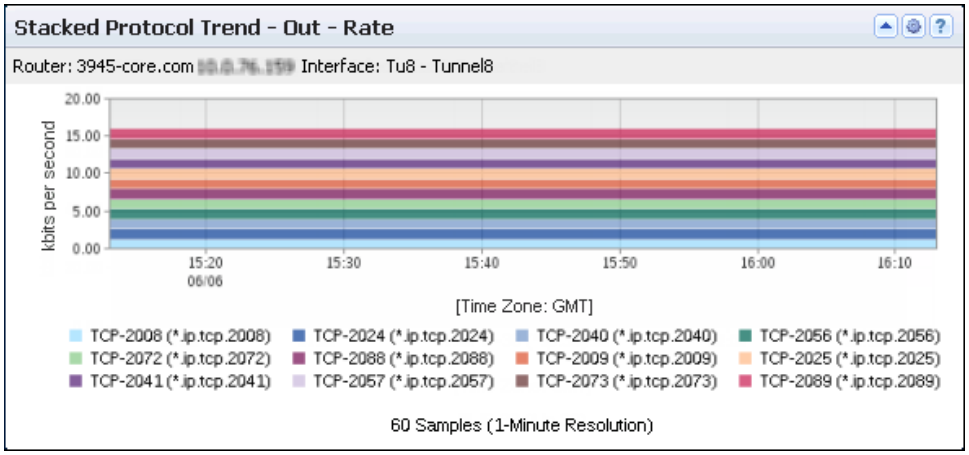
This section contains the following topics:

Stacked Protocol Trend (see page 172)
Stacked ToS Trend (see page 175)

Stacked Protocol Trend

The Stacked Protocol Trend views in the Performance Center Console show the protocols that are used the most heavily for traffic on the selected interface. The views also show when the traffic occurred.

The example graphic shows a Stacked Protocol Trend view in the CA Performance Center Console. A timeline of rates is included for each listed ToS value. You can configure the view to display rate, utilization, or volume information.



The views include the following information:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

Protocol Bands

Show the data rate, the data volume, or the interface capacity utilization for each top protocol that is associated with traffic on the interface.

Time (All Views)

Point in time during data transmission--expressed in hours and minutes (X-Axis).

Measurement Setting:

- **Rate:** Data rate at each point in time expressed in kilobits per second, for example (Y-Axis). The rate is calculated by dividing the data volume by the elapsed transmission time.
- **Bytes** (Volume): Data volume at each point in time expressed in kilobytes, for example (Y-Axis).
- **Percent** (Utilization): Percentage of the total interface capacity that the protocol uses (Y-Axis). The utilization percentage is calculated by dividing the data rate by the data speed.

Depending on the data direction, the view shows inbound, outbound, or total data on the interface.

Legend

Identifies the protocol for each color band by protocol keyword and tcp/udp port (bottom of the view).

Performance Center views show the data from the time range that is defined for the page.

Opening the Views

To see these views in the Performance Center Console, go to one of the following locations:

- (CA PC) Interface Pages (with an interface selected): Custom dashboard (see page 226); IP Performance and CBQoS tabs
- (NPC) Interface Pages (with an interface selected): Interface Capacity, Interface QoS, and custom tabs

Note: You can add Multi-Interface Stacked Protocol Trend views to a custom dashboard or to a custom tab in the Interface pages in the CA NetQoS Performance Center Console. This view consists of a group of interface-specific stacked protocol trend charts

Available Actions

You can perform several actions in this view, including the following ones:

- Change the traffic direction, the type of measurement (Rate, Volume, or Utilization), and the view name by editing the view settings (see page 215). If the view is on a custom interface context dashboard in the CA Performance Center Console, you can change the interface.
- (CA PC) Zoom in to narrow the time frame.

- (CA PC) Display only the data for a single protocol: Right-click a protocol in the legend at the bottom of the view and click Focus. This menu is available for a view that has multiple protocols. (This option is active when the legend contains multiple protocols.)
- (CA PC) Hide data for one of multiple protocols: Right-click a protocol in the legend at the bottom of the view and click Hide.
- (CA PC) Position your cursor over legend items to display explanatory Tooltips.
- Jump to details on an NFA console Interface page by double-clicking a protocol in the legend.
- (NPC) Jump to details on the corresponding Interface page by double-clicking a protocol band in the view. To choose a destination tab on the Interface page, right-click the protocol band and select a tab from the menu.

Find Protocol Trend Data in the NFA Console

You can display protocol volume in the NFA console in trend charts or stacked trend charts for a selected interface:

- *Overview* -- Report type: Overview. Presentation menu options: Mixed Chart; Volume.

  Views: Stacked Protocol Trend (In and Out) for the Top N Protocols, plus other overview views.

- *Top N Protocols, Stacked Trends* -- Report type: Protocols. Filter: Top N Protocols. Presentation menu options: Stacked Trend Chart; Volume.

  Views: Stacked Trend for the Top N Protocols (In, Out, and Total).

- *Top N Protocols, Trends* -- Report type: Protocols. Filter: Top N ToS. Presentation menu options: Trend Chart; Volume.

  Views: Trend (In, Out, and Total) for each of the Top N Protocols.

- *Single Protocol* -- Report type: Protocols. Filter: Single protocol.

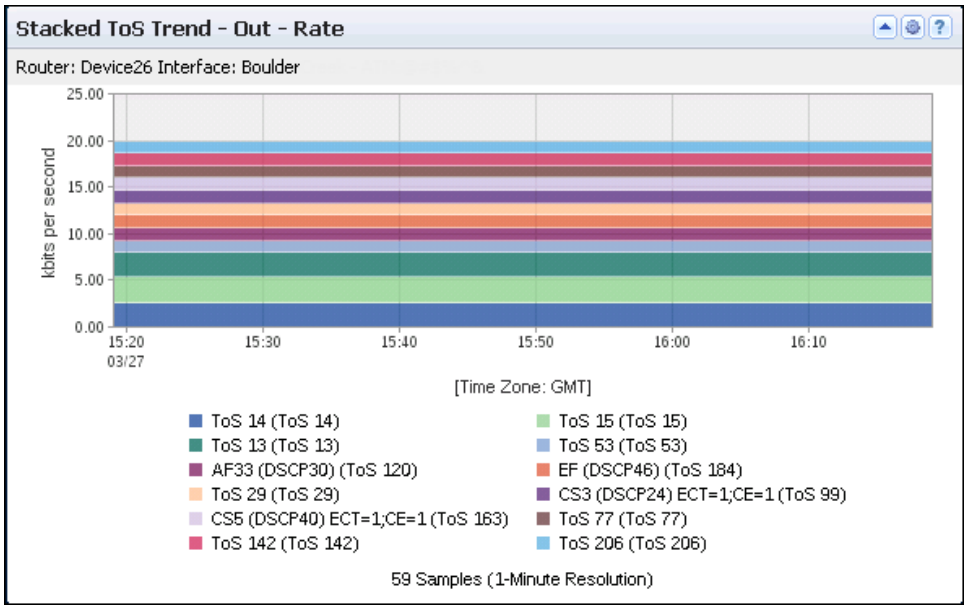
  Views: (Depending on the selected report subtype): trends, stacked trends, trend summaries, and multi-trend summaries for protocols, protocol hosts, and protocols in conversations.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Stacked ToS Trend

The Stacked ToS Trend views show the interface traffic for the top ToS, including the time the traffic occurred.

The example graphic shows a Stacked ToS Trend view in the CA Performance Center Console. A timeline of rates is included for each ToS value. You can configure the view to display rate, utilization, or volume information.



The view includes the following information:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

ToS Bands

Show the data rate, data volume, or interface capacity utilization for each top ToS that is associated with traffic on the interface.

Time

Point in time during data transmission expressed in hours and minutes (X-Axis).

Measurement Setting:

- **Rate:** Data transfer rate at each point in time expressed in kilobits per second or a rate that is appropriate for the highest-volume ToS (Y-Axis). The rate is calculated by dividing the data volume by the elapsed transmission time.

- **Bytes** (Volume): Data volume at each point in time expressed in a scale that is appropriate for the highest-volume ToS (Y-Axis).
- **Percent** (Utilization): Percentage of the total interface capacity that the ToS traffic uses (Y-Axis). The utilization percentage is calculated by dividing the data rate by the data speed.

Depending on the data direction, the view shows inbound, outbound, or total data on the interface.

Legend

Identifies the ToS for each color band by ToS number and label (bottom of the view).

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226); Interface Pages (with an interface selected): CBQoS tab
- (NPC) Interface Pages (with an interface selected): Interface QoS and custom tabs

Note: You can add Multi-Interface Stacked ToS Trend views to a custom dashboard or to a custom tab in the Interface pages of the CA NetQoS Performance Center Console. This view consists of a group of interface-specific stacked ToS trend charts

Available Actions

You can perform several actions in this view, including the following ones:

- Change the traffic direction (In, Out, or Total), the type of measurement (Rate, Volume, or Utilization), and the view name by editing the view settings (see page 215). If the view is on a custom interface context dashboard in the CA Performance Center Console, you can change the interface.
- (CA PC) Zoom in to narrow the time frame.
- (CA PC) Display only the data for a single ToS: Right-click a ToS in the legend at the bottom of the view and click Focus. This menu is available for a view that has multiple ToS values. (This option is active when the view contains multiple ToS values.)
- (CA PC) Hide data for one of multiple ToS values: Right-click a ToS in the legend at the bottom of the view and click Hide.

- (CA PC) Position your cursor over legend items to display explanatory Tooltips.
- Jump to details on an NFA console Interface page by double-clicking a ToS value in the legend.

Find ToS Trend Data in the NFA Console

You can display ToS volume in trend charts or stacked trend charts in the NFA console for a selected interface:

- *Overview* -- Report type: Overview. Presentation menu options: Mixed Chart or Mixed Trend; Volume.

  Views: Stacked ToS Trend (In and Out) for the Top N ToS, plus other overview views.

- *Top N ToS, Stacked Trends* -- Report type: ToS. Filter: Top N ToS. Presentation menu options: Stacked Trend Chart; Volume.

  Views: Stacked Trend for the Top N ToS (In, Out, and Total).

- *Top N ToS, Trends* -- Report type: ToS. Filter: Top N ToS. Presentation menu options: Trend Chart; Volume.

  Views: Trend (In, Out, and Total) for each of the Top N ToS.

- *Single ToS, Stacked Trends/Trends* -- Report type: ToS. Filter: Single ToS value. Presentation menu options: Mixed Trend; Volume.

  Views: Trend (In and Out with baselines), Stacked ToS Trend (In and Out).

- *Single ToS, Trends* -- Report type: ToS. Filter: Single ToS value. Presentation menu options: Mixed Chart; Volume.

  Views: Stacked ToS Trend (In and Out).

- *Conversation* -- Report type: Conversations. Filter: Single conversation source and destination. Report subtype: Protocols. Presentation menu options: Volume.

  Views: Conversation Trend (maximum of 7 views for different timespans).

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Interface: ToS Summaries

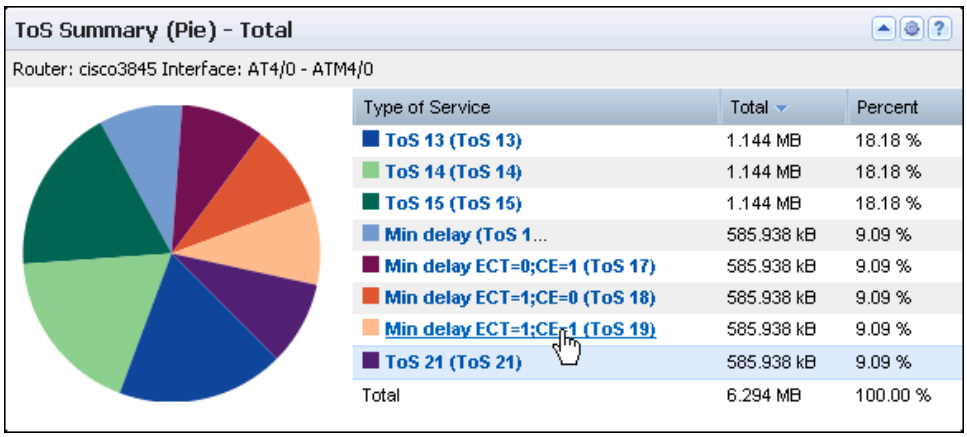
The ToS Summary views show the Type of Service (ToS) values for traffic on the selected interface. The views are described in the topics that follow.

This section contains the following topics:

ToS Summary (Pie) (see page 178)
ToS Summary (Table) (see page 180)

ToS Summary (Pie)

The ToS Summary (Pie) view shows an overview of the Type of Service (ToS) values for traffic on the selected interface. The example graphic shows the view in the CA Performance Center Console.



The view includes a pie chart and table of information about the high-volume ToS values in use on the selected interface. The table includes the following information by default:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

Type of Service

Name of the ToS values associated with high-volume traffic, identified by number and label.

Total

Shows the total data volume for the reporting period.

Percent

(CA PC) Lists the percentage of the total data volume for the Top N ToS.

Performance Center views show the data from the time range that is defined for the page.

Opening the Views

To see these views in the Performance Center Console, go to one of the following locations:

- (CA PC) Interface Pages (with an interface selected): IP Performance tab; Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the traffic direction and view name by editing the view settings (see page 215). If the view is on a custom interface context dashboard in the CA Performance Center Console, you can change the interface.
- (CA PC) Change the type of measurement.
- Jump to details on an NFA console Interface page by double-clicking a ToS name.

Find ToS Summary Pie Charts in the NFA Console

You can display pie charts of ToS summary data in the NFA console for a selected interface:

- *Overview* -- Report type: Overview. Presentation menu option: Pie Chart.

  View: ToS Summary (In and Out) for the Top N ToS.

- *Top N ToS Summary* -- Report type: ToS. Filter: Top N ToS. Presentation menu option: Pie Chart.

  View: ToS Summary (In, Out, and Total) for the Top N ToS.

- *Single ToS Summaries* -- Report type: ToS. Filter: Single ToS. Report subtype: Overview. Presentation menu option: Pie Chart.

  Views: ToS Protocol Summary (In and Out) for the single ToS; ToS Hosts Summary (From and To) for the single ToS; ToS Conversations Summary (Total) for the single ToS.

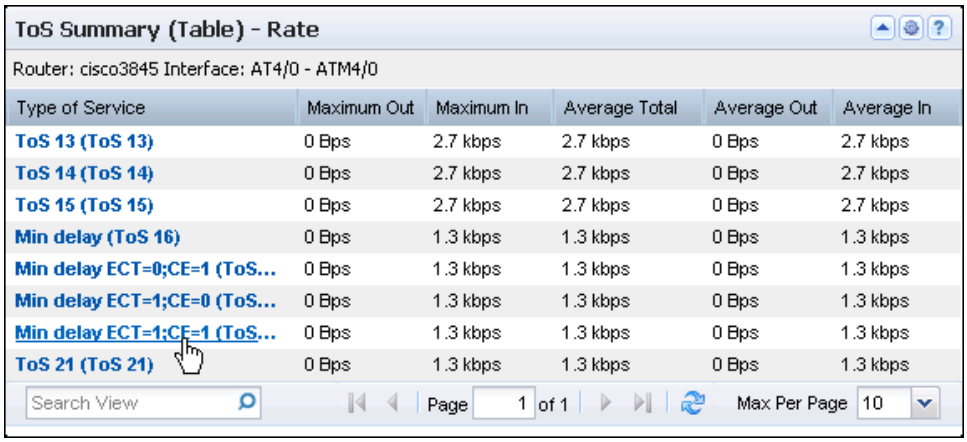
  Note: You can view additional versions of the summary pie charts by selecting Protocols, Hosts, or Conversations as the report subtype.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

ToS Summary (Table)

The ToS Summary (Table) views show rate, volume, or utilization for the top ToS values of the traffic on a particular interface. You can use this information to compare traffic for each of the top ToS values.

The example graphic shows the view in the CA Performance Center Console. The table shows the rate for each listed ToS value. You can configure the view to display rate, utilization, or volume information.



An interface identification string is shown under the view title. The table contains a row for each ToS with the Type of Service identifier (EF/AF, DSCP, and ToS values) and the following rate, volume, or utilization information:

- Rate:
  - (CA PC/NPC) Average rate of total, inbound, and outbound data for each ToS (Average Total. Average Out, and Average In)
  - (CA PC) Maximum rate of data that is outbound or inbound on the interface for each ToS (Maximum Out and Maximum In)

  The rate is calculated by dividing the data volume by the elapsed transmission time.
- Volume: Volume of outbound, inbound, and all data for each ToS (Out, In, and Total), expressed in a scale that is appropriate for the highest-volume ToS.
- Utilization:
  - (CA PC/NPC) Average utilization of total, outbound, and inbound data that each ToS consumes (Average Total. Average In, and Average Out)
  - (CA PC) Maximum percentage of interface capacity that the outbound or inbound utilizes for each ToS (Maximum Out and Maximum In)

  The utilization percentage is calculated by dividing the data rate by the data speed.

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Interface QoS or custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the type of measurement (Rate, Volume, or Utilization) and the view name by editing the view settings (see page 215).
- (CA PC) Change the interface.
- Re-sort the table data by clicking a column heading. Click again to toggle between descending and ascending order.
- Change the Max Per Page value to show more or fewer items on each table page.
- (CA PC) Change the columns that are shown in the table: Click near a column border, click Columns, then choose the columns to display.
- Click a Type of Service link to display more information about the ToS on Interface report pages in the NFA console.

Find ToS Summary Tables in the NFA Console

You can display ToS summary tables in the NFA console for a selected interface:

- *Top N ToS Summary* -- Report type: ToS. Filter: Top N ToS. Presentation menu options: Summary Table; Volume.

  View: ToS Summary Table for the Top N ToS.

- *Protocol Summary for a Single ToS* -- Report type: ToS. Filter: Single ToS. Report subtype: Protocols. Subtype filter: Top N Protocols. Presentation menu options: Summary Table; Volume.

  Views: ToS Protocol Summary Table for the single ToS.

- *Host Summary for a Single ToS* -- Report type: ToS. Filter: Single ToS. Report subtype: Hosts. Subtype filter: Top N Hosts. Presentation menu options: Summary Table; Volume.

  Views: ToS Hosts Summary Table for the single ToS.

- *Conversation Summary for a Single ToS* -- Report type: ToS. Filter: Single ToS. Report subtype: Conversations. Subtype filter: Top N Conversations. Presentation menu options: Summary Table; Volume.

  Views: ToS Conversations Summary Table for the single ToS.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Interface: Top Conversations

The Top Conversations views show the conversations that generate the highest traffic on the currently selected interface. The views are described in the topics that follow.

This section contains the following topics:

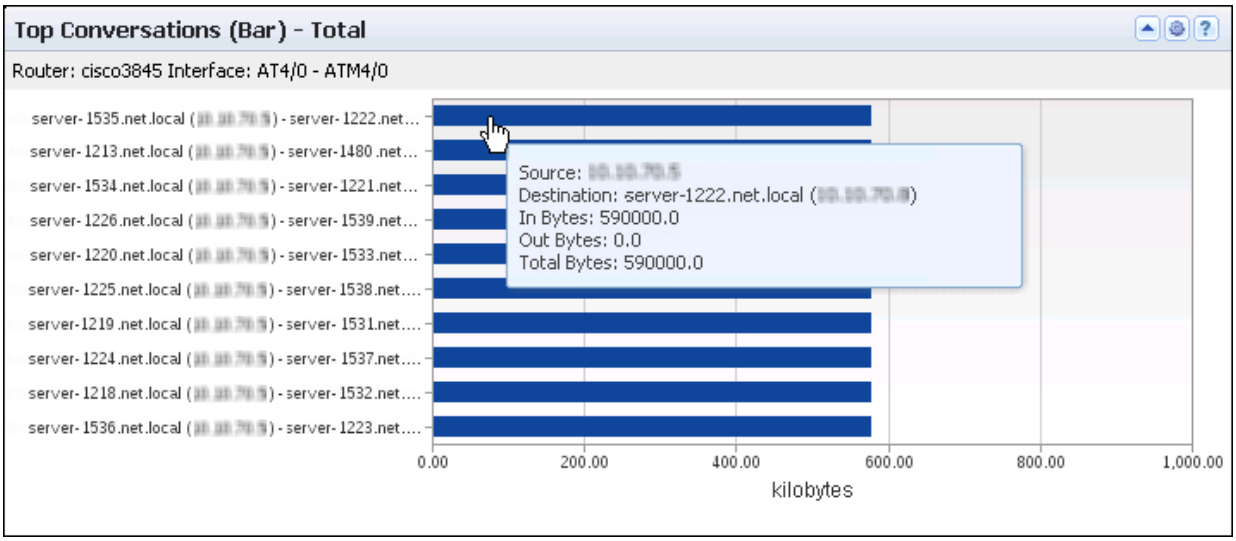
Top Conversations (Bar) (see page 183)
Top Conversations (Pie) (see page 185)
Top Conversations (Table) (see page 187)

Top Conversations (Bar)

The Top Conversations (Bar) views show the conversations that have the highest traffic on the selected interface. A bar graph shows the volume for each conversation.

For example, use conversation information to determine the IP addresses of high-volume hosts. Contact the host owners or users to investigate the nature and purpose of the traffic.

You can view the conversations for incoming data, outgoing data, or all data as shown in the example view in the CA Performance Center Console.



The view includes a bar for each top conversation on the selected interface. A maximum of 10 conversations are shown. The view includes the following information:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

Conversation Pair

Identifies the conversation source and destination servers by their names (the fully qualified DNS names, if they are available), followed by the IP addresses (Y-Axis).

Volume

Measures the total amount of data that was exchanged in the conversation expressed in a scale that is appropriate for the highest-volume conversation (X-Axis).

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Interface Capacity or custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the view name by editing the view settings (see page 215).
- (CA PC) Change the traffic direction and the interface.
- Display details in a Tooltip by holding your cursor over a bar.
- Jump to conversation details on an NFA console Interface report page by clicking a bar or name.

Find Conversation Data in the NFA Console

You can display conversation volume trend charts in the NFA console for any interface you have selected:

- *Overview Multi-Trend* -- Report type: Overview. Presentation menu options: Mixed Trend; Volume.

  View: Conversations Multi Trend Summary (Total) for the Top N Conversations, plus other views.

- *Top N Conversations Trend* -- Report type: Conversations. Filter: Top N Conversations. Presentation menu options: Trend Chart; Volume.

  View: Conversations Trend for the Top N Conversations.

- *Conversations for a Single Protocol* -- Report type: Protocols. Filter: Single protocol. Report subtype: Conversations. Conversation Filter: Top N Conversations. Presentation menu option: Trend Chart.

  View: Protocol Conversations Summary (Total) for a single protocol.

- *Conversations for a Single ToS* -- Report type: ToS. Filter: Single ToS. Report subtype Conversations. Conversation Filter: Top N Conversations. Presentation menu options: Trend Chart; Volume.

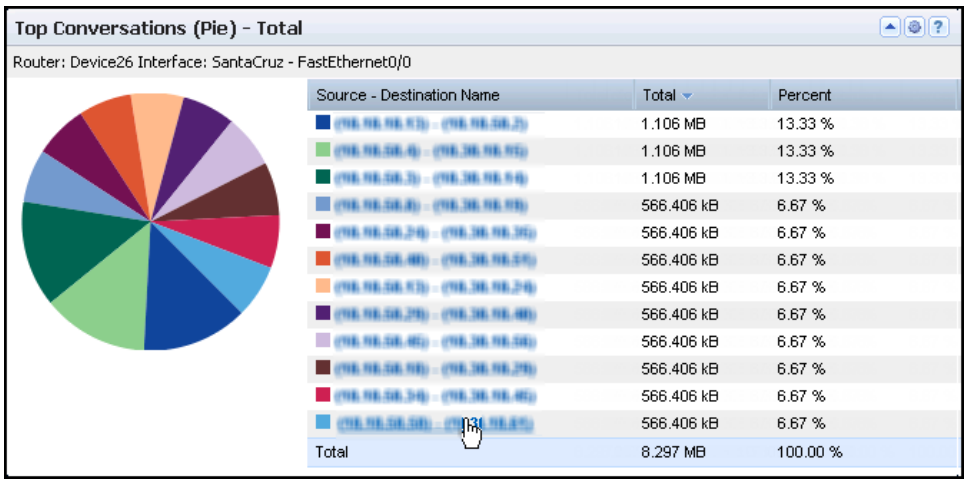
  View: ToS Trend view for each conversation that uses the single ToS.

Note: To see trend charts for a single conversation, click Top N Conversations and select a single conversation as the filter.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Top Conversations (Pie)

The Top Conversations (Pie) view includes a pie chart of the conversations that account for the most traffic on the selected interface. The example graphic shows the view in the CA Performance Center Console.



The view includes a pie chart and table of information about the high-volume conversations on the selected interface. A text string near the top of the view identifies the interface whose data is displayed. The table includes the following information by default:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

Source - Destination Name

Identifies the host servers that initiated and received the conversation data by their fully qualified DNS names (if available) and IP addresses.

Total

Shows the total amount of data in the conversation expressed in a scale that is appropriate for the highest-volume conversation.

Percent

(CA PC) Records how much the conversation consumes out of the total traffic that is displayed.

Performance Center views show the data from the time range that is defined for the page.

Opening the Views

To see these views in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226); Interface Pages (with an interface selected): IP Performance tab
- (NPC) Interface Pages (with an interface selected): Interface QoS or custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the view name by editing the view settings (see page 215).
- (CA PC) Change the traffic direction and the type of measurement. If the view is on a custom interface context dashboard in the CA Performance Center Console, you can change the interface.
- (CA PC) Change the columns that are shown in the table: Click near a column border, click Columns, then choose the columns to display.
- Jump to details on an NFA console Interface page by clicking a link.

Find Conversation Pie Charts in the NFA Console

You can display conversation pie charts in the NFA console for any interface you have selected:

- *Overview* -- Report type: Overview. Presentation menu option: Pie Chart.

  View: Conversations Summary (Total) for the Top N Conversations, plus other overview views.

- *Top N Conversations* -- Report type: Conversations. Filter: Top N Conversations. Presentation menu option: Pie Chart.

  View: Conversations Summary (Total) for the Top N Conversations.

- *Conversations for a Single Protocol* -- Report type: Protocols. Filter: Single protocol. Report subtype: Conversations or Overview. Conversations Filter: Top N Conversations. Presentation menu option: Pie Chart or Mixed Chart.

  View: Protocol Conversations Summary (Total) for a single protocol.

- *Conversations for a Single ToS* -- Report type: ToS. Filter: Single ToS. Report subtype: Conversations. Conversation Filter: Top N Conversations. Presentation menu option: Pie Chart.

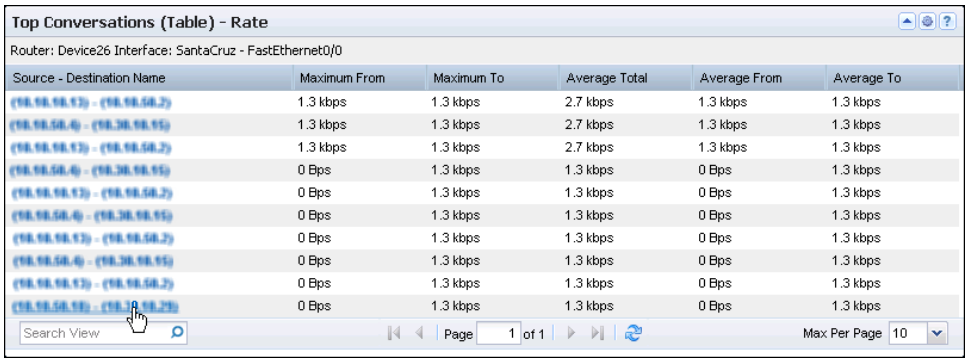
  View: ToS Conversations Summary (Total) for a single ToS.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Top Conversations (Table)

The Top Conversations (Table) views show data for the top highest-volume conversations on a particular interface. The maximum number of top conversations shown is ten.

The example graphic shows a Top Conversation (Table) view in the CA Performance Center Console, which is set to show conversation rates. You can configure the view to display rate, utilization, or volume information.



The table contains a row for each conversation with the source and destination - The fully qualified DNS host name (if available) and IP address of the servers that initiated and received the conversation data. The table also contains the following rate, volume, or utilization information:

- Rate:
  - (CA PC/NPC) For each conversation, the average rate of total data (Average Total), data that goes to the destination host (Average To), and data that comes from the source host (Average From).
  - (CA PC) For each conversation, maximum rate of data that comes from the source host (Maximum From) and goes to the destination host (Maximum To).

  The rate is calculated by dividing the data volume by the elapsed transmission time.
- Volume: For each conversation, total amount of data (Total), data that comes from the source host (From), and data that goes to the destination host (To), expressed in a scale that is appropriate for the highest-volume conversation.

- Utilization:
  - (CA PC/NPC) For each conversation, average utilization by data that comes from the source host (Average From), data that goes to the destination host (Average To), and total data (Average Total).
  - (CA PC) For each conversation, maximum percentage of interface capacity that is used by the data that comes from the source host (Maximum From) or that goes to the destination host (Maximum To).

  The utilization percentage is calculated by dividing the data rate by the data speed.

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the type of measurement (Rate, Volume, or Utilization) and the view name by editing the view settings (see page 215).
- (CA PC) Change the interface.
- (CA PC) Change the columns that are shown in the table: Click near a column border, click Columns, then choose the columns to display.
- Click one of the links to jump to a pre-filtered Interface page report in the NFA console.

Find Conversation Tables in the NFA Console

You can display tables with conversation volumes in the NFA console for a selected interface:

- *Top N Conversations* -- Report type: Conversations. Filter: Top N Conversations. Presentation menu option: Summary Table; Volume.

  View: Conversation Summary Table for the Top N Conversations.
- *Conversations for a Single Protocol* -- Report type: Protocols. Filter: Single protocol. Report subtype: Conversations. Subtype filter: Top N Conversations. Presentation menu option: Summary Table; Volume.

  View: Protocol Conversation Summary Table for a single protocol.

- *Conversations for a Single ToS* -- Report type: ToS. Filter: Single ToS. Report subtype: Conversations. Subtype filter: Top N Conversations. Presentation menu options: Summary Table; Volume.

  View: ToS Conversations Summary Table for a single ToS.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Interface: Top Hosts

The Top Hosts views show the hosts that generate the highest traffic on the currently selected interface. The views are described in the topics that follow.

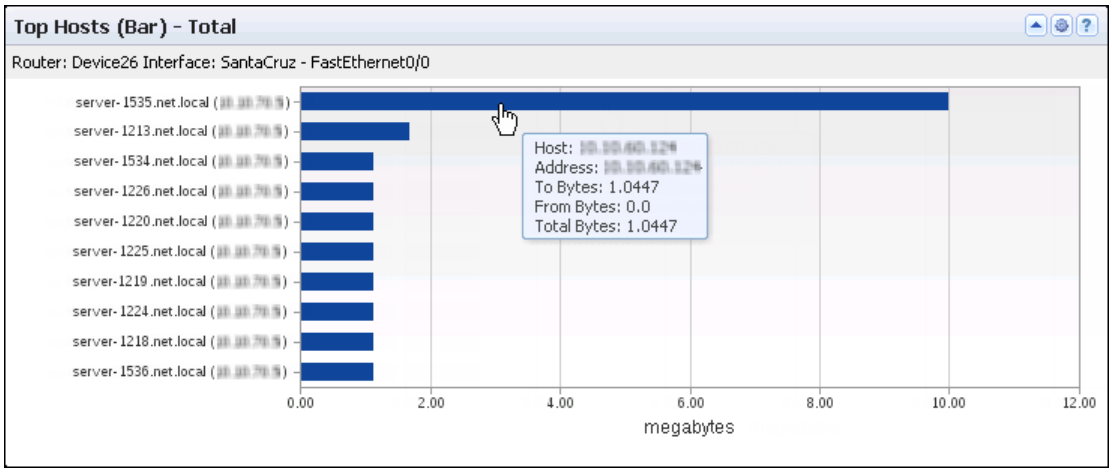
This section contains the following topics:

Top Hosts (Bar) (see page 189)
Top Hosts - Pie (see page 191)
Top Hosts (Table) (see page 193)

Top Hosts (Bar)

The Top Hosts (Bar) views show the top high-volume hosts for a particular interface. You can use this view to determine the IP addresses of hosts that are responsible for high volumes of network traffic. You can then contact the owner or user of each host to investigate the nature and purpose of the traffic.

You can view the hosts for incoming flows, outgoing flows, or all flows, as shown in the example of a view in the CA Performance Center Console.



The bar chart includes the following information for a maximum of 10 hosts:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

Host Name

Identifies the host server by its fully qualified DNS name (if available) and IP address (Y-Axis).

Volume

Measures the total amount of data for the host on the interface, expressed in a scale that is appropriate for the highest-volume host (X-Axis).

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Interface Capacity or custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the traffic direction and the view name by editing the view settings (see page 215).
- (CA PC) Change the interface.
- Display details in a Tooltip by holding your cursor over a bar.
- Jump to details for a specific host on an NFA console Interface page by clicking a bar.

Find Host Trend Views in the NFA Console

The Enterprise Overview page in the NFA console displays traffic volume for the top hosts in a bar chart.

You also can display host volume in trend charts for a selected interface:

- *Overview* -- Report type: Overview. Presentation menu options: Mixed Trend; Volume.

  View: Hosts Multi Trend Summary (From and To) for the Top N Hosts, plus other overview views.

- *Top N Host Trend* -- Report type: Hosts. Filter: Top N Hosts. Presentation menu options: Trend Chart; Volume.

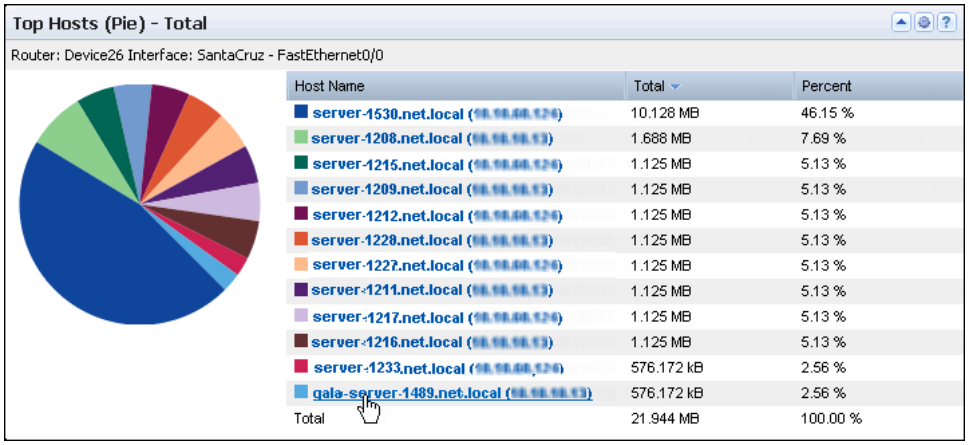
  View: Host Trend for each of the Top N Hosts.

Note: To see trend charts for a single host, click Top N Hosts and select a host as the filter.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Top Hosts - Pie

The Top Hosts (Pie) views show the hosts that account for the highest volumes of network traffic on the selected interface. The example graphic shows the view in the CA Performance Center Console.



The table includes the following information by default:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

Host Name

Identifies the host server by its fully qualified DNS name (if available) and IP address.

Total

Records the total amount of data for the host on the interface, expressed in a scale that is appropriate for the highest-volume host.

Percent

(CA PC) Records how much the host consumes out of the total traffic that is displayed.

Performance Center views show the data from the time range that is defined for the page.

Opening the Views

To see these views in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226); Interface Pages (with an interface selected): IP Performance tab
- (NPC) Interface Pages (with an interface selected): Interface QoS or custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the traffic direction and the view name by editing the view settings (see page 215). If the view is on a custom interface context dashboard in the CA Performance Center Console, you can change the interface.
- (CA PC) Change the columns that are shown in the table: Click near a column border, click Columns, then choose the columns to display.
- Jump to details on an Interface report page in the NFA console by clicking a host link in the view.

Find Host Pie Charts in the NFA Console

You can display pie charts with host volumes in the NFA console for a selected interface:

- *Overview* -- Report type: Overview. Presentation menu option: Pie Chart.

  View: Host Summary (From and To) for the Top N Hosts, plus other overview views.
- *Top N Hosts Summary* -- Report type: Hosts. Filter: Top N Hosts. Presentation menu option: Pie Chart.

  View: Host Summary (From, To, and Total) for the Top N Hosts.

- *Hosts for a Single Protocol* -- Report type: Protocols. Filter: Single protocol. Report subtype: Overview. Presentation menu option: Pie Chart.

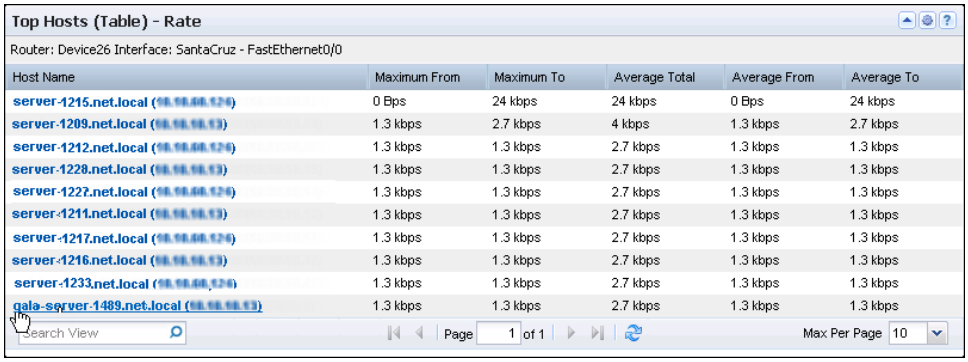
  View: Protocol Hosts Summary (From, To, and Total) for the single protocol.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Top Hosts (Table)

The Top Hosts (Table) views show rate, volume, or utilization for the hosts who exchange the highest volume of data on a particular interface.

The example shows a Top Hosts (Table) view in the CA Performance Center Console. The view is configured to show the rate for each listed host. You can configure the view to display rate, utilization, or volume information.



The view contains an interface identification string and a table. The table contains a row for each host with the fully qualified DNS host name (if available) and IP address, as well as the following rate, volume, or utilization information (by default):

- Rate:
  - (CA PC/NPC) For each host, the average rate of total data (Average Total), data that goes to the host (Average To), and data that comes from the host (Average From).
  - (CA PC) For each host, maximum rate of data that comes from the host (Maximum From) and goes to the host (Maximum To).

  The rate is calculated by dividing the data volume by the elapsed transmission time.
- Volume: For each host, total amount of data (Total), data from the host (From), and data to the host (To), expressed in a scale that is appropriate for the highest-volume host.

- Utilization:
  - (CA PC/NPC) For each host, average utilization by data that comes from the host (Average From), data that goes to the host (Average To), and total data (Average Total).
  - (CA PC) For each host, maximum percentage of interface capacity that is used by the data from the host (Maximum From) or that goes to the host (Maximum To).

  The utilization percentage is calculated by dividing the data rate by the data speed.

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the type of measurement and the view name by editing the view settings (see page 215).
- (CA PC) Change the interface.
- (CA PC) Change the columns that are shown in the table: Click near a column border, click Columns, then choose the columns to display.
- Click a name to jump to a pre-filtered Interface page report in the NFA console.

Find Host Tables in the NFA Console

You can display tables with host volumes in the NFA console for a selected interface:

- *Top N Hosts Summary* -- Report type: Hosts. Filter: Top N Hosts. Presentation menu option: Summary Table; Volume.

  View: Host Summary Table for the Top N Hosts.
- *Hosts for a Single Protocol* -- Report type: Protocols. Filter: Single protocol. Report subtype: Overview. Presentation menu option: Summary Table; Volume.

  View: Protocol Host Summary Table for the single protocol.

- *Hosts for a Single ToS* -- Report type: ToS. Filter: Single ToS. Report subtype: Hosts. Subtype filter: Top N Hosts. Presentation menu options: Summary Table; Volume.

  View: ToS Hosts Summary Table for the single ToS.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Interface: Top Protocols

The Top Protocols views show the protocols associated with the highest traffic on the currently selected interface. The views are described in the topics that follow.

This section contains the following topics:

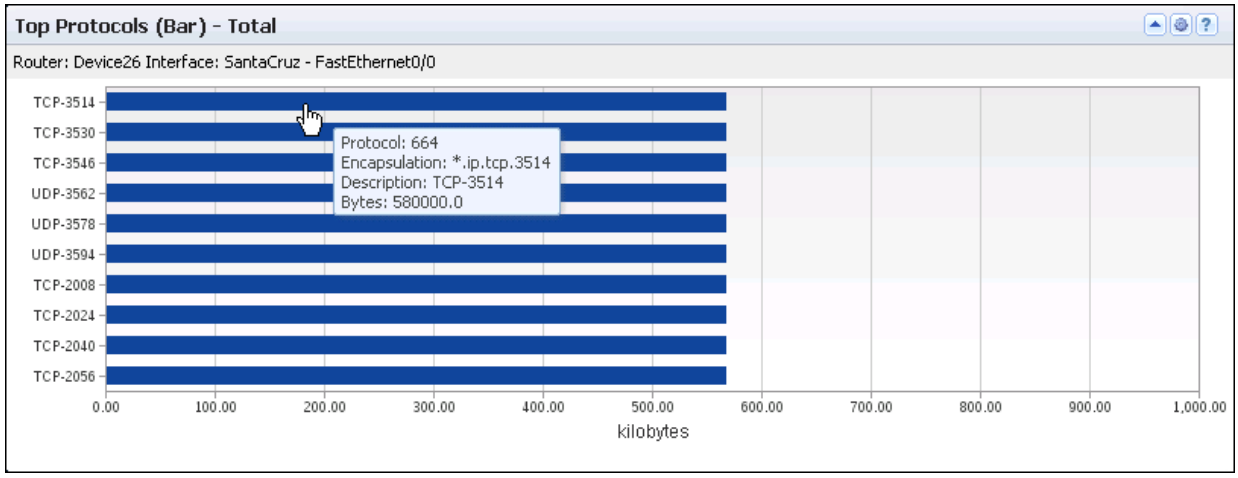
Top Protocols (Bar) (see page 196)
Top Protocols (Pie) (see page 198)
Top Protocols (Table) (see page 200)

Top Protocols (Bar)

The Top Protocols (Bar) views show the top high-volume IP protocols for traffic on a particular interface. A bar chart shows which protocols account for the most traffic on the selected interface.

This view gives you an overall picture of how much data is associated with particular protocols--and, therefore, with applications--on the interface. The view also lets you determine whether the application protocols are related to business-critical processes, or are related to low-priority or non-business related processes such as unauthorized web use.

You can view protocol traffic for incoming flows, outgoing flows, or all flows--as shown in the example graphic of a view in the CA Performance Center Console.



The bar chart includes the following information for a maximum of 10 protocols:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

Protocol

Identifies the protocol by its descriptor (Y-Axis).

Volume

Measures the total amount of protocol data expressed in a scale that is appropriate for the highest-volume protocol (X-Axis).

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the traffic direction and the view name by editing the view settings (see page 215).
- (CA PC) Change the interface.
- Display details in a Tooltip by holding your cursor over a bar.
- Jump to details for a specific protocol on an NFA console Interface page by clicking a bar or name.

Find the Comparable View in the NFA Console

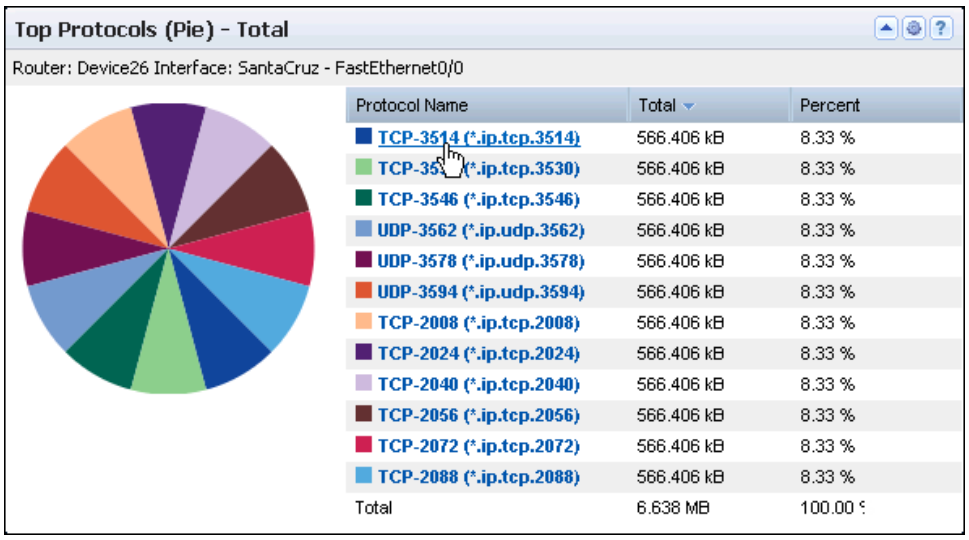
The Top Protocols bar charts in the Performance Center Console are similar to the Top Protocol view on the Enterprise Overview page in the NFA console.

Also See:

Stacked Protocol Trend (see page 172)

Top Protocols (Pie)

The Top Protocols (Pie) views show the protocols that are associated with the highest traffic volumes on the selected interface. The example graphic shows the view in the CA Performance Center Console.



The table includes the following information by default:

Identifier

Identifies the interface that is used for the report. The identifier string consists of the router name, interface name, and interface description (under the view title).

(NPC) The identifier line also includes the interface speed.

Protocol Name

Identifies the protocol by its keyword and TCP/UDP port assignment.

Total

Records the total volume of network traffic on the interface that is associated with the protocol

Percent

(CA PC) Records how much the protocol consumes out of the total traffic that is displayed.

Performance Center views show the data from the time range that is defined for the page.

Opening the Views

To see these views in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Interface QoS or custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the traffic direction and the view name by editing the view settings (see page 215).
- (CA PC) Change the interface.
- (CA PC) Change the columns that are shown in the table: Click near a column border, click Columns, then choose the columns to display.
- Jump to details on an NFA console Interface page by clicking a protocol name.

Find Protocol Pie Charts in the NFA Console

You can display pie charts with protocol traffic volumes in the NFA console for a selected interface:

- *Overview* -- Report type: Overview. Presentation menu option: Pie Chart.

  View: Protocol Summary (In and Out) for the Top N Protocols, plus other overview views.

- *Top N Protocol Summaries* -- Report type: Protocols. Filter: Top N Protocols. Presentation menu option: Pie Chart.

  View: Protocol Summary (In, Out, and Total) for the Top N Protocols.

- *Hosts or Conversations for Single Protocol* -- Report type: Protocols. Filter: Single protocol. Presentation menu option: Pie Chart.

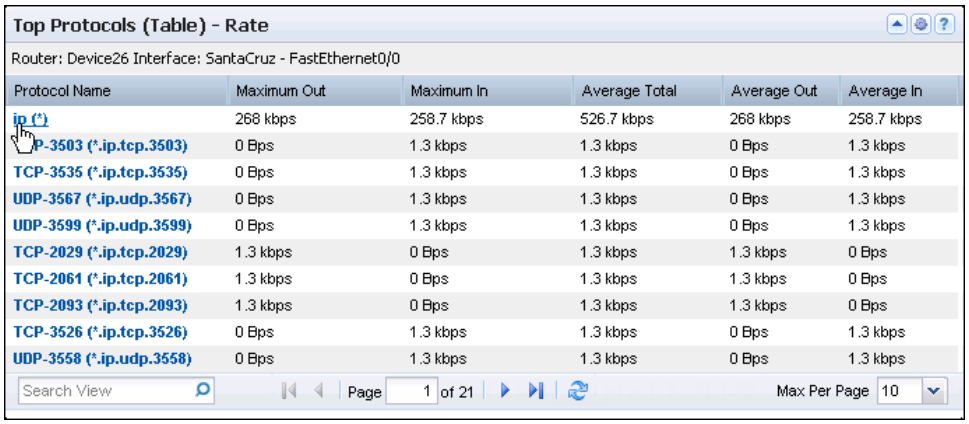
  Views: Protocol Hosts Summary (From and To) for the single protocol; Protocol Conversations Summary (Total) for the single protocol.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

Top Protocols (Table)

The Top Protocols (Table) views are tables that show the rate, volume, or utilization for the highest-volume protocol traffic on a particular interface. You can use this information to compare the data volume or utilization for particular protocols, for example.

The example graphic shows a Top Protocols (Table) view in the CA Performance Center Console. The view is set to show the traffic volume for each listed protocol. You can configure the view to display rate, utilization, or volume information.



The view contains an interface identification string and table. The table has a row for each protocol with the protocol name (keyword and TCP/UDP port assignment) and the following rate, volume, or utilization information (by default):

- Rate:
  - (CA PC/NPC) Average rate of total (Average Total), inbound (Average In), and outbound data (Average Out) for each protocol.
  - (CA PC) Maximum rate of data that is outbound, inbound, or both outbound and inbound (Maximum Out, Maximum In, and Maximum Total) on the interface for each protocol

  The rate is calculated by dividing the data volume by the elapsed transmission time.
- Volume: Number of bytes/megabytes of outbound data (Out), inbound data (To), and all data (Total) for each protocol.

- Utilization:
  - (CA PC/NPC) Average utilization by inbound data (Average In), outbound data (Average Out), and total data (Average Total) for each protocol.
  - (CA PC) Maximum percentage of interface capacity that the outbound (Maximum Out) or inbound protocol data utilizes (Maximum In)

  The utilization percentage is calculated by dividing the data rate by the data speed.

Performance Center views show the data from the time range that is defined for the page.

Opening the View

To see this view in the Performance Center Console, go to one of the following locations:

- (CA PC) Custom dashboard (see page 226)
- (NPC) Interface Pages (with an interface selected): Custom tab

Available Actions

You can perform several actions in this view, including the following ones:

- Change the type of measurement (Rate, Volume, or Utilization) and the view name by editing the view settings (see page 215).
- (CA PC) Change the interface.
- Re-sort the table data by clicking a column heading. Click again to toggle between descending and ascending order.
- Change the Max Per Page value to show more or fewer items on each table page.
- (CA PC) Change the columns that are shown in the table: Click near a column border, click Columns, then choose the columns to display.
- Click a name to jump to a pre-filtered Interfaces report in CA Network Flow Analysis.

Find Protocol Tables in the NFA Console

You can use these ways to display tables of protocol volume data in the NFA console for a selected interface:

- *Top N Protocols* -- Report type: Protocols. Filter: Top N Protocols. Presentation menu options: Summary Table; Volume.

  View: Protocol Summary Table for the Top N Protocols, plus other overview views.

- *Protocols for a Single Host* -- Report type: Hosts. Filter: Single host. Report subtype: Protocols. Presentation menu options: Summary Table; Volume.

  View: Host Protocol Summary Table for the single host.

- *Protocols for a Single Conversation* -- Report type: Conversations. Filter: Single conversation. Report subtype: Protocols. Presentation menu options: Summary Table; Volume.

  View: Conversation Protocol Summary Table for the single conversation.

To display Flow Forensics-level detail, click the Flow Forensics link and run a Flow Forensics report.

CA Anomaly Detector Views in Performance Center

CA Anomaly Detector is a CA Infrastructure Management product that gives you visibility into the highly variable traffic patterns of servers and clients. The program continually monitors behaviors and rapidly analyzes multiple network data patterns to search for signs of misconfiguration, malicious attacks, or poor application delivery. CA Anomaly Detector can send alerts for as many as 27 types of potential anomalies from a number of data sources, depending on which data sources are the product is configured to monitor:

- Flow distillation by CA Network Flow Analysis
- SNMP collection by CA NetVoyant
- TCP application performance from CA Application Delivery Analysis
- Voice and video performance from CA Unified Communications Monitor

To see the predefined CA Anomaly Detector reports, go to one of the following locations:

- (CA PC) Open the CA Performance Center Console and select Dashboards, Operations Displays: Anomaly Detector.
- (NPC) Open the CA NetQoS Performance Center Console and select Reports, Operations: Anomaly Detector.

Note: To view the reports, your user account must be assigned a role that gives you access to the report menu. User account settings are managed in the Performance Center Console, as described in the *Administrator Guide* for your Performance Center version.

You can customize the Anomaly Detector page to meet your specific needs. For more information about customizing the page, see Change the View Settings (see page 215).

Built-in CA Anomaly Detector Views on the Anomaly Detector Page:

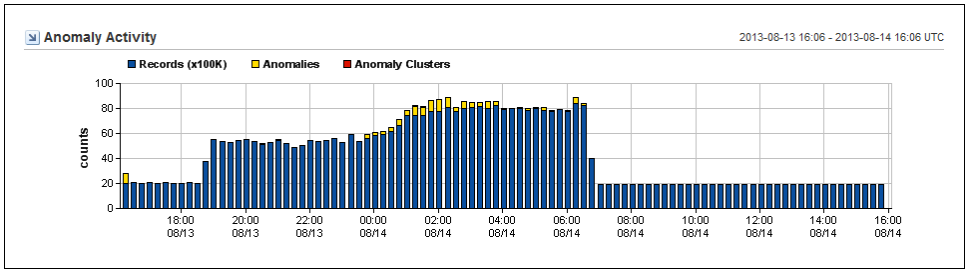
- Anomaly Activity (see page 203)
- Anomaly Detector Overall Status (see page 204)
- Enterprise-Wide Correlated Anomalies (see page 206)
- Top Anomalies by Host (see page 205)
- Top Anomalies by Interface (see page 206)
- Top Enterprise-Wide Network Anomalies (see page 204)

Additional View that You Can Add to a Custom Page:

- Enterprise-Wide Anomalies (see page 208)

Anomaly Activity

The Anomaly Activity view displays anomalous activity as a bar chart. This view gives you a visual overview of how many anomalies and anomaly clusters occurred in comparison to all of the records that were processed.



The example graphic shows the number of records in the hundreds of thousands (Y-Axis) over a 24-hour period. Activity is shown along the X-Axis each time the program runs (usually at 15-minute intervals).

You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 218).

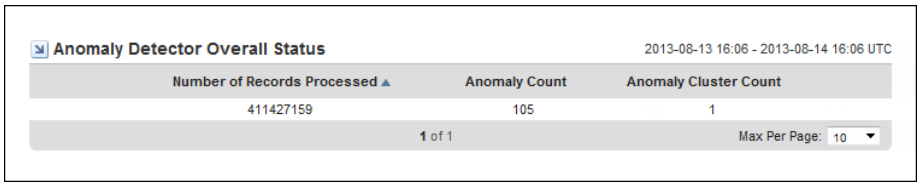
  By changing the time frame for the page, you can discover when the issue began and look for patterns.

- View title and context (see page 215).

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Anomaly Detector Overall Status

The Anomaly Detector Overall Status table shows the number of records that were processed during the selected time frame, the number of anomalies, and the number of anomaly clusters.



You can edit the following view settings:

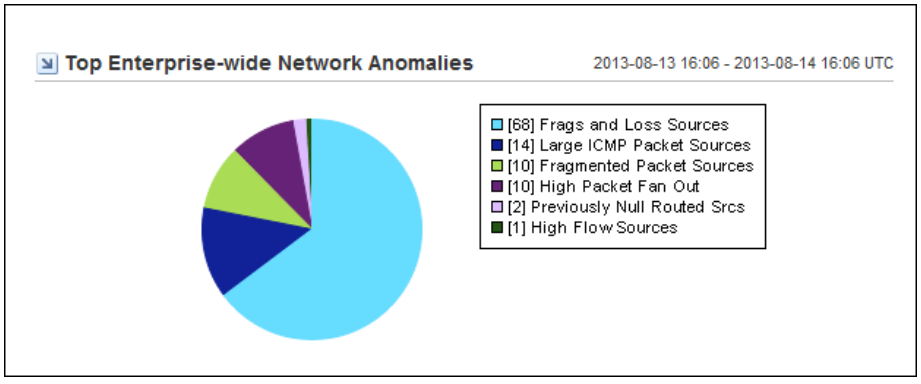
- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 218)
- View title and context (see page 215)

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Top Enterprise-Wide Network Anomalies

The Top Enterprise-Wide Network Anomalies pie chart shows the top anomaly types for the reporting time frame.

This view shows the type of network traffic that had the highest proportion of anomalous traffic. This data may give you the first insight into poor network performance.



The legend identifies the number of instances and the colors for each anomaly type. Anomaly types are named for the corresponding sensors. For a description of each sensor, see Sensors Overview.

The Top Enterprise-Wide Network Anomalies view is most useful for tracking sudden changes in network behavior. For example, suppose that the Enterprise-Wide Network Anomalies view shows that the Large DNS Packet Sources category accounts for 25% of all potentially anomalous behavior for the past week. If the summary indicates that Large ICMP Packets account for 50% of such traffic today, you would follow up with an investigation.

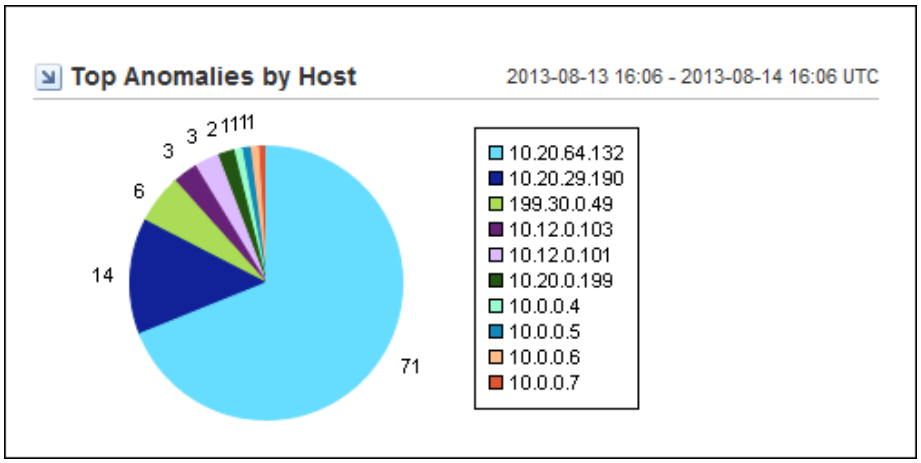
You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 218)
- View title and context (see page 215)

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Top Anomalies by Host

The Top Anomalies by Host pie chart shows the top anomalous hosts, ranked by the number of anomalies for the reporting time frame. A maximum of 10 hosts are included. The number of instances is shown next to each pie slice.



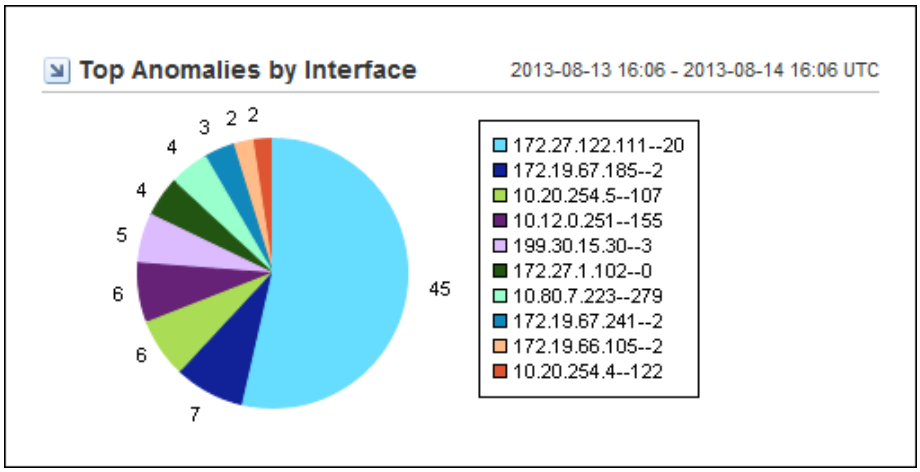
You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 218)
- View title and context (see page 215)

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Top Anomalies by Interface

The Top Anomalies by Interface pie chart shows the anomalies for the top interfaces, ranked by number of anomalies. A maximum of 10 anomalies are included. The number of instances is shown next to each pie slice.



You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 218)
- View title and context (see page 215)

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

Enterprise-Wide Correlated Anomalies

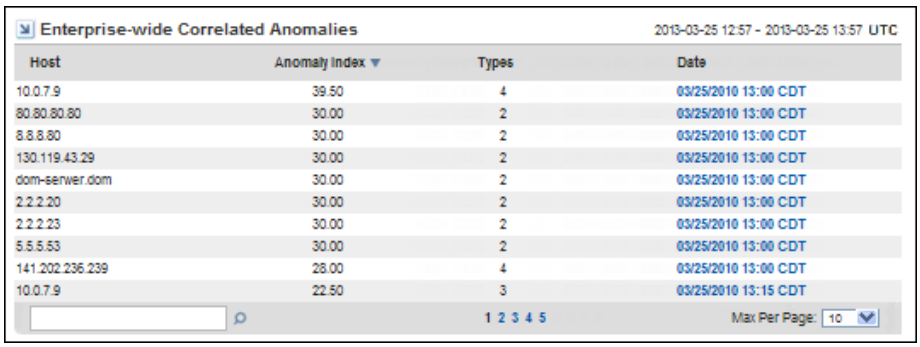
The Enterprise-Wide Correlated Anomalies table summarizes the anomalous behaviors that are most likely to be damaging to the network. This view identifies network locations that you can begin investigating if you suspect malicious activity.

Anomaly clusters are better indicators for problems than single anomalies. Many types of attacks involve multiple instances of anomalous network behavior. Instances are often clustered around a group of a few hosts at first, then the behavior spreads in a fan-out behavior. In a fan-out behavior, seemingly unrelated devices are affected and unexpected traffic is produced from multiple sources.

Correlation is performed by using an algorithm that considers the typical patterns for each type of monitored network traffic.

An anomaly is *correlated* when the following requirements are met:

- Three or more anomaly instances exist.
- Two different anomaly types are present or have an Anomaly Index above 2.0.
- One device is the source of the anomalies.


Enterprise-wide Correlated Anomalies 2013-03-25 12:57 - 2013-03-25 13:57 UTC

Host	Anomaly Index	Types	Date
10.0.7.9	39.50	4	03/25/2010 13:00 CDT
80.80.80.80	30.00	2	03/25/2010 13:00 CDT
8.8.8.80	30.00	2	03/25/2010 13:00 CDT
130.119.43.29	30.00	2	03/25/2010 13:00 CDT
dom-serwer.dom	30.00	2	03/25/2010 13:00 CDT
2.2.2.20	30.00	2	03/25/2010 13:00 CDT
2.2.2.23	30.00	2	03/25/2010 13:00 CDT
5.5.5.53	30.00	2	03/25/2010 13:00 CDT
141.202.236.239	28.00	4	03/25/2010 13:00 CDT
10.0.7.9	22.50	3	03/25/2010 13:15 CDT

1 2 3 4 5 Max Per Page: 10

You can change the time frame for this view and all views on the page, as described in Set a Custom Time Frame (see page 218).

You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 218)
- View title and context (see page 215)

This view is included by default on the Anomaly Detector page in the Performance Center Console. The example graphic shows the view as it appears in the CA NetQoS Performance Center Console.

The view provides the following information about anomalous network behavior:

Host

The IP address of the host that displays the anomalous behavior. The host may be a client computer, a server, a router, or an interface. The program attempts to resolve the hostname of the IP address and displays that name in the Host field.

Anomaly Index

The count of the anomalies in the cluster, weighted by their role as either primary or secondary. The anomaly correlation algorithm compares each particular behavior to the typical patterns for the network traffic type. The higher the index number, the more severe the issue is.

Types

The number of different types of anomalous network behavior that occurred during the reporting period.

Date

The date and time of the first correlated anomaly on the host.

The time may vary by up to 15 minutes from the time when the flows actually took place. Data is pulled from the Harvesters for analysis at 15-minute intervals.

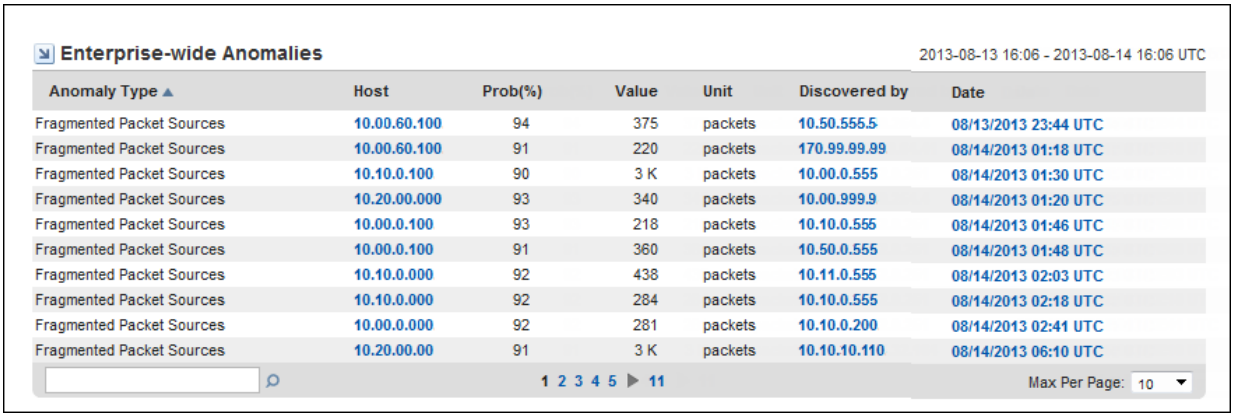
Date Link

Click the *Date* link In the Enterprise-Wide Correlated Anomalies view to go to the Anomaly Detector Drill-In table (see page 209).

Enterprise-Wide Anomalies

The Enterprise-Wide Anomalies view is a comprehensive summary of the anomalous behavior during the reporting time frame, with details about the anomaly type, location, and size.

This view is useful for beginning an investigation of problem behavior or for initiating troubleshooting procedures to stem an attack. The view provides more detailed information about the anomalies you see in other views. This view also identifies network locations to begin investigating.



You can edit the following view settings:

- Time frame for all views on the page, as described in Set a Custom Time Frame (see page 218)
- View title and context (see page 215)

This view is not included by default on the Anomaly Detector page in the Performance Center Console. To see this view, add it to a page or to a new custom page. The graphic shows an example view in the CA NetQoS Performance Center Console.

The view provides the following information about anomalous network behavior:

Anomaly Type

The type of anomalous behavior. For a description of each anomaly type that you can enable for monitoring, see Sensors Overview.

Host

The name or IP address of the host on which the anomalous behavior is detected. The host may be a client system, a server, a router, or an interface. The program attempts to resolve the hostname of any IP address and displays that name in this field.

Probability

The calculated likelihood that flagged packet flows are truly anomalous.

Probability is expressed as a percentage. For example, if the probability for an anomaly type is 91%, the packet flows that triggered the reported anomalous behavior are calculated to have a 91% probability of being truly anomalous. In this case, the packet flows have a low probability of occurring normally on this network.

For more information about the probability algorithm, see Probability Thresholds.

Date

The date and time that the anomalous behavior is detected. The time may vary by up to 15 minutes from the time when the flows actually took place. Data is pulled from the Harvesters for analysis at 15-minute polling intervals.

Links and Detail Pages

Links are included in some views to help kick-start anomaly troubleshooting. Links take you to preconfigured reports or to a general page of additional detail. The following views include links:

- Enterprise-Wide Correlated Anomalies
- Enterprise-wide Anomalies
- Anomaly Detector Drill-In

Date Link

Click the *Date* link to go to the Anomaly Trend view (see page 212). This view shows the value and probability of the anomaly over time.

Discovered by Link

Click a *Discovered By* link to view details. The link destination is determined by the type of anomaly:

- CA Network Flow Analysis Anomalies: Router or interface page in the Performance Center Console
- Anomalies from other data sources: Main page for the originating product

Host Link

Click a *Host* link to go to more granular information about the device that has the anomaly. Clicking a Host link may be the first step in troubleshooting the anomaly.

Host link destinations are based on the sensor type. For many CA Network Flow Analysis sensors, the Host link opens the page for defining a Flow Forensics report in the NFA console, which has pre-populated report filters.

Anomaly Drill-In

If you drill into an anomaly cluster from the Enterprise-wide Correlated Anomalies view (see page 208), the Anomaly Drill-In table opens. For each anomaly, the table lists the probability, value, originating router and interface, and the time that the anomaly occurred. You can use the Date link to drill into a trend chart that shows the value and probability over time.

The Anomaly Drill-In view provides the following information about each anomaly:

Anomaly Type

The type of anomalous behavior. For a description of each anomaly type that you can enable for monitoring, see Sensors Overview.

Host

The name or IP address of the host on which the anomalous behavior is detected. The host may be a client system, a server, a router, or an interface. The program attempts to resolve the hostname of any IP address and displays that name in this field.

Host Link

Click a *Host* link to go to more granular information about the device that has the anomaly. Clicking a Host link may be the first step in troubleshooting the anomaly.

Host link destinations are based on the sensor type. For many CA Network Flow Analysis sensors, the Host link opens the page for defining a Flow Forensics report in the NFA console, which has pre-populated report filters.

Prob(%)

The calculated likelihood that flagged packet flows are truly anomalous.

Probability is expressed as a percentage. For example, if the probability for an anomaly type is 91%, the packet flows that triggered the reported anomalous behavior are calculated to have a 91% probability of being truly anomalous. In this case, the packet flows have a low probability of occurring normally on this network.

For more information about the probability algorithm, see Probability Thresholds.

Value

The value that triggered the report of anomalous behavior, expressed in the units of measure shown in the Unit column. For example, the value could be the number of gigabytes of data in the anomalous flow.

Metric/Unit

The unit of measurement that is used to express the Value, such as packets, flows, or destination hosts (dest hosts).

Discovered by

The router, interface, or data source that detected the anomalous data.

Discovered by Link

Click a *Discovered By* link to view details. The link destination is determined by the type of anomaly:

- CA Network Flow Analysis Anomalies: Router or interface page in the Performance Center Console
- Anomalies from other data sources: Main page for the originating product

Date

The date and time that the anomalous behavior is detected. The time may vary by up to 15 minutes from the time when the flows actually took place. Data is pulled from the Harvesters for analysis at 15-minute polling intervals.

Date Link

Click the *Date* link to go to the Anomaly Trend view (see page 212). This view shows the value and probability of the anomaly over time.

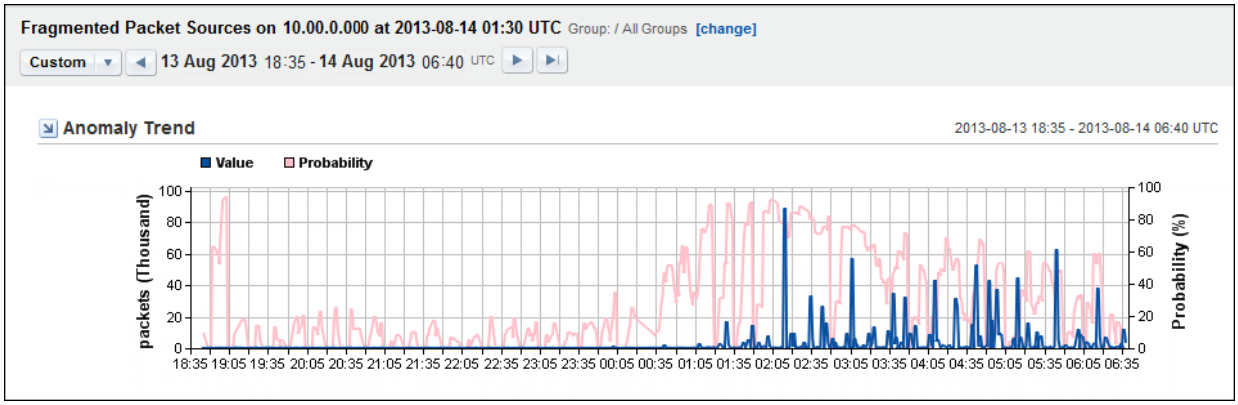
You can edit the following view settings:

- Time frame, as described in Set a Custom Time Frame (see page 218).
- View title (see page 215).

Note: If your deployment includes CA Performance Center, you can use the Zoom feature to interactively limit the time frame (see page 219).

Anomaly Trend

The Anomaly Trend view shows the value and probability of the anomaly over time. To display this trend chart, click a link in the Date column in either the Anomaly Drill-in view (see page 210) or the Enterprise-Wide Anomalies view (see page 208). The following example shows an Anomaly Trend view in the CA NetQoS Performance Center Console.



The view shows the pattern of deviation from normal network behavior. You can see when the behavior began and how severe the behavior was. A longer term view can help to determine patterns over days, weeks, or months.

The recorded values are shown as a blue trend line on the X-Axis. The probability that the behavior is a true anomaly is shown as a pink trend line on the Y-Axis.

You can edit the following view settings:

- Time frame, as described in Set a Custom Time Frame (see page 218)
- View title (see page 215)

Note: If your deployment includes CA Performance Center, you can use the Zoom feature to interactively limit the time frame (see page 219).

Customizing Dashboards and Views

The icons at the top of each dashboard or view page give you access to time frame settings and other options for all of the views. The icons in the title bar of each view let you modify view settings, export views, and access Help.

You can select predefined or custom time frames for dashboards. The time frame setting affects all of the views on the page.

View Options in CA Performance Center

This topic describes view options in the CA Performance Center Console.

Many views offer a search feature and other settings that you can change to modify the view. In addition to filtering and time frame options, the following options are available for most data views:

- Editing view settings  , such as changing its title or severity categories.
- Seeing more data by selecting another "page" of a table view.
- Increasing or decreasing the number of items that are shown per "page".
- Collapsing the view so that the data is hidden.
- Changing the managed item context for the data shown in the view.

  Note: Users with the 'Save Changes to Shared Views' role right can save view modifications to their own user account. The changes persist after logout. However, other users cannot see changes to views.

Other view options are specific to the selected view. The available options depend on the format and data source.

Trend View Options

The trend views that are available in context pages let you quickly and easily change the trend lines that are displayed on the graph. The following options also apply to multitrend views:

- Right-click a metric in the chart legend and select Hide to remove it from the view.
- Exclude all other metrics by right-clicking a metric in the legend and selecting Focus.
- Narrow the focus to a precise time frame using the zoom feature.

Trend views also include an option to add a "goal line" as a visual indication of performance levels or thresholds. You can supply any value or label for the goal line, and you can show or hide the goal line for a selected trend view.

Table View Options

In table views, you can drill down to detailed data for individual items. Use the page feature to see metrics from a longer list of items. Increase the Max Per Page value to increase the size of the view and the number of table rows per page.

You can sort table data columns by selected metrics and also select columns to include. Click a table column to sort. A white arrow on the column lets you access a menu of table column options. Select Columns to enable and disable the metrics that were enabled for the table by default.

Browser View Options

The *browser view* is a unique view type that lets you add a URL to a selected report page. You can use this view to compare external factors alongside your network performance views. Also, the browser view lets you update internal and external data dynamically. The URL must be for a web page that supports embedded iframes.

Multiple external factors can affect the performance of your network and servers, such as world events and adverse weather conditions. The ability to view a weather map and news headlines alongside performance data views on a single report page can help you better understand patterns in network performance.

Device Admin Option

When a view does not display CA Infrastructure Manager Data Aggregator data, this option lets you drill down directly to the CA Infrastructure Manager Data Aggregator Admin page to troubleshoot monitored devices and items.

View Options in CA NetQoS Performance Center

This topic describes some of the view options in the CA NetQoS Performance Center Console.

Many views offer a search feature and other settings that you can change to modify the view. In addition to filtering and time frame options (see page 218), the following options are available for most views:

- Editing view settings  , such as changing the view title or data direction.
- Increasing or decreasing the number of items on a table "page" by using the Max Per Page option.
- Changing the context, so that the view data is restricted to a particular group

  Note: Users with the 'Persist Shared View Edits' role right can save view modifications to their own user account, but other users cannot see the changes. The changes persist after logout.

Many view options are specific to the selected view. The available options depend on the view format and data source.

Table View Options

In table views, you can drill down to detailed data for individual items. Use the page feature to see metrics from a longer list of items. Increase the Max Per Page value to increase the size of the view and the number of table rows per page.

You can click a table column to sort the table data by the values in the column.

Browser View Options

The *browser view* is a unique view type that lets you add a URL to a selected report page. You can use this view to compare external factors alongside your network performance views. Also, the browser view lets you update internal and external data dynamically. The URL must be for a web page that supports embedded iframes.

Multiple external factors can affect the performance of your network and servers, such as world events and adverse weather conditions. The ability to view a weather map and news headlines alongside performance data views on a single report page can help you better understand patterns in network performance.

View In Option

Some Interface page views allow you go directly to the data source to see detailed data. Click the arrow () and select the 'View in' option. The option opens the view in the NFA console, for example.

Change the View Settings

You can change several settings for an enterprise-wide view or an interface-specific view. The available settings depend on the view.

For example, some views have settings for data direction--so you can display inbound data, outbound data, or all data. Other views have settings for the type of measurement--so you can set the view to display data rates, data volumes, or interface capacity utilization.

Follow these steps:

1. Open the dashboard that contains the view that you want to modify.
2. (Optional) Change the time frame, if necessary.
3. Open the dialog for editing the view settings:
   - (CA PC) Click the Edit icon  in the view title bar and select Edit from the menu.
   - (NPC) Click the View icon  next to the view name and select Edit from the menu.

     The settings dialog opens.
4. (Optional) Edit the Title to change the name in the view title bar.

5. (Optional) If the view has Measurement Settings, select the type of measurement to show in the report:
   - Rate: Rate of traffic, expressed in Mbps.
   - Bytes: Volume of traffic.
   - Utilization: Percentage of total capacity used by the traffic.
6. (Optional) If the view has Direction settings, select the direction of the data on the selected interface:
   - Out: Outbound traffic on the interface.
   - In: Inbound traffic on the interface.
   - From: Traffic on the interface that comes from the host (Host view) or the source host (Conversation view).
   - To: Traffic on the interface that goes to the host (Host view) or the destination host (Conversation view).
   - Total: All traffic on the interface.
7. (Optional) (CA PC) For an enterprise-wide view or interface-specific view, change the interface for the view: Select a different interface from the Context Settings table.

   For example, to restrict the interface set to a domain, select the domain from the IP Domains list.

   Note: You can change the context for a view on some custom dashboards in the CA Performance Center Console. You cannot change the context for built-in views or for interface context pages.

   To re-sort the table, click a column heading. Click the arrow to sort in the opposite direction.

   (CA PC) To change the columns that are included in the table, display the Columns list: Click near the right edge of a column heading, then click the white arrow and select Columns.
8. (Optional) Specify which users are affected by the setting changes: Select a value from the Apply Changes list:
   - For All Tenant Users: (CA PC) Saves the changes so that they apply to all users.
   - My User Account: Saves the changes to your user account as the default setting for this view.
   - My Current Session: Reverts the changes when you log out.

   Note: The availability of these options depends on your user account role rights.

9. Click Save (CA PC) or OK (NPC) to save your changes.

   The settings dialog closes. The view reflects your changes.

Note: You can also change the context for a dashboard in the CA Performance Center Console. In this case the context change applies the selected group or managed item as a filter to all views on the page.

Change the Context for a View

You can change the context for some individual views on a dashboard. Change the context of an enterprise-wide view to show data from a different set of managed items. Change the context of an interface-specific view in the CA Performance Center Console to show data from a different interface.

Changing the view context can be useful for troubleshooting. You can compare data from different locations, for example.

Follow these steps:

1. Open the dashboard that contains the view that you want to change.
2. (Optional) Change the time frame, if necessary.
3. Open the dialog for editing the view settings:
   - (CA PC) Click the Edit icon  in the view title bar and select Edit from the menu.
   - (NPC) Click the View icon  next to the view name and select Edit from the menu.

     The settings dialog opens.
4. Take one of the following steps:
   - (CA PC) Enterprise view: Click to expand folders in the Groups filter tree, and select the group whose data you want to see in the view.
   - (CA PC) Interface view: Locate the interface whose data you want to see in the view, and click the link in the table.
   - (NPC) Click the 'Filter by' value and select a group in the Select Context dialog.

     If the settings dialog does not contain a 'Filter by' option, you cannot change the context for the view.

   The context types that are available depend on the type of view.
5. (Optional) Change the view Title to reflect the new context.

6. Select the scope of your changes from the Apply Changes drop-down. Select one of the following options:
   - (CA PC) For All Tenant Users: Saves the changes so that they are only available to users associated with your tenant (possibly the Default Tenant).
   - My User Account: Saves the changes to your user account as a default for this view.
   - My Current Session: Reverts the changes when you log out.

   Note: The availability of these options depends on your user account role rights.
7. Click Save (CA PC) or OK (NPC).

   The view is updated to show data from the new context.

You can also change the context for a custom dashboard, which applies the selected group or managed item as a filter to all views on the page.

Set a Custom Time Frame

You can select a different time frame for the data shown in the current dashboard or view page. You can select the day, the start time, and the end time using the time period selectors.

Follow these steps:

1. Navigate to a dashboard or view page.
2. Click the date links in the upper-left corner of the dashboard page to open the calendar panes.
3. Select the beginning day and ending day of the new time period on the calendar panes.
4. Click the hours or minutes links to specify the beginning and ending times of the new time period.
5. Click Set.

   The custom time frame is applied to all of the views on the dashboard or page.

Zoom In to Narrow the Time Frame

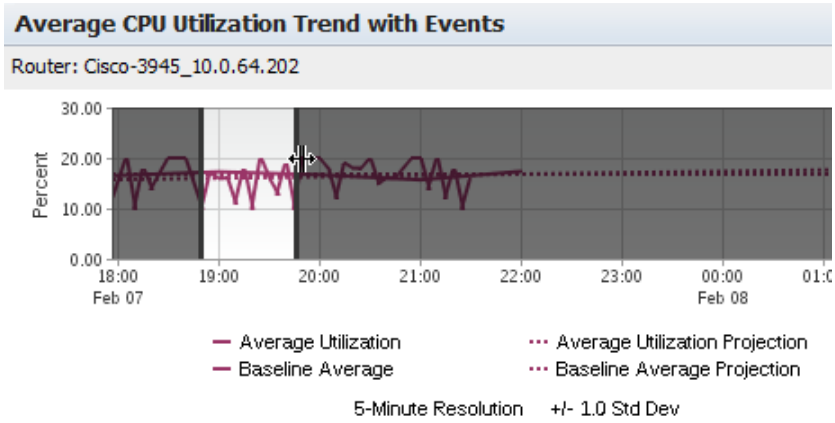
This topic describes how to zoom in to narrow the time frame for a trend chart in the CA Performance Center Console. This option is not applicable to trend charts in the CA NetQoS Performance Center Console.

You can look more closely at the data points from a small range by using the zoom feature. The ability to "zoom in" on a time frame is available for views that contain trend (line) charts. The feature is not available for bar charts, tables, or gauges.

Follow these steps:

1. Navigate to a dashboard page.
2. (Optional) Change the time frame, if necessary.
3. Select a view that contains a line chart.

   Note: You cannot zoom in on a bar chart, table, or gauge.
4. Click and drag, using the mouse to select an area of the chart.



   Select an area that spans at least 30 minutes. Black lines appear to indicate a valid selection.

   When you release the mouse button, the custom time period you selected is applied to the current view.
5. (Optional) Click Undo, just below the view, to return to the previous time frame.

   The view is refreshed. The previous time period is now applied to the view.
6. (Optional) Click Apply to Dashboard.

   The dashboard page is refreshed. The new time period is now applied to all views on the current dashboard page.

Custom Dashboards

Custom dashboards are useful for displaying data from a particular item or group of items. With a custom dashboard, you can select the item context for individual views and can make other modifications to meet the requirements of a selected operator.

Custom dashboards are often used on a temporary basis to troubleshoot an issue. However, they are also deployed on a long-term basis to monitor categories of items. For example, an operator who is responsible for a region requires a dashboard that shows only items in that region. Or an operator might require a dashboard to monitor all ESX servers.

To create a custom dashboard quickly, you can edit an existing dashboard and save it with a new title. Your user account must have the Edit Dashboards role right.

Note: Roles rights are slightly different in CA NetQoS Performance Center, For more information, see the *CA NetQoS Performance Center Help.*

Create a Custom Dashboard

If you have the necessary role rights, you can create custom dashboards. You can select views for the dashboard and set their location on the page. You also can select the menus that list the dashboard so that it can be shared with other operators.

You also can customize the views in a custom dashboard. For example, you can change the view title or the group context.

For step-by-step instructions, see the following topics:

- (CA PC Help) Create a Custom Dashboard
- (NPC Help) Creating Custom Reports in My Reports
- To include all views of CA Network Flow Analysis data: Build a Custom View for a Single Interface (see page 226)

Also See:

Build a Custom View for a Single Interface (see page 226)

Edit a Dashboard

This topic describes how to customize dashboard pages in the CA Performance Center Console. For information about customizing report pages in the CA NetQoS Performance Center Console, see the *CA NetQoS Performance Center Help*.

You can customize dashboard pages if your user account has the 'Administer Shared Dashboards' or the 'Create a Dashboard' role right. You can add or remove data views, rearrange views, or select a different context filter for a dashboard. You can then export the new dashboard as a report.

Follow these steps:

1. Log in as a user with the required administrative role rights.
2. Use the Dashboards tab to access the dashboard that you want to edit.
3. Click the More menu, and select Edit Dashboard.

   The Edit Dashboard Layout page opens.
4. Change the following menu and dashboard options, as needed:

   Menu for Dashboard

   Is the menu where you want the dashboard to appear. The default is the menu that you used to open this dashboard page.

   Menu Item

   Is the name of the dashboard as you want it to appear in the menu.

   Dashboard Title

   Is the name that you want to appear at the top of the new dashboard.
5. Select a layout template for the dashboard from the Layout buttons.
6. Remove unwanted views from the dashboard page if desired. In the Layout pane, click:
   - Clear to remove all views from the page.
   - An [X] to remove an individual view from the page.

Note: By default, the context is Summary. With the *Summary context* setting, the available views display summary data for the current group context of the dashboard. The Summary setting does not require you to select a specific group or item. Summary views dynamically update the context when you change the context of the page.

7. (Optional) Apply a group or context filter to the views. You can select a group, device, or interface by taking the following steps:

   a. Click Select Context.

   b. Select a Context Type, such as a type of managed item. Select Group to see the Groups tree.

      By default, the list is filtered to show only items and item types to which you have access. For example, if you are not monitoring any servers, the Context Type list does not include the Servers option. Select 'Show All Context Types' to see all context options.

   c. Select a specific context item or a group context.

   d. Click OK to save the new context filter.

   The views that are available to be added to the page are shown in categorized lists. The lists are filtered by the selected group or item context.

   All registered data sources are represented.

8. Click to expand the categories of views. Check the Display All Views option only if you want to see views from data sources that you have not registered.

9. Select a view, drag it to the Layout pane, and drop it where you want it to appear.

   Note: The maximum number of views per dashboard is 25.

10. (Optional) Use the editing shortcut buttons to create a copy of the view or access view settings, such as the Metric Family.

    For example, click the Copy icon  to place a copy of the view just below the original view in the layout. You can then alter view settings so that two similar views display different data.

11. (Optional) Click Revert to discard your changes.

    The layout returns to the settings that you last saved. Or, if you have not customized the dashboard, it returns to the predefined settings.

12. Click Save.

    The dashboard page refreshes to reflect your changes. The changes persist across login sessions.

Change the Context for a Dashboard

You can customize a dashboard by selecting a different data context for the data. The default group setting for the views that are shown on all dashboards is 'All Groups'. When you select another group for a standard dashboard, you apply a new filter to all views on the page. From a context page, such as details about a single router, you can select another managed item as the view context.

You can also view dashboards in multiple windows and apply a different data context to each dashboard.

Follow these steps:

1. Navigate to the dashboard that you want to modify.
2. (Optional) Change the time frame, if necessary.
3. Click the [change] link above the time period selectors.

   [change] link

   Lets you select another group or managed item context for reporting.

   A dialog opens with filtering options.
4. Click to select another managed item. Or expand nodes in the Groups tree to select a group context.

   Data from the new item or group appears in the view.
5. Click OK.

   All views on the page are refreshed to reflect the new data context. The change applies until you log out. To change the context so that the change persists across login sessions, edit the dashboard.
6. (Optional) Open another browser instance, log in, and open the same dashboard.

   You can now compare the same views with two different item context settings.

Change the Time Frame for a Dashboard

You can change the time frame for a dashboard you are viewing. Change the time frame to see performance data from an earlier time of day or from another date.

Changing the time frame is useful for troubleshooting performance issues. For example, if data from the past day contains an anomaly, you can change the time frame to show data from the last seven days. The time frame helps you determine whether the same issue is occurring regularly.

When you change the time frame for a dashboard, it is applied to all views on the page, and to all dashboards in that window. However, you can view dashboards in multiple windows and can apply a different time frame to each dashboard.

Follow these steps:

1. Select a dashboard from the Dashboards tab.
2. Click to select some of the following time and date options on the toolbar:

   Time period drop-down list

   Lets you select a predefined time frame for the data.

   Default: Last Hour.

   Back button

   Shifts the time frame for the data back by one increment of the present interval (such as Last Day or Last Hour).

   Date and Calendar drop-down lists

   Let you select a start and end date for the data from a calendar view.

   Time of Day drop-down lists

   Let you select a start and end time from a list of 15-minute time intervals in the 24-hour format.

   Forward button

   Shifts the time frame for the data forward by one increment of the present interval (such as Last Day or Last Hour).
3. To define a custom time frame, take one or more of the following steps:
   - Click the start date and select a new start date from the calendar that appears.
   - Click the end date and select a new end date from the calendar that appears.
   - Click the start hour or minute and select a new hour or minute from the drop-down menu.
   - Click the end hour or minute and select a new hour or minute from the drop-down menu.
4. Click Set.

   The page is refreshed, and the data displayed in the views reflects the new time frame.
5. (Optional) Scroll backward or forward in time. Use the Back and Forward buttons on either side of the timestamp to shift the time frame by one increment of the present interval.

   If you are viewing data for the last day, click the left arrow to scroll back in time by one day. Or click Latest to see the most recently collected data.

Change the Time Frame for a Dashboard

You can change the time frame for a dashboard or Interface page that you are viewing. Change the time frame to see data from an earlier time of day or from another date, for example

Changing the time frame is useful for troubleshooting performance issues. For example, if data from the past day contains an anomaly, you can change the time frame to show data from the last seven days. The time frame helps you determine whether the issue occurs repeatedly.

When you change the time frame for a dashboard or Interface page, it is applied to all views on the page, and to all dashboards in that window. You can view dashboards in multiple windows and can apply a different time frame to each dashboard, however.

Follow these steps:

1. Select a dashboard from the Dashboards tab or navigate to an Interface page.
2. (Optional) Click to select any of the following time and date options at the top of the page:

   Time period drop-down list

   Lets you select a predefined time frame for the data.

   Default: Last Hour.

   Back button

   Shifts the time frame for the data back by one increment of the present interval (such as Last Day or Last Hour).

   Date and Calendar drop-down lists

   Let you select a start and end date for the data from a calendar view.

   Time of Day drop-down lists

   Let you select a start and end time from a list of 15-minute time intervals in the 24-hour format.

   Forward button

   Shifts the time frame for the data forward by one increment of the present interval (such as Last Day or Last Hour).

3. (Optional) Define a custom time frame:
   a. Complete one or more of the following steps
      - Click the start date and select a new start date from the calendar that opens.
      - Click the end date and select a new end date from the calendar that opens.
      - Click the start hour or minute and select a new hour or minute from the drop-down menu.
      - Click the end hour or minute and select a new hour or minute from the drop-down menu.
   b. Click Set.

      The data in the views reflects the new time frame.
4. (Optional) Scroll backward or forward in time. Use the Back and Forward buttons on either side of the timestamp to shift the time frame by one increment of the present interval.

   If you are viewing data for the last day, click the left arrow to scroll back in time by one day. Or click Latest to see the most recently collected data.

Build a Custom View for a Single Interface

You can create custom views that contain CA Network Flow Analysis data for a single interface. You can add these interface views to a custom dashboard in the Performance Center Console.

Several interface views are available in addition to the views that are displayed by default on the interface pages.

Follow these steps:

1. Log in as a user with the required administrative role rights.
2. Navigate to the dashboard page that will contain the new custom view.
3. Click the More menu, and select Edit Dashboard (CA PC) or Edit Report (NPC).

   The page for editing the dashboard opens.
4. Open the dialog for selecting the context:
   - (CA PC) Click the Select Context link in the Views pane.
   - (NPC) Click the 'Filter by' value in the left pane.

   The dialog for selecting the context opens.

5. Select Interface from the Context Type list (CA PC) or Type list (NPC).

   A table of interfaces opens, which shows the available interfaces or interfaces and routers (CA PC).

6. Locate and select an interface.
7. (CA PC) Click OK.

   You return to the Edit Dashboard Layout page.

8. Expand the view category:
   - (CA PC) IP Flow
   - (NPC) Interface
9. Drag one or more of the interface views into the layout.

   A dashboard can contain a maximum of 25 views. If you include multiple copies of the same view type, you can edit each view on the custom dashboard to show content from a different interface.

10. Click Save.

    The dashboard page refreshes.

Sharing Data with Other Users

Multiple options let you share dashboards and views with coworkers. You can export a dashboard to a static report in PDF format. You can print reports or send them by email. You can set up a schedule to send a report automatically on a regular basis.

You can also export individual views. You can publish views on a web page, such as an intranet site. Or you can export data from a view to a file in CSV format. For all data-export options, certain user account role rights are required.

Print a Report

If your user account has the required role right, you can export the current dashboard contents as a printed report. The Print feature first displays the current dashboard page in PDF format.

Follow these steps:

1. Navigate to the dashboard that you want to export as a report.
2. (Optional) Change the time frame (see page 223).
3. Click the Print link on the toolbar.

   The report is exported as a PDF. Typically, it is displayed in a separate browser window.

   The data uses the current dashboard settings.
4. (Optional) Save the PDF to the local computer using the options in your PDF viewer.
5. Click the Print icon in the browser toolbar.

   The report page is sent to the local default printer.

Send a Report by Email

You can export the current dashboard or Interface page as a PDF report attached to an email message. The Email feature lets you specify the email address of the recipient and the Subject line of the email message.

Sending reports as email attachments requires an administrator to specify an SMTP server. In CA Performance Center, your user account must also have the required role, 'Send Reports by Email.' For more information, see the Related Topics.

Follow these steps:

1. Open the dashboard or Interface page that you want to send in an email message.
2. (Optional) Change the time frame, if necessary.
3. Click the Email icon on the toolbar.
4. Supply information for the following fields:

   Send To

   Specifies the email addresses where the report should be sent. Use the standard format:

   <name>@<domain>

   Note: Use commas or semicolons to separate multiple addresses. Or you can enter an email alias that includes multiple recipients.

Subject

Appears in the email Subject line; describes the emailed report.

Example: The dashboard title and any components whose data is included in the report.

Message

(Optional) Is a message to accompany the emailed report.

5. Select Send Now to send the email message immediately.

   Or select Send on a Schedule to create a schedule to send the email message on a regular basis. For more information, see Set Up a Recurring Email Schedule (see page 229).

   If the dashboard contains at least one multiview, a check box labeled 'Display maximum results for multiple-chart views' appears. Select this option if you want to include more charts from the multiview than can be displayed on the current "page" of results.

6. Click OK.

   The server generates a PDF from the current dashboard and sends the report as an attachment to an email message.

Set Up a Recurring Email Schedule

Each dashboard and Interface page contains options to export and send data in reports.

You can send a report by email immediately, or you can create a schedule for recurring emailed reports. For example, you can email interface utilization reports each week to coworkers in the IT department for capacity planning.

Note: The administrator must specify an email server to enable this feature. In CA Performance Center, your user account must have the 'Send Reports by Email' role.

Follow these steps:

1. Log in to the Performance Center Console.
2. Navigate to the dashboard or Interface report page that interests you.
3. Click Email.

   The Email Dashboard dialog opens.

4. Supply information in the following fields:

   Send To

   Specifies the email addresses where the report should be sent. Use the standard format:

   <name>@<domain>

   Subject

   Appears in the email Subject line; describes the emailed report.

   Example: The dashboard title and any components whose data is included in the report.

   Message

   (Optional) Is a message to accompany the emailed report.

5. Select one of the following Scheduling Options:

   Send Now

   Sends the email message immediately. Scheduling is not enabled.

   Send Daily

   Sends the email message once or more per day. If you select this option, select the day or days of the week when the report is sent.

   Default: Send the emailed report every weekday (Monday - Friday) at 0:30 hours in the time zone of the logged-in user. The data in the report reflects the previous 24 hours.

   Send Weekly

   Sends the email message once per week. If enabled, lets you select the day of the week to send the report.

   By default, the weekly schedule sends the emailed report every Sunday at 01:00 in your time zone.

   Default: The data in the report reflects the previous seven days (Saturday - Sunday).

   Week Ends on

   Determines the day when the week ends. The start of the week is automatically adjusted to include seven days.

Send Monthly

Sends the email message once per month. The report is sent on the first Sunday of each month at 01:00 in the time zone of the Management Console. The data in the report reflects the previous 30 days.

Send Email at

Determines the time of day when the message is sent. The start of the month is automatically adjusted to include 30 days.

Send Quarterly

Sends the email message once per quarter. The report is sent on the first Sunday of each quarter at 01:00 in the time zone of the Performance Center Console. The data in the report reflects the previous three months.

First Quarter Ends in

Determines the month when the quarter ends. The start of the quarter is automatically adjusted to include three months. All other quarters are also adjusted to proceed from the first quarter.

Send Yearly

Sends the email message once per calendar year. Sends the report on the last day of the month you select for the 'Year ends in' parameter. The data in the report reflects the previous 12 months.

Year Ends in

Determines the month when the year ends. The start of the year is automatically adjusted to include 365 days.

Send email at [time of day]

Sends the email message at a time you select.

6. Click Save to save the schedule.

   The report is saved as a PDF file and attached to an email message. It is sent immediately or according to the schedule you selected.

Manage Email Schedules

Users with the required role rights can set up schedules to send reports by email on a recurring basis. Selected dashboard or Interface page data is exported in report format and sent to designated users according to a regular schedule.

Users who have the role right to schedule emails can also manage email schedules for other users.

Follow these steps:

1. Log in to the Performance Center Console as a user with the appropriate role right. In CA Performance Center, you need the to 'Send Reports by Email' role.
2. Open the list of scheduled emails:
   - (CA PC) Select Admin, System Settings, and click Scheduled Emails.
   - (NPC) Select Admin, User Settings, and click Scheduled Emails.

   The list of scheduled emails opens.

   Note: Tenant administrators only see the items that are associated with their tenant.
3. Select the email schedule that you want to change, and click Edit.

   The dialog for editing the email schedule opens.
4. View or change the settings for email schedules. For more information, see Set Up a Recurring Email Schedule (see page 229).
5. Click Save.

   The list of scheduled emails reflects your changes.

Generate a URL for a View

You can export a view and share it with coworkers who do not have access to dashboards. Performance Center can generate a special uniform resource locator (URL) to recreate a selected data view on demand. The URL lets you add the view to a web page or intranet site. The Generate URL feature lets you involve others in capacity planning and infrastructure upgrade decisions, for example. This feature also lets you share status information.

A security token is included with each URL. This token is based on the user who is logged in at the time of URL generation. Consequently, any user who can access the exported view can see the same data that the original user who exported the URL could see. Note, however, that the token applies only to the initial view. If the user who is accessing the exported view attempts to drill in, he or she is asked to authenticate. The drilldown only succeeds after successful authentication, and then only for a user account with the Drill into Views role right. Finally, an option is included to let the token (and thus, the view) expire after a selected time period.

Follow these steps:

1. Log in as a user with the appropriate role right: 'Generate URLs from Views' (CA PC) or 'Allow User to Generate URLs' (NPC).
2. Navigate to the dashboard or Interface report page that contains the view that you want to generate as a URL.
3. Open the Generate URL dialog:
   - (CA PC) Click the Edit icon  on the view, and select Generate URL.
   - (NPC) Click the Edit icon  on the view, and select Generate URL.

   The Generate URL dialog opens. The URL is displayed in the URL field.
4. Enable or disable the following required parameters for the exported view:

   View Container

   Displays the chart or graph with a surrounding container. The container includes the title of the view in a title bar and a black outline around the chart or graph.

   Default: Enabled

   Copyright

   (CA PC) If enabled, shows the copyright information for the web page in the view.

   Drill Down

   Enables users to drill down from the view into the underlying data source for more detailed data. These users must have a minimal product privilege to the data source and the 'Drill into Data Sources' role right to use this feature.

   Default: Enabled.
5. Select from the following time frame options:

   Time Options

   (CA PC) Let you change the time frame for the data in the exported view. Supply a custom time frame in the Start Time and End Time fields, or select a Time Range from the drop-down list.

Time Span

(NPC) Let you select a time frame for the data in the exported view.

Token Expiration Options

Control view expiration. The default, 'Never' expires, lets the exported view display indefinitely.

If you want the view to expire, select a timeout period from the Token Expiration list. The URL includes an encrypted token that causes the view to expire after the specified timeout period.

The token does not enable the user who interacts with the generated view to drill down for more data.

6. (Optional) Click Preview (CA PC) or View Preview (NPC) to see how the view looks with the options you selected.
7. Copy the URL displayed at the top of the page to the Clipboard.
8. Paste the URL to the destination for displaying the view.
9. Click OK.
10. The Generate URL window closes.

Organizing Dashboards in Menus

Dashboards are organized into menus that have a central troubleshooting or monitoring purpose. You see a list of available dashboards and menus when you hover on the Dashboards tab (CA PC) or Reports tab (NPC).

Users with the required administrative role rights can reorganize menus. They also can create custom menus that contain built-in or custom dashboards. The users can associate the new menus with user account roles. When product operators log in, the dashboards they need for their daily tasks are organized in a meaningful way.

Administrators can remove a dashboard from any menu and add it to a shared menu.

View a List of Menus

This topic describes the menus in the CA Performance Center Console. For information about the CA NetQoS Performance Center Console menus, see the *CA NetQoS Performance Center Help*.

The Manage Menus page contains a list of currently defined menus. Before you add custom menus, only predefined menus are included in the list. The user account role determines the menus that each user can access.

Custom menus are defined for each tenant. Only the factory menus are shared among tenants. The global administrator sees a list of menus not explicitly associated with a tenant.

Follow these steps:

1. Log in as a user with the required administrative role rights.
2. Select Admin, User Settings, and click Menus.

   The Manage Menus page opens.

   The page displays the current list of menus. The following menus are provided with CA Performance Center and appear by default in the Menu List:

   Infrastructure Health

   Contains summary and overview dashboards with at-a-glance views of system and device health and performance, events, and threshold compliance.

   Application Health

   Contains overviews and detailed analysis of application performance. Also contains related dashboards, such as performance by protocol and server performance.

   Capacity Planning

   Contains dashboards that are related to projections, thresholds, and recent changes to systems or devices.

   Management

   Contains at-a-glance scorecards and overview dashboards, as well as high-level summary and comparison dashboards.

   Operations Displays

   Contains high-level overview dashboards appropriate for display in the Operations Center and for use by Network Operators.

To perform any action on this page, select a menu, and then click a button.

If any dashboards have been customized, the following additional menu appears:

My Dashboards

Contains frequently used dashboards for an individual user account. Any dashboards that this user modified become available in this menu.

Note: Users with the required role right can edit the My Dashboards menu for a user account by proxying that user account. For more information, see Proxy a User Account.

Custom Menus

Administrators and designers can create custom menus for the Dashboards tab (CA PC) or Reports tab (NPC). Custom menus let you determine which dashboards are available to each user account. For example, an operator might log in and see three or four menus of dashboards. The menus can be configured sot that the operators see only the data that they require.

If your user account has the necessary role right, you also can create custom dashboards (see page 220) to populate a custom menu.

Custom dashboards that are in a user's My Dashboards (CA PC) or My Reports (NPC) menu are not visible to other users. Users can therefore copy a dashboard from a factory menu to their My Dashboards or My Reports menu and customize it.

A custom menu is not available to any users until the administrator edits a role to include it. The role must, in turn, be assigned to a user account.

Add a Menu

Custom menus let you organize dashboards and make them available to selected roles. Administrators and designers can create custom menus and can select dashboards for each menu.

A custom menu is not available to any users until the administrator edits a role to include it. The role must, in turn, be assigned to a user account.

Follow these steps:

1. Log in as a user with the required administrative role rights.
2. Select Admin, Menus.

   The current list of menus opens.

3. Click New.

   The Add Menu page opens.

4. Supply values in the following fields:

   Name

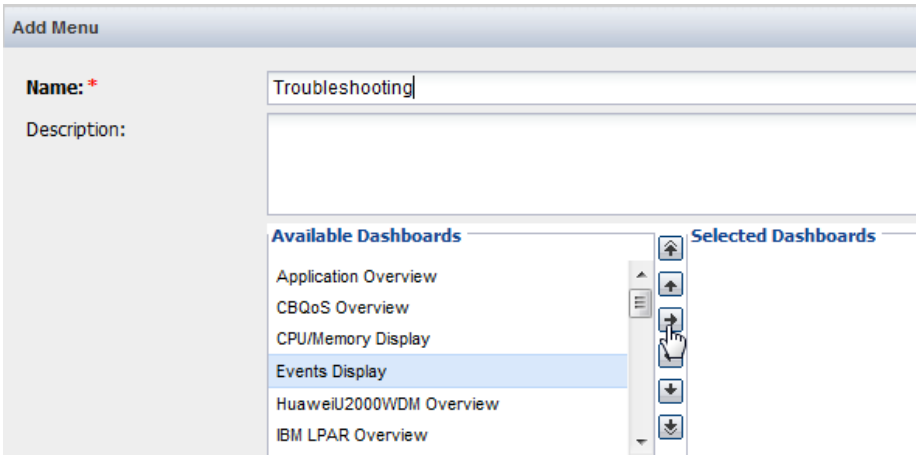
   Is a name for the menu. This name appears when you click the Dashboards tab.

   Description

   (Optional) Describes the menu to help other operators identify it.

5. Select a dashboard to include from the Available Dashboards list (CA PC) or Available Reports list (NPC).

   The following graphic shows the Add Menu page as it appears in the CA Performance Center Console.



6. Click the right arrow.

   The dashboard moves to the Selected Dashboards list (CA PC) or Selected Reports list (NPC).

   Use Shift + Click or Ctrl + Click to select multiple dashboards.

   (CA PC) Use the up and down arrows to change the order of the dashboards in the menu.

   Note: A maximum of 20 dashboards can be assigned to a single menu. An error message appears if you try to add more than 20 dashboards.

7. Click Save to save the menu and close the Add Menu page. Click Save & Add Another to save the menu and add another menu.

Edit a Menu

Administrators and designers can edit menus to meet the changing needs and new job responsibilities of operators. Administrators can edit custom or built-in menus by adding, removing, and reordering dashboards.

Follow these steps:

1. Log in as a user with the required administrative role rights.
2. Select Admin, Menus.

   The current list of menus opens.
3. Select the menu that you want to modify.
4. Click Edit.
5. Modify the menu settings as required.

   For example, to remove a dashboard from the menu, complete the following steps:

   - Select the menu in the Selected list.
   - Use the arrow button to move it to the Available list.

   Note: A maximum of 20 dashboards can be assigned to a single menu. An error message appears if you try to add more than 20 dashboards.
6. Click Save.

   The menu is edited.

Glossary

Autonomous System

Autonomous System (AS) refers to a connected group of Internet Protocol (IP) routing prefixes. The IP routing prefixes have a single, clearly defined routing policy and are controlled by one or more network operators. Meaningful AS data is available in reports only when routers and interfaces are configured to export it.

baseline

A *baseline* is a record of typical behavior, which is computed from past behavior. Baselines help you compare changes over time and predict future data or performance. Comparing current values to baseline projections is useful for determining whether current values are typical. The baseline in a trend plot is computed by using data from the six weeks before the selected date range, excluding the data point already in the trend plot.

conversation

A *conversation* is a session of subnet-to-subnet or user-to-user (host-to-host) traffic. The NFA console displays conversation information, so you can find out whether a particular conversation is causing a traffic spike on an interface, for example. You can create and run reports to identify the top volume-based conversations.

dashboards

Dashboards are dynamic report-building pages in the Performance Center Console. Dashboards are accessible from the Dashboards tab (CA PC) or Reports tab (NPC). Each dashboard is a collection of views that present data from registered data sources on a single web page. The layout, views, time interval, and group context of each dashboard can be customized.

drill down

To *drill down* is to navigate from one data view to another, more detailed data view or context page. The new page displays data from the same time frame, for the same managed item or set of items. You can drill down to details in CA Network Flow Analysis from views in CA Performance Center.

filter

A *filter* in a report is a set of selection criteria that are used to focus a report on the desired data.

flow

A *flow* is a set of IP packets that pass a network observation point during a certain time interval. In CA Network Flow Analysis 9.3.0, flow may consist of NetFlow v5, v7, or v9 or one of the following flow types that conforms to the standards for NetFlow v5, v7, or v9: sFlow version 5; or IPFIX, J-Flow, cFlow, or Huawei NetStream flow .

In order for data from non-sampled flows to appear in reports of 15-minute (historical) data, the following minimum fields are required:

- One of the following: 1 - IN_BYTES, 85 - IN_PERMANENT_BYTES, 231 - FW_INITIATOR_OCTETS, or 232 - FW_RESPONDER_OCTETS
- All of the following: 4 - PROTOCOL, 7 - L4_SRC_PORT, 8 - IPV4_SRC_ADDR, 10 - INPUT_SNMP, 11 - L4_DST_PORT, 12 - IPV4_DST_ADDR, and 14 - OUTPUT_SNMP

host

A *host* is a specific computer engaged in an exchange across the network. In some cases, a host represents a managed services provider whose IT staff manage and monitor the networks and systems of multiple customers. In CA Network Flow Analysis, hosts are identified by name or IP address. You can track host activity to find out whether a specific server or end-user system is responsible for significant traffic on an interface, for example. You can create and run reports about the traffic that is generated or is received by specified hosts.

interface

An *interface* is a point of connection, such as a Serial, Frame Relay, Fast Ethernet, ATM, or PVC interface. CA Network Flow Analysis reports on any logical interface that is enabled on a supported router that has flow enabled. The NFA console displays the interfaces that are monitored in your environment.

NetFlow

NetFlow is a transaction between two hosts, which uses a unique pair of port numbers and IP addresses and which includes certain network traffic information. A Cisco router can be configured to export flow information by sending UDP packets that contain flow statistics to one or more collectors such as the Harvesters. CA Network Flow Analysis supports NetFlow versions 5, 7, and 9 and sFlow version 5. CA Network Flow Analysis also supports IPFIX, J-Flow, cFlow, and Huawei NetStream that complies with the standards for NetFlow v5, v7, or v9.

Performance Center

Performance Center is a term this documentation uses to refer to CA Performance Center and CA NetQoS Performance Center collectively. CA Network Flow Analysis is designed to be used with one of these programs. Page names or functions that are specific to a Performance Center version may be identified by the full program name or acronym. *CA PC* is used as an acronym for CA Performance Center and *NPC* is used for CA NetQoS Performance Center.

protocol

A *protocol* is a standard for regulating communication between computers. Common protocols include: HTTP, SNMP, FTP, and VoIP. The information that is displayed may include the top protocols in and out for a particular interface. This information can help identify which application is causing network traffic. You can also create and run reports to determine which protocols and applications are used by different groups in your organization.

QoS (Quality of Service)

QoS (Quality of Service) is a defined level of performance--quality of transmission and service availability--in a data transmission system.

report

A *report* is a display of collected data, which you view in the NFA console from the Enterprise Overview, Interfaces, Custom Reporting, Flow Forensics, and Analysis pages. You can print or save reports in PDF format. You can also export reports as comma-separated value (CSV) files. An Administrator can set up some reports to be sent by email at scheduled intervals.

reporting period

A *reporting period* is a user-specified time range for data to be included in a CA Network Flow Analysis report. The time options vary with each report type, but the report period could consist of hours, days, weeks, or months.

Summary views

Summary views provide an overview of high-level information, such as averages from groups of managed items. Summary views often provide drilldown paths to more detailed, related pages.

threshold

A *threshold* is a user-definable limit. Meeting or exceeding a threshold may trigger an alarm. Thresholds are also used in some views to determine the status colors for items. For example, the Interface Utilization view on the Enterprise Overview page uses user-definable utilization thresholds for the status colors of the top interfaces.

two-tier or three-tier architecture

Two-tier or three-tier architecture refers to the type of CA Network Flow Analysis deployment in use. The components work together in both architectures to collect, process, and store flow data; display the data in reports; and generate traps, events, and scheduled reports.

A two-tier architecture deployment consists of the NFA console and one or more new Harvesters. These components may be located on separate servers or on a stand-alone server. A three-tier architecture deployment also includes one or more servers that have a DSA (Data Storage Appliance) component. The DSA stores the 15-minute (historical) data. Separate servers are used to host the components in a three-tier architecture deployment.

view

Views, or *data views*, present report data, usually as a bar graph, pie chart, table, trend chart, or stacked trend chart. A view is created on the fly when you display data in the NFA console or the Performance Center Console. For example, the Enterprise Overview page in the NFA console consists of a collection of views. In some cases you can export the view data to a file in CSV format or create a PDF report from it.

Index

.

.CSV (comma-separated value) files
  saving reports/views as • 18

1

15-minute (historical) data
  collected for reports • 21

A

Administration page
  brief description of use • 15
Analysis reports
  Analysis page described • 15
  capabilities • 135
  creating • 136
  creating folder for • 107
  deleting report folders • 109
  editing • 142
  filter combinations • 135
  moving reports between folders • 108
  overview • 135
  possible uses of • 15
  renaming folder for • 108
  Report Definition Summary • 142
  using report wizard • 136
  viewing • 140
applications
  creating Custom Reports about use • 84
Apply Conversation Filter dialog
  Custom Reports • 99
Apply Host Filter dialog
  Custom Reports • 99
AS (Autonomous System) data
  Stacked AS Trend report • 70
  Top N AS Numbers report (Interfaces) • 59

B

baselines
  showing in Flows report (Interfaces) • 48

C

CA Anomaly Detector (AD) views
  Anomaly Activity • 203
  Anomaly Detector Overall Status • 204
  Anomaly Drill-In • 210
  Anomaly Trend (drill-in) • 212
  Enterprise-Wide Anomalies • 208
  Enterprise-Wide Correlated Anomalies • 206
  links • 209
  Top Anomalies by Host • 205
  Top Anomalies by Interface • 206
  Top Enterprise-Wide Network Anomalies • 204
CA Network Flow Analysis
  capabilities/benefits • 14
CA Network Flow Analysis components
  briefly described • 15
CA PC/NPC
  navigating context pages • 155
  need for Performance Center • 21
  report page types • 154
calculations
  Calculations options (Capacity Planning) • 58
  data in kilobytes • 21
Calendar Chart/Utilization report (Interfaces)
  contents/working with • 50
  described/illustrated • 75
  example of • 81
  in CA PC/NPC • 169
Capacity Planning report (Interfaces)
  Calculations options • 58
  described/opening • 52
  time filters • 58
  Trend Settings display options • 56
  views and fields • 53
conversations
  adding as filters to Custom Reports • 99
  adding to an Analysis report • 136
  Apply Conversation Filter dialog • 99
  Conversation Summary report • 74
  lifespan of collected data • 21
  Top N Conversations report (Interfaces) • 46
Custom Reports
  creating • 86
  creating folder for • 107
  deleting filters • 102
  deleting report definitions • 109
  deleting report folders • 109
  disabling interfaces • 93

excluding/including filters • 102
list of functions • 85
managing/organizing • 107
moving reports between folders • 108
page briefly described • 15
protocol filters • 97
renaming folder for • 108
Report Definition Summary • 90
report types and typical uses • 84
rules for including utilization • 96
selecting a time filter • 104
setting reporting period • 104
setting resolution • 104
setting schedules • 105
valid filter combinations • 96
viewing • 106

D

dashboards (CA PC)
Calendar Heat Chart (Flow) view • 169
changing data context • 223
changing time frame • 218
creating • 220
creating NFA interface views • 226
Interfaces Over Threshold • 165
Stacked Protocol Trend view • 172
Stacked ToS Trend view • 175
Top Conversations (Bar) view • 183
Top Conversations (Pie) view • 185
Top Conversations (Table) view • 187
Top Enterprise Hosts by Volume • 160
Top Enterprise Protocols by Volume • 161
Top Flows by Interface • 163
Top Hosts (Bar) view • 189
Top Hosts (Pie) view • 191
Top Hosts (Table) view • 193
Top IP Interface Utilization (Flow) • 162
Top Protocols (Bar) view • 196
Top Protocols (Pie) view • 198
Top Protocols (Table) view • 200
ToS Summary (Pie) view • 178
ToS Summary (Table) view • 180
data
raw data in Flow Forensics • 128
types collected for reports • 21
documentation
location/list of • 4
drilldown reports
changing interface • 17
links to open • 16
opening for protocols • 31
opening from CA PC/NPC • 36
Duration report
description • 86
specifying Analysis report type • 136

E

email
Email Information dialog • 18
Interface page option • 33
reports • 18
scheduled Analysis reports • 136
scheduled Custom Reports • 86
Enterprise Overview page
accessing • 23
brief description of use • 15
briefly described • 15
Interface Utilization view • 26
Refresh/Email/Print icons • 23
setting utilization thresholds • 27
Top Hosts view • 30
Top Interfaces view • 28
Top Protocols view • 30

F

filters
combinations for Custom Reports • 96
filter combinations for Analysis reports • 135
Interface Index list • 17
on-the-fly Flow Forensics filters • 128
Flow Forensics page
accessing • 128
briefly described • 15
Flow Forensics reports
capabilities • 128
creating • 128
creating report folders • 107
deleting report folders • 109
link on Interface page • 33
moving reports between folders • 108
overview • 111
renaming report folders • 108
viewing • 133
VLAN-based reports • 126
WAAS Segment reports • 127
Flows report (Interfaces)

contents/working with • 48
Show Baselines • 48
Top Flows by Interface (CA PC view) • 163
folders
creating report folders • 107
deleting report folders • 109
renaming report folders • 108

G

groups
locating interfaces by group • 35
Growth report (Interfaces)
described/illustrated • 51

H

hops
Next Hops report (Flow Forensics) • 119
hosts
adding as filters to Custom Reports • 99
adding to an Analysis report • 136
Apply Host Filter dialog (Custom Reports) • 99
displaying extra information in Tooltips • 16
Flow Forensics reports • 111
Host Summary report • 73
lifespan of collected data • 21
opening drilldown reports • 32
opening for hosts • 32
Stacked Host Trend report • 69
Top Enterprise Hosts (CA PC/NPC) • 160
Top Hosts (Enterprise Overview) • 30
Top N Hosts report (Interfaces) • 43

I

ICMP
Flow Forensics reports • 115
icons/links
Change (interface for report) • 17
Jump Down arrow • 17
Scroll Back/Forward • 62
Interface Group Selection dialog
Jump Down arrow • 17
interface groups
adding to Custom Reports • 91
report dependencies on • 93
Interface Index page
locating interfaces (Group tab) • 35
Router tab • 34
searching/filtering • 17
Interface page report types
Calendar Chart - illustrated • 75
Calendar Chart (Utilization) • 50
Calendar Chart example • 81
Capacity Planning report • 52
Conversation Summary • 74
Flows report • 48
Growth report • 51
Host Summary • 73
Mixed Chart/Mixed Trend • 82
Overview report • 37
Pie Charts - example • 79
Protocol Summary • 72
Stacked AS Trend • 70
Stacked Host Trend • 69
Stacked Protocol Trend • 67
Stacked ToS Trend • 68
Stacked Trend Charts - example • 76
Summary Table - example • 80
Top N AS Numbers report • 59
Top N Conversations report • 46
Top N Hosts report • 43
Top N Protocols report • 38
Top N ToS report • 41
Trend Charts - examples • 77
Interface page reports
accessing from Enterprise Overview • 16
brief description of page • 15
built-in timeframe • 62
changing interface for • 60
changing timeframe for • 61
customizing timeframe for • 63
displaying rate/volume/utilization • 67
for hosts (Enterprise Overview) • 32
for protocols (Enterprise Overview) • 31
Interface page overview • 33
Presentation menu options • 64
scrolling timeframe for • 62
Show Other option • 67
Interface Utilization view
Enterprise Overview • 26
Interfaces Over Threshold (CA PC/NPC) • 165
Top IP Interface Utilization (CA PC/NPC) • 162
interfaces
adding as Custom Reports filters • 91
adding as Flow Forensics filters • 128
changing in interface report • 60
configuring utilization view • 27
creating NFA views in CA PC/NPC • 226

displaying Tooltips about • 16
drilldown report (Enterprise Overview) • 16
Interface/ Group Index (Analysis) • 136
report dependencies on • 93
searching for (Interface Index) • 34
setting utilization thresholds • 27
shown on Enterprise Overview page • 26
Top Interfaces (Enterprise Overview) • 28
utilization view (Enterprise Overview) • 26
IP Summary (Capacity Planning)
report contents described • 53

J

Jump Down arrow
described • 17

K

Keep Settings at Top option
Presentation menu (Interfaces) • 64
kilobytes
number of bytes used in display data • 21

M

MAC
MAC adddress reports (Flow Forensics) • 118
masks
adding as Custom Report filters • 86
adding as Flow Forensics filters • 128
Max per Page option
Interface Index • 34
Mixed Chart/Trend options
Presentation menu • 82
moving
reports between folders • 108
MPLS
Flow Forensics filters • 119

N

navigation tips
NFA console • 16
NFA console
address for logging in • 15
briefly described • 15
Custom Reporting page • 83
Enterprise Overview page • 23
Interface page • 33
navigation tips • 16

O

online help
accessing • 18
Overview report (Interfaces)
contents/working with • 37

P

Pie Charts
example of • 79
ports
adding as Flow Forensics filters • 112
Presentation menu (Interfaces)
Mixed Chart/Trend options • 82
options for interface reports • 64
selecting Rate/Volume/Utilization • 67
Show Other option • 67
print
Interface page option • 33
protocol groups
using as filters (Analysis reports) • 136
using as filters (Custom Reports) • 97
protocols
Capacity Planning report • 53
opening drilldown reports • 31
Protocol Summary report (Interface reports) • 72
Top Enterprise Protocols (CA PC/NPC) • 161
Top N Protocols report (Interfaces) • 38
Top Protocols (Enterprise Overview) • 30
using as filters (Custom Reports) • 97

R

rate
displaying in interface reports • 67
Refresh option
Interface page • 33
Report Definition Summary
for Custom Reports • 90
report folders
creating • 107
renaming • 108
Report Types dialog
Flow Forensics reports • 128
reporting periods
setting for Custom Reports • 104
reports
Analysis • 135
Custom Reporting • 85

emailing • 18
Enterprise Overview • 23
Flow Forensics • 128
Interface page • 33
printing • 20
saving data to CSV files • 18
sorting lists/table data • 16
views of NFA data in CA PC/NPC • 156
resolution
setting for Analysis report • 136
setting for Custom Reports • 104
routers
adding as Flow Forensics filters • 128
displaying contents (Interface Index) • 34
Routers with Most Flow Traffic (CA PC/NPC) • 168

S

schedules
Custom Reports (Duration type) • 86
setting for Analysis reports • 136
setting for Custom Reports • 105
Scroll Back/Forward icons
for interface report timeframe • 62
servers
creating Custom Reports about activity • 85
Show Other option
in interface reports • 67
Stacked AS Trend report (Interfaces)
described/illustrated • 70
Stacked Host Trend report (Interfaces)
described/illustrated • 69
Stacked Protocol Trend report
in CA PC/NPC Interface pages • 172
on Interfaces report page • 67
Stacked ToS Trend report (Interfaces)
described/illustrated • 68
Stacked Trend Charts (Interfaces)
example of • 76
Start-and-End report
specifying Analysis report type • 136
specifying Custom Report type • 86
summary data types
selecting for Custom Reports • 96
Summary Tables (Interfaces)
example of • 80

T

tables
sorting by column heading • 16
Summary Table report example • 80
TCP
TCP Flags report (Flow Forensics) • 125
thresholds
defining top interfaces • 28
for Analysis reports • 136
for interface utilization • 27
time filters
adding to Analysis reports • 136
adding to Custom Reports • 86
selecting for Custom Reports • 104
time frames
built-in options for interface reports • 62
changing for interface reports • 61
customizing for interface reports • 63
scrolling for interface reports • 62
Tooltips
use described • 16
Top Flows by Interface view
view in CA PC/NPC • 163
Top Hosts view
bar chart (CA PC/NPC) • 189
Enterprise Overview page • 30
pie chart (CA PC/NPC) • 191
table (CA PC/NPC) • 193
Top Enterprise Hosts by Volume (CA PC/NPC) • 160
Top Interfaces view
Enterprise Overview • 28
Top N AS Numbers report (Interfaces)
contents/working with • 59
Top N Conversations report
bar chart (CA PC/NPC) • 183
contents/working with • 46
pie chart (CA PC/NPC) • 185
table (CA PC/NPC) • 187
Top N Hosts report (Interfaces)
contents/working with • 43
Top N Protocols report
bar chart (CA PC/NPC) • 196
Interface report page • 38
table (CA PC/NPC) • 200
Top Protocols (Pie) (CA PC/NPC) • 198
Top N ToS report (Interfaces)
contents/working with • 41

Top Protocols view
CA PC/NPC protocol views • 161
Enterprise Overview • 30
ToS
adding as Custom Reports filters • 98
adding as Flow Forensics filters • 128
Capacity Planning report • 53
Stacked ToS Trend report • 68
Stacked ToS Trend view (CA PC/NPC) • 175
Top N ToS report (Interfaces) • 41
ToS Summary (Pie) (CA PC/NPC) • 178
ToS Summary (Table) (CA PC/NPC) • 180
ToS, creating Custom Reports • 84
ToS/ToS Group Index (Analysis) • 136
ToS groups
adding as filters to Custom Reports • 98
Trend Charts
examples of • 77
Stacked Protocol Trend report • 67
Trend Settings
calculation options (Capacity Planning) • 58
display options (Capacity Planning) • 56
troubleshooting
Unknown interface group message • 93

U

Unknown interface group message
Custom Reports • 93
utilization
configuring display (Enterprise Overview) • 27
creating Custom Reports about • 84
displaying in interface reports • 67
Interface Utilization (Enterprise Overview) • 26
rules for use in reports • 96
thresholds for display • 27
Top Interfaces (Enterprise Overview) • 28
Utilization/Calendar Chart report (Interfaces)
contents/working with • 50
described/illustrated • 75

V

views (AD data in Performance Center)
AD views list/opening • 202
Anomaly Activity • 203
views (NFA data in Performance Center)
changing context • 217
changing settings • 215
creating custom views • 220
creating NFA interface views • 226
Interfaces Over Threshold • 165
list of views • 156
Stacked Protocol Trend • 172
Stacked ToS Trend • 175
Top Conversations (Bar) • 183
Top Conversations (Pie) • 185
Top Conversations (Table) • 187
Top Enterprise Hosts by Volume • 160
Top Enterprise Protocols by Volume • 161
Top Flows by Interface • 163
Top Hosts (Bar) • 189
Top Hosts (Pie) • 191
Top Hosts (Table) • 193
Top IP Interface Utilization (Flow) • 162
Top Protocols (Bar) • 196
Top Protocols (Pie) • 198
Top Protocols (Table) • 200
ToS Summary (Pie) • 178
ToS Summary (Table) • 180
VLAN
Flow Forensics reports • 126
volume
adding as Flow Forensics filter • 128
displaying in Flow Forensics • 128
displaying in interface reports • 67

W

WAAS segments
Flow Forensics reports • 127
wild cards
used in Interface Index searches • 17