Cascade Pilot Reference Manual

Version 3.0

May 2011

riverbed®

Think fast.™

This manual is for informational purposes only. Addresses shown in screen captures were generated randomly by simulation software and used only on an internal network. They are for illustrative purposes only and are not intended to represent any real traffic involving any registered IP or MAC addresses.

The content of this manual is furnished on a RESTRICTED basis and is subject to change without notice and should not be construed as a commitment by Riverbed Technology, Incorporated. Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in Subparagraphs (c) (1) and (2) of the Commercial Computer Software Restricted Rights at 48 CFR 52.227-19, as applicable. Riverbed Technology, Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in this book.

riverbed

Riverbed Technology
199 Fremont Street
San Francisco, CA 94105

Phone: 415.247.8800
Fax: 415.247.8801
Web: http://www.riverbed.com

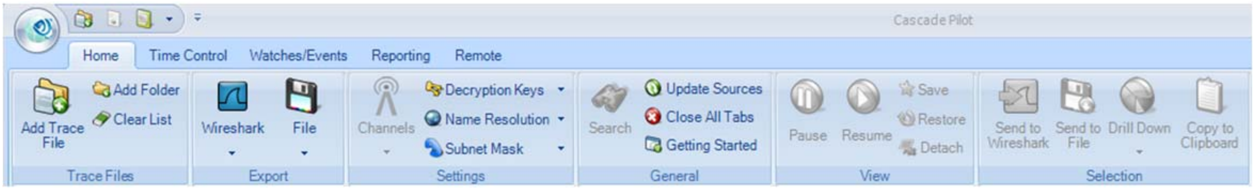
712-00094-01

Contents

About this guide

The purpose of this reference manual is to document and explain each Cascade Pilot feature. It is assumed that the reader is familiar with networking protocols and the principles of a networking stack. Care has been taken to avoid technical explanations except when necessary for conceptual understanding or functional explanation.

This manual is not intended to be a tutorial on the use of Cascade Pilot. Video tutorials on how to perform common actions are available in the product. Upon startup, the Cascade Pilot displays links to video tutorials. These can also be accessed at any time by clicking the *Getting Started* icon. This is located in the “General” section of the “Home” tab.



Overview

Cascade Pilot works with the Cascade Shark to provide a complete enterprise-wide solution for increased network visibility through live traffic monitoring, line-rate packet capture, real-time and historical traffic analysis, monitoring, and reporting from multiple locations.

Cascade Shark and Cascade Pilot provide a seamless distributed network analysis, visualization, monitoring, recording, and reporting solution.

Cascade Shark architecture

Figure 1: Cascade Shark appliances

The Cascade Shark appliance, which houses the traffic analysis engine along with a custom packet recording facility, extends the reach of the Cascade Pilot analyzer to geographically-dispersed network locations. Cascade Shark appliances are designed for placement at strategic points throughout your network, thereby providing the visibility necessary for global monitoring and troubleshooting. Cascade Shark comes as a fully configured rack mountable appliance including one or more network interfaces for network traffic capture.

The Cascade Shark also includes the Shark Packet Recorder, a customized packet capture application for high fidelity, multi-gigabit per second network traffic recording.

Cascade Pilot

Figure 2: Cascade Pilot

Cascade Pilot seamlessly and securely interfaces with one or more Cascade Shark appliances to display, drill down into, rewind, alert on, and report on, network traffic captured and/or analyzed by Cascade Shark appliances. Cascade Pilot is an analysis tool tailored to distributed environments with the ability to efficiently access and manipulate large packet trace files. It contains an extensive collection of network traffic analysis metrics (Views), drag and drop drill-downs, visualization and analysis of long-duration capture statistics, flexible trigger-alert mechanisms, and professional report generation.

After connecting to a Cascade Shark appliance, Cascade Pilot can access remote network data seamlessly. Users can apply Views to remote traffic sources (live or off-line), which are computed by Cascade Shark and the results are transmitted to Cascade Pilot for rendering.

Together, Cascade Pilot and Cascade Shark provide a powerful distributed network analysis, visualization, monitoring, recording, and reporting solution.

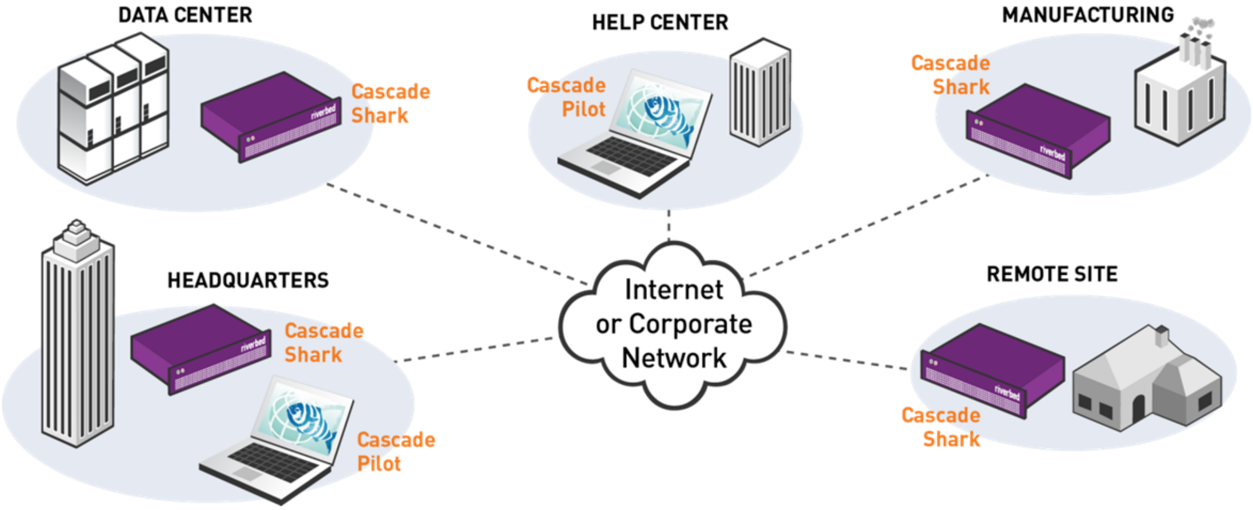


Figure 3: Deployment example

Cascade Pilot – Feature Summary

Cascade Pilot includes the following features:

- Graphical user interface for displaying data collected by remote Shark appliances and local network traffic sources
- Wireshark Integration
- Views and Charts
- Drill-down
- Time Control
- Watches
- Report Generation
- Access to the Cascade Shark appliance Web Interface
- Interface to the Shark Packet Recorder’s Jobs Repository

Graphical User Interface

Cascade Pilot can view and analyze network traffic on local interfaces or trace files, and also connect to and manage one or more remote Shark appliances. When connected to remote Shark appliances, Cascade Pilot can analyze and view traffic from network interfaces of the Shark appliances as if these remote interfaces were local.

A single Cascade Pilot can simultaneously connect to multiple Shark appliances, while multiple instances of Cascade Pilot can simultaneously connect to the same Shark appliance. Access to a single appliance from multiple locations provides excellent visibility into the network as well as an intuitive mechanism for sharing network Views, Watches, and Reports with co-workers and management.

Wireshark Integration

Cascade Pilot and the Shark appliance are fully integrated with Wireshark, allowing you to leverage your team's existing expertise with the world's most popular and widely deployed network and protocol analysis tool. During any stage of the analysis, Cascade Pilot can select a local or remote traffic source and send it to Wireshark for packet filtering or deep packet inspection.

Views and Charts

Views are the core analysis and visualization paradigm in Cascade Pilot. The system offers over 200 views providing a broad range of protocol support for both wireless[1] and wired network analysis. When views are applied to a traffic source, the results are displayed via a collection of interactive components called Charts. The collection of Charts includes bar, pie, and strip charts, sequence diagrams, scatter plots, conversation rings, and grids. All charts are interactive – they can be resized, moved, and, most importantly, users can make visual selections on graphical elements within a Chart (such as individual bars in a bar chart or time intervals in a strip chart) and drill down from there. Charts can be customized, saved, imported/exported in a variety of formats, and shared with colleagues. Chart data can also be exported included as part of Cascade Pilot automated report generator.

Drill-down

Drill-down is one of the most powerful and unique features of Cascade Pilot. When you apply a View to a packet data source, a Chart is displayed, revealing the network traffic results specified by the chosen View. Drill-down occurs when you then apply additional View selections to a Chart display. This simple yet powerful exercise increases your analysis capabilities many-fold. By employing this visually based Drill-down feature, Pilot can analyze very large trace files quickly, guiding you to the handful of packets responsible for anomalous network behavior.

Time Control

Viewing metrics computed over days, weeks, and months can be overwhelming. With the Pilot "back-in-time" technology, however, you can move through View metrics computed over extended periods of time with just a few mouse clicks. Based on your selected time interval, sub-sampling and aggregation techniques are used to optimize the granularity of the visual presentation, allowing you to easily zoom in and out of the View metrics. The Time Control technology applies to live and off-line traffic.

Filtering

In addition to Drill-down, filtering is a powerful resource to analyze data and focus down on packet data sources. Filters can be chosen from the Filter panel and easily applied to the current view by dragging them over existing charts. In addition, the currently applied filters can be edited and/or combined by using the Filter Bar on the top of the view, which enables fast and responsive data analysis. Users can create filters from existing charts by selecting elements such as time ranges, or choose among Pilot, BPF, Wireshark and time filters. Users can also organize custom filters in folders in the Filter panel.

Watches

The Cascade Pilot includes a sophisticated triggering and alerting technology called Watches. With Watches, you are able to create a trigger on many View metrics and be alerted when a specified condition computed on a metric is met. For instance, you can be alerted when unusually high bandwidth utilization, slow server response times, high

[1] Live wireless analysis only applies to locally attached AirPcap traffic sources.

TCP round-trip times, and other conditions occur. When a Watch detects that a trigger condition is met, a specified action is taken, such as logging the event, sending email, starting a packet trace capture, and more.

Report Generation

Customized reports can be automatically generated to show elements such as:

- Conversations (at any or all network layers)
- IP Fragmentation Analysis
- DHCP Address Assignments
- TCP Top Talkers
- Unicast vs. Multicast vs. Broadcast Traffic
- And others

Cascade Shark Web Interface

Cascade Pilot provides access to the Shark appliance configuration manager. The Web Interface supports the following configuration tabs:

- **Appliance Status** – Shows the status and enables restart of the Shark appliance.
- **Capture Jobs** – Shows the status of all of the current Capture Jobs, and enables adding, editing, deleting, starting, or stopping capture jobs.
- **Export Packets** – Allows exporting packets saved in a Capture Job to a trace file.
- **User Management** – Provides access to users/groups and the ability to add or remove users/groups.
- **Capture Ports Setup** – Configures the packet capture board(s) on the Shark appliance.
- **Port/Protocol Definition** – Adds or edits new protocol definitions and protocol groups.
- **Logs** – Provides access to the Shark appliance logs.
- **Settings** – Configures various settings of the appliance.

Interface to the Shark Packet Recorder Jobs Repository

The packet storage associated with a Capture Job is called a *Job Trace*. Each Job Trace is shown in the *Jobs Repository* folder of the Files panel. Depending upon how the Capture Job is configured and the speed of the network, the corresponding Job Trace may be a very large, multi-terabyte file. Using the “Trace Clip” creation feature of Cascade Pilot, you can have ready access to arbitrary time intervals within a Job Trace. Trace Clip time intervals, their location in time, and their size can be controlled easily. All Cascade Pilot operations that apply to trace files can be applied to Trace Clips as well.

In fact, hundreds of easy-to-use Charts can be scoped and limited to any requested format condition. Charts can be combined in a single report or recreated in separate reports in one or more formats. Supported formats include:

- PDF
- Microsoft Excel
- Microsoft Word
- HTML

All relevant trace files and their MD5 digests can be automatically packaged in a ZIP file along with the generated reports for easy distribution.

Hardware and Software Requirements for Cascade Pilot

Cascade Pilot is available on most Windows platforms. Although the system requirements for a Cascade Pilot scale with usage, in order to use Cascade Pilot effectively, the following minimum configuration is recommended:

Operating System

Windows XP, Windows Vista, Windows 7

Host Hardware

A dual-core 2.0 GHz CPU or better

Available Disk Space

A base installation requires approximately 300MB of disk space. Additional space is required to store generated reports or trace files created with Cascade Pilot.

Memory

2 GB or more of system memory

Video Hardware and Settings

A graphics card with a minimum resolution of 1024 x 768

Graphical User Interface

Graphical User Interface Components

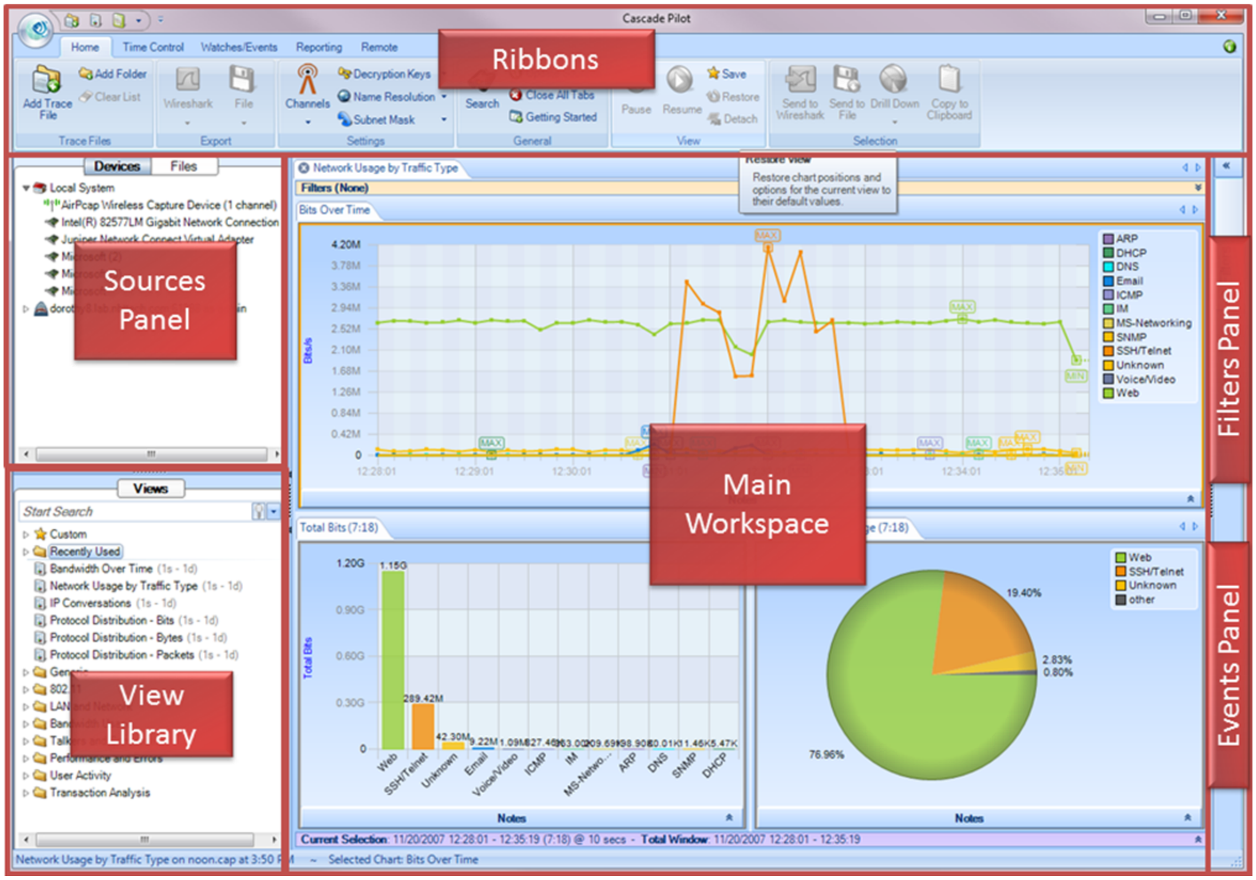


Figure 4: User Interface Breakdown (Major)

The graphical user interface of Cascade Pilot, divided into the five main sections, is shown in Figure 4. Each section represents a major topic in this manual. The descriptions below are conceptual overviews of each section.

Ribbon Panel

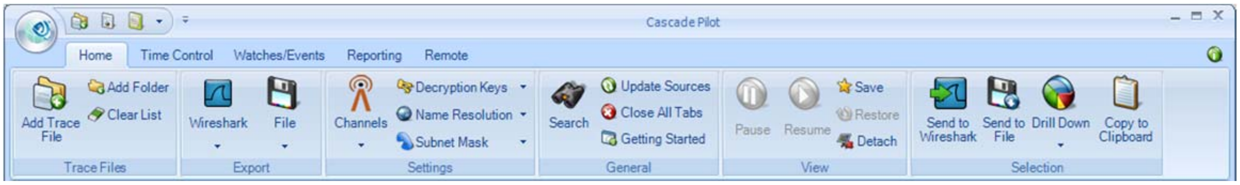


Figure 5 Ribbon panel

The *Ribbon Panel* provides access to global settings, management, and general actions. There are five ribbon panels (Home, Time Control, Watches/Events, Reporting, and Remote) that can be tabbed through using the mouse wheel.

Sources Panel

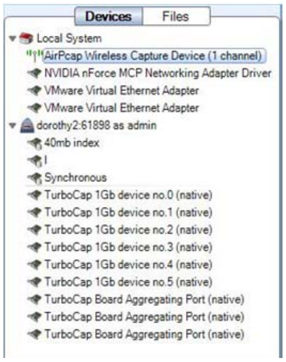

Devices
Files
Local System
AirPcap Wireless Capture Device (1 channel)
NVIDIA nForce MCP Networking Adapter Driver
VMware Virtual Ethernet Adapter
VMware Virtual Ethernet Adapter
dorothy2:61898 as admin
40mb index
I
Synchronous
TurboCap 1Gb device no.0 (native)
TurboCap 1Gb device no.1 (native)
TurboCap 1Gb device no.2 (native)
TurboCap 1Gb device no.3 (native)
TurboCap 1Gb device no.4 (native)
TurboCap 1Gb device no.5 (native)
TurboCap Board Aggregating Port (native)
TurboCap Board Aggregating Port (native)
TurboCap Board Aggregating Port (native)

Figure 6: Shark appliances, Devices, and Files panel

The *Sources Panel* contains representations of Shark appliances, interfaces, and trace files and is one of the most important parts of Cascade Pilot. It has two tabs, “Devices” and “Files” that can be cycled through by clicking on them.

Devices

Shows both local interfaces under the Local System icon and interfaces on connected Shark appliances that offer live sources of network traffic.

Files

Shows folders and trace files on the local system and connected Shark appliances.

Views Panel

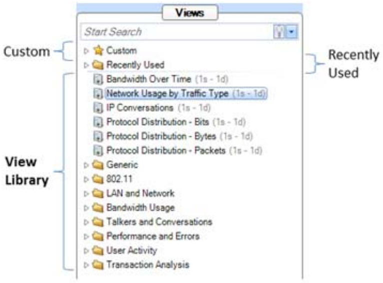

Views
Start Search
Custom
Custom
Recently Used
Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)
IP Conversations (1s - 1d)
Protocol Distribution - Bits (1s - 1d)
Protocol Distribution - Bytes (1s - 1d)
Protocol Distribution - Packets (1s - 1d)
Recently Used
View Library
Generic
802.11
LAN and Network
Bandwidth Usage
Talkers and Conversations
Performance and Errors
User Activity
Transaction Analysis

Figure 7: Views panel

The Views Panel contains a set of network traffic analyses called “Views”. Each View computes specific metrics, such as bandwidth over time, IP conversations or protocol distributions from either a live or off-line source of network traffic and displays the results in the form of Charts (strip charts, bar charts, grids, etc.).

Main Workspace

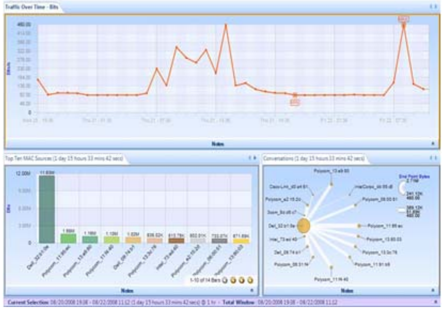


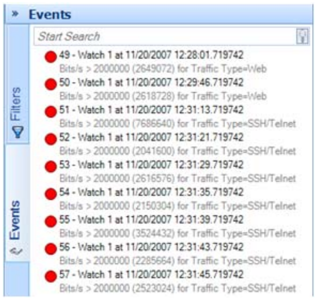
Figure 8 Main Workspace

The *Main Workspace* has tabbed windows that can be one of the following:

- Getting Started Tab
- Applied Views
- Report Preview

The windows can be moved by dragging them and can be closed either by clicking on the icon on the left-hand side of the tab name or by middle-clicking the tab itself.

Events Panel



```
49 - Watch 1 at 11/20/2007 12:28:01.719742
Bits/s > 2000000 (2649072) for Traffic Type=Web
50 - Watch 1 at 11/20/2007 12:29:46.719742
Bits/s > 2000000 (2618728) for Traffic Type=Web
51 - Watch 1 at 11/20/2007 12:31:13.719742
Bits/s > 2000000 (7686640) for Traffic Type=SSH/Telnet
52 - Watch 1 at 11/20/2007 12:31:21.719742
Bits/s > 2000000 (2041600) for Traffic Type=SSH/Telnet
53 - Watch 1 at 11/20/2007 12:31:29.719742
Bits/s > 2000000 (2616576) for Traffic Type=SSH/Telnet
54 - Watch 1 at 11/20/2007 12:31:35.719742
Bits/s > 2000000 (2150304) for Traffic Type=SSH/Telnet
55 - Watch 1 at 11/20/2007 12:31:39.719742
Bits/s > 2000000 (3524432) for Traffic Type=SSH/Telnet
56 - Watch 1 at 11/20/2007 12:31:43.719742
Bits/s > 2000000 (2285664) for Traffic Type=SSH/Telnet
57 - Watch 1 at 11/20/2007 12:31:45.719742
Bits/s > 2000000 (2523024) for Traffic Type=SSH/Telnet
```

Figure 9: Events panel

The *Events Panel* contains entries corresponding to both internal and external events. Internal events are generated by “Watches” and external events are generated by external sources.

Filters panel

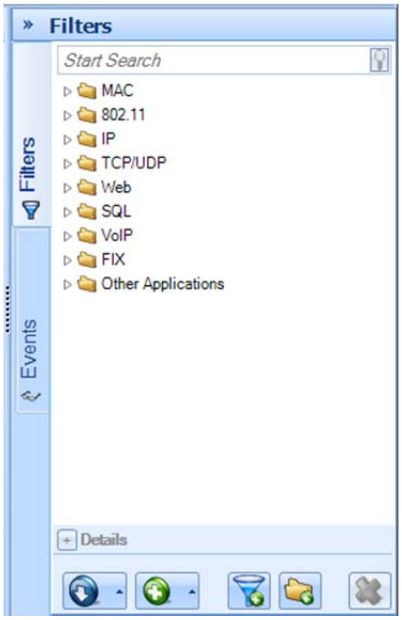
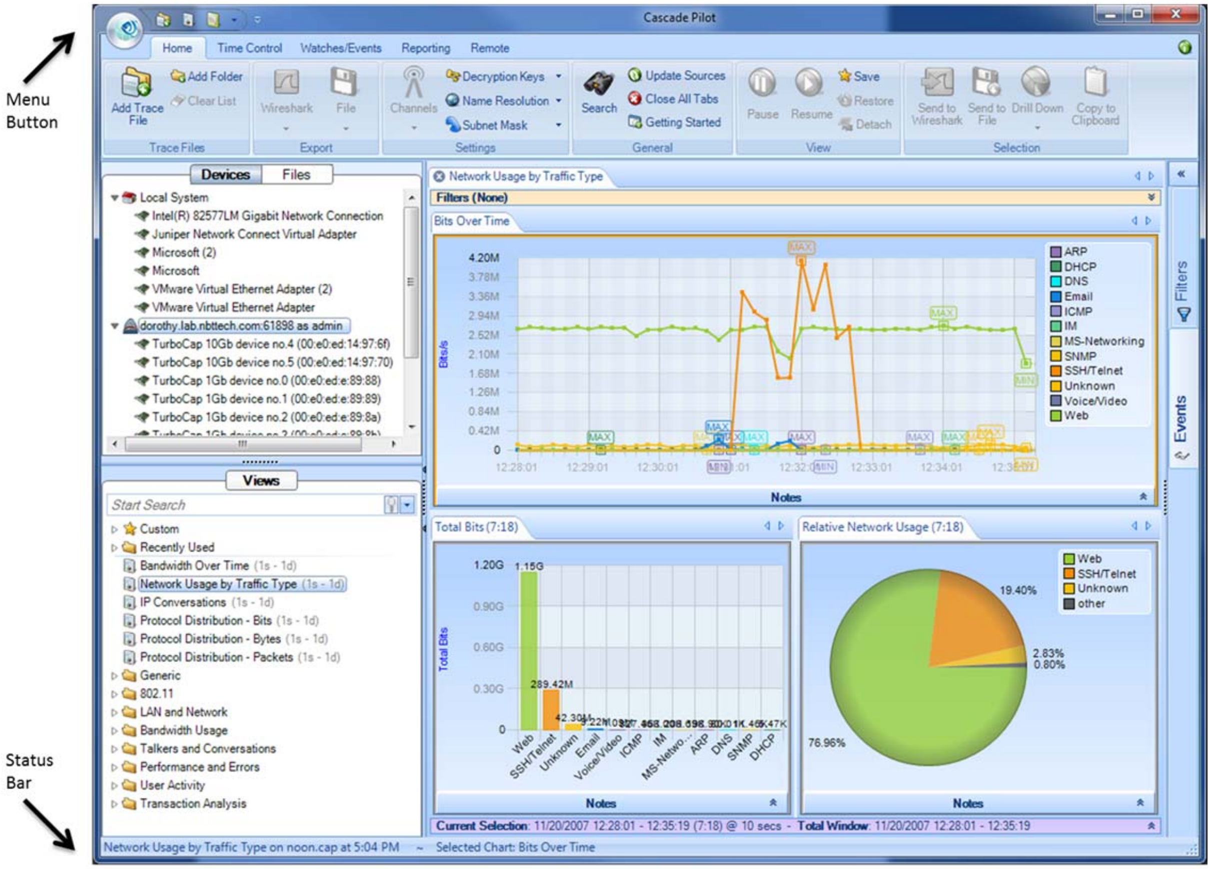


Figure 10: Filter panel

The *Filters Panel* contains all the user filters organized in folders. All existing filters can be copied or moved through folders, edited and removed. New filters can be created from scratch or dragged into the panel from a chart selection.

Menu Button and Status Bar

The user interface also includes a Menu button at the top and a Status bar at the bottom.

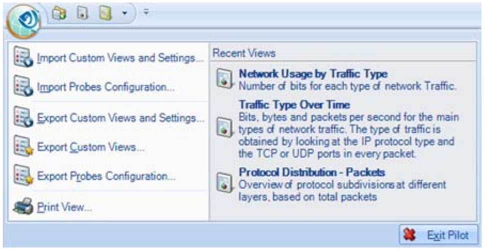


Current Selection: 11/20/2007 12:28:01 - 12:35:19 (7:18) @ 10 secs - Total Window: 11/20/2007 12:28:01 - 12:35:19

Network Usage by Traffic Type on noon.cap at 5:04 PM ~ Selected Chart: Bits Over Time

Figure 11 User Interface Breakdown (Minor)

Menu Button


Import Custom Views and Settings...
Import Probes Configuration...
Export Custom Views and Settings...
Export Custom Views...
Export Probes Configuration...
Print View...
Recent Views
Exit Pilot

Network Usage by Traffic Type
Number of bits for each type of network Traffic.

Traffic Type Over Time
Bits, bytes and packets per second for the main types of network traffic. The type of traffic is obtained by looking at the IP protocol type and the TCP or UDP ports in every packet.

Protocol Distribution - Packets
Overview of protocol subdivisions at different layers, based on total packets

Figure 12 Menu Button

The *Menu Button* has the following components:

Import Custom Views and Settings…

The *Import Custom Views and Settings…* menu option opens a file created by one of the two export menu options described below and applies it to Cascade Pilot. This applies to all settings in the global configuration file, which are enumerated throughout this manual. Briefly, it entails items such as

- Remote Shark appliances and probe groups
- Custom views
- Report settings
- Channel scan sequence
- Decryption keys

Additionally, the custom views from the exported configuration are imported and loaded in the custom views section of the Views panel.

Export Custom Views and Settings…

Prepares a file that can be imported into another instance of Cascade Pilot. This file contains the global configuration file, whose settings are enumerated throughout this manual.

Export Custom Views…

Prepares a file that can be imported into another instance of Cascade Pilot that contains only the custom views.

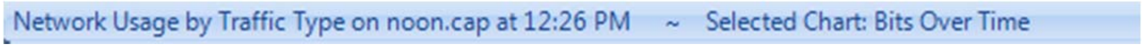
Print View…

Creates a default report from the current view and sends it to the printer. The report is not saved to disk.

Recent Views

Lists the five most recently applied views and their descriptions. Views selected from here are applied to the currently selected device or file, as described below in the section “Applying a View”.

Status Bar



Network Usage by Traffic Type on noon.cap at 12:26 PM ~ Selected Chart: Bits Over Time

Figure 13: Status Bar

The *Status Bar* lists the last operation that was done, such as applying a view to a device. During certain operations, the status bar also includes a graphical horizontal bar on its right hand side that displays the percentage completion of an operation.

Home Ribbon

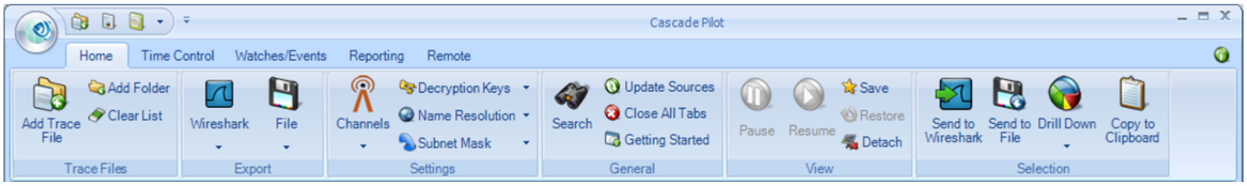


Figure 14: Home Ribbon

The *Home Ribbon* serves as the primary interface to Cascade Pilot. Most operations can be executed via this ribbon. Certain parts of the ribbon are disabled by default. This is to be expected, as will be explained below. The sections of the ribbon are broken down going left-to-right, top-to-bottom. The sections of the ribbon going left-to-right are:

- **Trace Files** – Includes operations such as adding a link to a trace file in the Sources panel.
- **Export** – Used to export traffic sources (either live or off-line) to Wireshark or to a trace file.
- **Settings** – Wireless channel and decryption settings, name resolution, and subnet mask.
- **General** – Miscellaneous actions.
- **View** – Buttons to Pause/Resume live analyses. Saving custom views and detaching from a view.
- **Selection** – Drill-down steps including Send to Wireshark/File.

Note: ***To close any submenu of the ribbon, such as the Decryption Keys or Channel Selector, click the button again or somewhere outside of the submenu. All changes take place immediately hence there is no need for confirmation buttons.***

Trace Files

This section describes the functionality of the Trace Files section of the Home Ribbon.

Note: ***The source and destination of "Add Trace File" and "Add Folder" are local to Cascade Pilot.***

Add Trace File

Icon 1 Add Trace File

The *Add Trace File* button adds a trace file to the Files panel for analysis. This operation adds only a reference to the file, and does not copy the whole file. Thus if the file moves on disk, the reference will be no longer valid.

Add Folder

Icon 2 Add Trace Folder

The *Add Folder* button adds a directory of trace files to the Files panel for analysis. The selected folder is scanned for all supported trace files. Similar to the add trace file operation, this operation adds a reference to the folder and relevant files and does not copy anything on disk.

This operation is not recursive and does not add subfolders.

Clear List

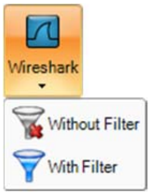
Icon 3 Clear List

The *Clear List* button clears the list of trace files and folders in the Files panel.

Export

The *Export* section lists the functions that export data out of Cascade Pilot either through Wireshark or a PCAP formatted trace file.

Wireshark



Submenu 1 Send to Wireshark

The *Wireshark* button sends traffic from the selected device or file to Wireshark. Note that this is a two click operation.

> *Note:* ***If the source of traffic is on a remote probe, then the traffic (live or off-line) is transmitted over the network to Wireshark running on the Cascade Pilot local system.***

The first click opens a submenu with two options:

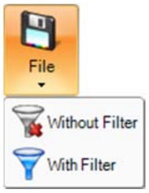
Without Filter

The *Without Filter* menu option sends all traffic from the selected device or trace file to Wireshark. In the case of a device, Wireshark presents, by default, a live scrolling capture. The default behavior can be changed by editing the *Wireshark* preferences.

With Filter

The *With Filter* menu option opens up a filter selection dialog (explained later) to filter the traffic to be sent to Wireshark.

File



Submenu 2 Send to File

The *File* button sends traffic from the selected device or file to a new trace file. Note that this is a two click operation.

Note: ***If the source of traffic is on a remote Shark appliance, then the traffic (live or off-line) is saved in the "My Files" directory on the appliance. If the source of traffic is on the Cascade Pilot local system, then the traffic is saved as a PCAP file located on the local system.***

The first click opens a submenu with two options:

Without Filter

The *Without Filter* button sends all traffic from the selected device or trace file and places it in a trace file of a specified name.

With Filter

The *With Filter* button opens up a filter selection dialog (explained later) to filter the traffic to be sent to a new trace file of a specified name.

After a trace file is created, it is immediately available in the Files panel of the *Device and Files* Panel.

Settings

The *Settings* section contains global settings that are immediately applicable to all open views and their charts.

Channels

Icon 4 Channel Selector

The *Channel Selector* button opens up a submenu that allows for the management of the set and duration of channels to scan or lock. This interface is a large topic and is explained in its own section: Channels Button.

Note: ***This operation applies to only AirPcap adapters installed on the Cascade Pilot host system.***

Decryption Keys

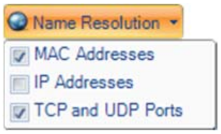
Icon 5 Wireless Decryption Key Manager

The *Wireless Decryption Key Manager* button opens a submenu that allows for the management of the list of keys to decode encrypted wireless traffic. This interface is explained in Decryption.

Note: ***Decryption is available for live AirPcap traffic sources on the local Cascade Pilot and on wireless trace files located on the local system or remote probes.***

Name Resolution

Icon 6 Name Resolution



Submenu 3 Name Resolution

The *Name Resolution* button opens a submenu that allows for the specification of whether certain things should be resolved automatically in a chart. The button gives a submenu with three modal options:

MAC Addresses

When the *Mac Addresses* check box is checked, a passive file-based lookup is done that converts the leftmost 3 bytes of a MAC address to its respective organization (OUI).

IP Address

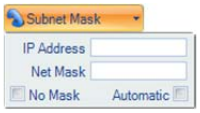
When the *IP Addresses* check box is checked, an active DNS lookup is done to resolve IP Addresses to domain names.

TCP and UDP Ports

When the *TCP and UDP Ports* check box is checked, a passive lookup is done to convert TCP and UDP port numbers into their well-known service names. This is simply a table lookup in a known ports file and does not do any form of service fingerprint matching.

Subnet Mask

Icon 7 Subnet Mask



Submenu 4 Subnet Mask

The *Subnet Mask* button opens a submenu allowing for specification of a global subnet mask to all applicable views and functions as a quick way to discard unwanted traffic. A View's tooltip indicates whether the net mask is applicable to that view.

> *Note:* ***Setting the subnet mask with a remote probe selected causes the subnet mask to be set in the remote probe. In this way, by selecting remote probes one at a time, a unique subnet mask can be set in each remote probe.***

The submenu contains two input boxes and two check boxes:

IP Address

The *IP Address* edit box is used to specify an IPv4 address using dot-decimal notation such as 192.168.0.100. The IP address does not need to be an actual address currently assigned. It is simply guidance for the filter.

Net Mask

The *Net Mask* edit box is used to specify an IPv4 net mask address such as 255.255.255.0. Together, the IP address and subnet mask form a CIDR address block. For instance, in the above example, with a net mask of 255.255.255.0 and an IP Address of 192.168.1.100, the CIDR address block would be 192.168.1.0/24.

No Mask

The *No Mask* check box disables the subnet mask entirely.

Automatic

The *Automatic* check box enables heuristic checks that derive subnet mask values from IP level traffic analysis.

General

The *General* section contains buttons that apply to all devices and tabs.

Search

Icon 8 Search

The *Search* button opens a search dialog window that can be used to find data in the charts. The search context is the labels of the items in a chart that can be selected. For instance, an IP address, MAC address, or hostname can be searched. The Search Dialog is described in its own section.

Update Sources

Icon 9 Update Sources

The *Update Sources* button updates the list of sources for the Devices and Files panels. Please note that a device will not be available immediately after it is plugged in, nor will the device disappear immediately after being unplugged. It takes about 10 seconds before Cascade Pilot recognizes a change of device. Cascade Pilot does not check for new adapters automatically. It checks only when this button is clicked.

Close All Tabs

Icon 10 Close All Tabs

The *Close All Tabs* button closes all open tabs. This applies to the following tabs:

- Views
- Report designer
- Getting started

Getting Started

Figure 15 Getting Started

The *Getting Started* button opens a tab in the main workspace that provides:

- Access to video tutorials

View

The *View* section has buttons used for View management.

Pause

Icon 11 Pause Live Capture

The *Pause Live Capture* button pauses processing on the current View and charts. This button is enabled only in a live capture. The network traffic continues to be processed while the View is paused and is available when the Resume button is clicked.

Resume

Icon 12 Resume Live Capture

The *Resume Live Capture* button resumes “viewing” the live metrics on the current View and charts. This button is enabled only in a “paused” live capture.

Save

Icon 13 Save Custom View

The *Save* button saves the current view as a custom View.

Restore

Icon 14 Restore Default View

The *Restore* button restores default View settings.

Detach

Icon 15 Detach

The *Detach* button detaches the currently selected View from the source, whether the source is live/off-line or local/remote. Once detached, the View is no longer visible in the Cascade Pilot main workspace. The View is still visible in the sources panel, but grayed out.

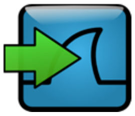
> *Note:* ***For live captures, the system (local or remote) continues to compute the corresponding View metric.***

You can “attach” to the View by right-clicking the View in the sources panel and selecting the Attach submenu item, thereby making the View visible in the Cascade Pilot main workspace.

Selection

Several functions are common among the charts and are enabled only if there is an active selection in a chart. These functions are on the Home ribbon in the Selection group. Each of these functions is also available through the context menu of any chart.

Send to Wireshark



Icon 16 Send to Wireshark

The *Send to Wireshark* button sends traffic from the current selection to Wireshark by spawning a new instance of Wireshark and delivering the selected packets to Wireshark.

> *Note:* ***If the source of traffic is on a remote probe, then the traffic (live or off-line) is transmitted over the network to Wireshark running on the Cascade Pilot local system.***

Send to Trace File

Icon 17 Send to File

The *Send to File* button sends traffic from the current selection and stores it as a trace file. This is useful for storing a subset of the original capture. If the traffic was encrypted and is being properly decrypted at the time, then the trace file stores the decrypted traffic.

> *Note:* ***If the source of traffic is on a remote probe, then the traffic (live or off-line) is saved in the “My Files” directory on the remote probe. If the source of traffic is local to Cascade Pilot, then the traffic is saved as a PCAP file located on the local system.***

Drill Down

Icon 18 Drill Down

The *Drill Down* button applies a View to the current selection in a chart. This is an important and powerful feature of Cascade Pilot and is explained in its own section. See the chapter on Drill Down.

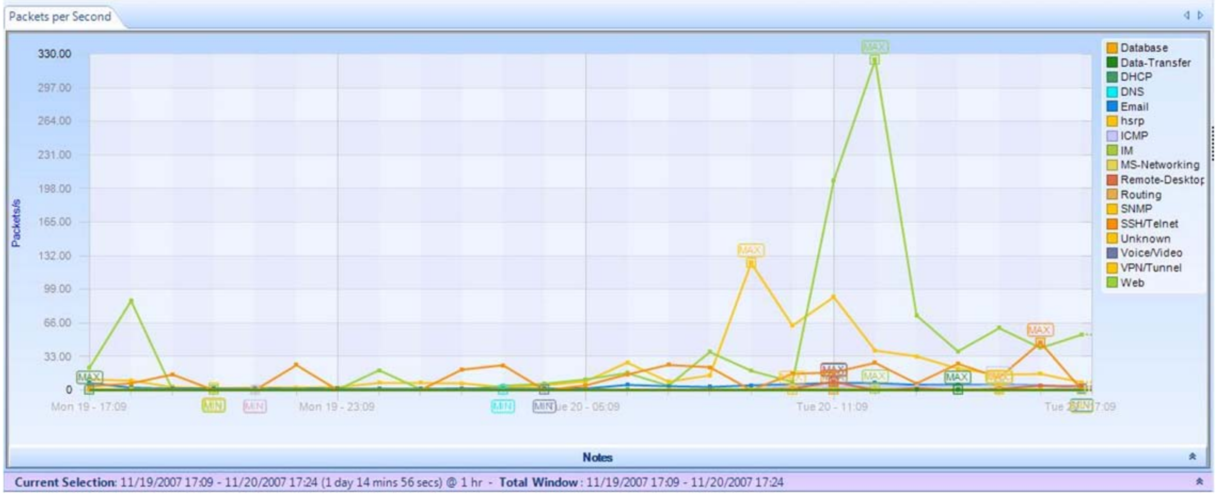
Copy to Clipboard

Icon 19 a

The *Copy to Clipboard* button copies a textual representation of the chart information from the current selection to the system clipboard to enable exporting to another application.

Time Control Ribbon

The Time Control feature of Cascade Pilot allows the user to go “back in time” over a View that has been computed over days, weeks, or months. It applies to Views computed over live and off-line sources. Based on the View and the selected time interval, subsampling and aggregation techniques are used to optimize the granularity of the visual presentation of the View metrics.



Current Selection: 11/19/2007 17:09 - 11/20/2007 17:24 (1 day 14 mins 56 secs) @ 1 hr - **Total Window**: 11/19/2007 17:09 - 11/20/2007 17:24

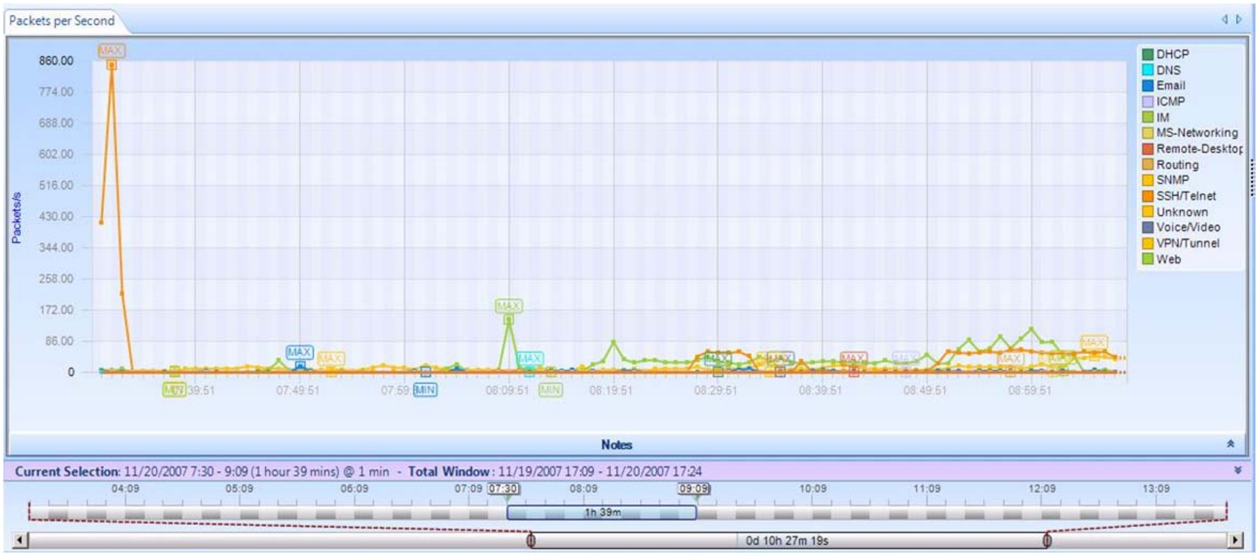
Figure 16 Traffic Type Over Time Showing Time Selection Windows

Figure 16 shows the Traffic Type Over Time View applied to a trace file. The purple bar just below the strip chart is called *Time Controller*. It has two fields, *Current Selection* and the *Total Window*.

The *Total Window* indicates the beginning and end time and date of the trace file.

The *Current Selection* is the interval of time displayed in the Charts above the *Time Controller*. The *Time Controller* shows the following information about the Current Selection: start date, start time, end date, end time, duration (in parenthesis) and sampling time (after the @). The Current Selection can be adjusted as explained later in this chapter, so that the temporal interval can be shorter than the Time Window. Sometimes the captured interval is too large to be displayed in a single Strip Chart at the sample rate indicated in the View metrics (e.g. several days of traffic with 1-second sample rate). In these cases Pilot automatically aggregates displayed data, subsampling the trace file and displaying traffic with a lower granularity. Higher resolution is still available when you zoom in to analyze shorter time intervals. The Cascade Pilot analysis engine (the local or remote Shark appliance) automatically selects the best level of subsampling based on the duration of the Current Selection.

Figure 17 shows the time control “zoomed-in” on the View so that the Current Selection interval is shorter and thus the sampling rate is smaller. The change in resolution is handled automatically in Cascade Pilot, thereby making it very easy to move around and to zoom in and out of very long-duration trace files and live captures.



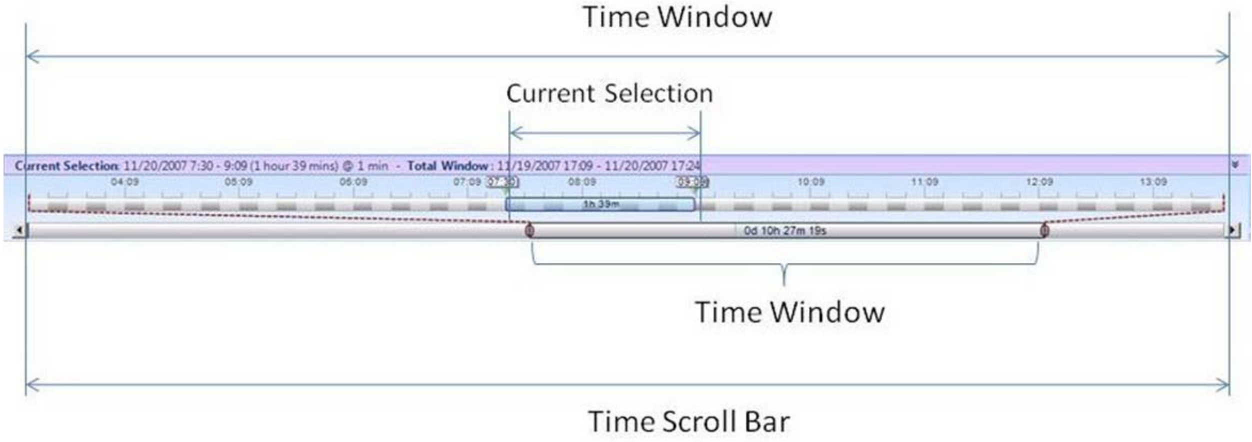
Current Selection: 11/20/2007 7:30 - 9:09 (1 hour 39 mins) @ 1 min - Total Window: 11/19/2007 17:09 - 11/20/2007 17:24

Figure 17 Traffic Type Over Time with Multi-Level Zoom Selection

Figure 18 shows the Time Control Bars in more detail. The bottom bar is called the *Time Scroll Bar* and it represents the entire trace file or live capture. The *Time Window* depicts an interval of time within the overall trace file or live capture. The Time Window element within the Time Scroll Bar can be resized and moved throughout the file. It affects only what is visible on the upper bar. The upper bar represents a magnified view of the Time Window and any change to the size and position of the *Current Selection* on it affects what is visible in the View Charts. The *Current Selection* is the time interval within the trace file or live capture that is displayed in the View.

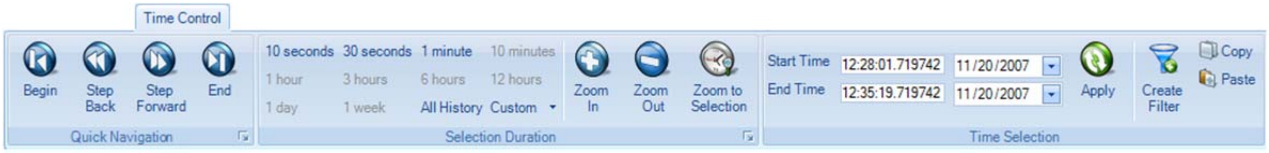
You can change the position and size of the two bars as follows:

- Using buttons within the Time Control Ribbon to move the Current Selection and change the Current Selection duration.
- Dragging the Current Selection element or its endpoints.
- Clicking and dragging just above the expanded Time Window to create a new Current Selection.
- Double-clicking the Current Selection to expand the Current Selection to the complete View history. (Double-clicking again returns the Current Selection to its previous location.)



Current Selection: 11/20/2007 7:30 - 9:09 (1 hour 39 mins) @ 1 min - Total Window: 11/19/2007 17:09 - 11/20/2007 17:24

Figure 18 Time Control Bars



Start Time 12:28:01.719742 11/20/2007

End Time 12:35:19.719742 11/20/2007

Figure 19 Time Control Ribbon

The Time Control feature of Cascade Pilot allows the user to go “back in time” over a View that has been computed over days, weeks, or months. The Time Control Ribbon provides additional mechanisms for moving through a long-duration View. There are three sections within the Time Control Ribbon: Quick Navigation, Selection Duration, and Time Selection. These are described next.

Quick Navigation

Begin

The *Begin* button allows a user to move the Current Selection interval to the beginning of the View (back-in-time).

Step Back

The Step Back button allows the user to move the Current Selection interval one step back in time where the size of the step is equal to the length of the Current Selection interval.

Step Forward

The Step Forward button allows the user to move the Current Selection interval one step forward in time where the size of the step is equal to the length of the Current Selection interval.

End

The End button allows the user to move the Current Selection interval to the end of the current View.

Selection Duration

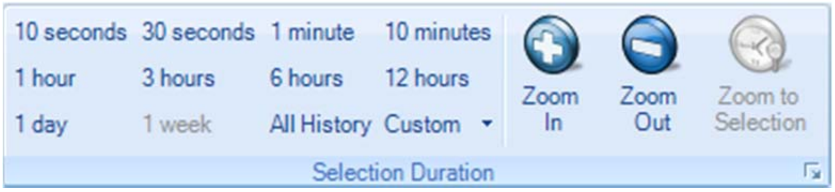


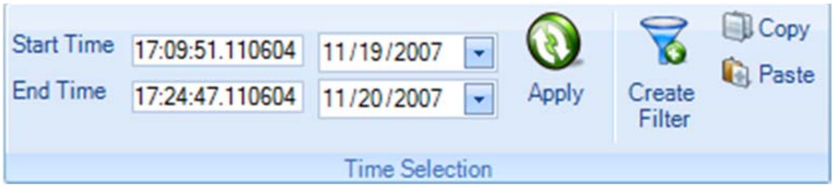
Figure 20 Selection Duration Section of the Time Control Ribbon

The Selection Duration section of the Time Control ribbon provides a number of alternatives for setting the length of the Current Selection interval. Recall that the Current Selection interval corresponds to the portion of the View metric that is displayed in the Charts that make up a View. For example, if the Chart is a strip chart, then the duration of the visible portion of the strip chart is precisely the Current Selection interval. For other charts, the visible portion of the Chart shows the View metric computed for the span of time equal to the Current Selection interval. For example, if the Chart is a conversation ring, then the conversation ring shows the host conversations that have taken place during the Current Selection interval.

The Selection Duration section contains some fixed durations to choose from, such as 10 seconds, 10 minutes, All History, etc. For a trace file, the All History selection corresponds to the duration of the entire trace file. For a live capture, All History ends at the present time and begins either at the start of the capture or at an amount of time equal to the Data Retention Time of the capture, whichever is smaller. There is also a Custom setting option allowing the user to pick an arbitrary time interval.

Finally, there are Zoom In, Zoom Out, and Zoom to Selection options. Clicking the Zoom In button reduces the Current Selection interval by 66%. Clicking the Zoom Out button increases the duration of the Selection interval to 150% of its current duration. If a time duration selection is made in a Strip Chart, the Zoom to Selection button changes the Current Selection interval to the selection made on the Strip Chart.

Time Selection


Start Time 17:09:51.110604 11/19/2007

End Time 17:24:47.110604 11/20/2007

Figure 21 Time Selection Section of the Time Control Ribbon

The *Time Selection* section of the Time Control ribbon allows the user to pick the absolute location and duration of the Current Selection interval within the current View (either live or off-line) by setting the *Start Time*, the *End Time*, and then clicking *Apply*.

Create Filter – When the user clicks on the Create Filter button, a new Filter is created that will filter out all packets that do not fall within the Current Selection interval. This filter can be used when applying a new View to a source and is very useful for comparing two different Views with respect to the same time interval. For example, one can compare Bandwidth Over Time and IP Conversations during the same time interval to see which hosts were contributing to the spike in bandwidth.

Copy – Copies the Current Selection interval to the clipboard.

Paste – Changes to Current Selection interval to the interval contain on the clipboard. (The destination Chart must be selected to paste an interval on it.)

Watches and Events Ribbon

A Watch consists of a Trigger Condition and one of more associated Actions. Every time the Trigger Condition is satisfied, then the associated Actions are "executed".

A Watch is always associated with a particular Chart contained in a View and the trigger condition is based on the metric computed in the Chart. The View itself is applied to a source, which can be either live or off-line, and can be either on the local system or a remote Shark appliance.

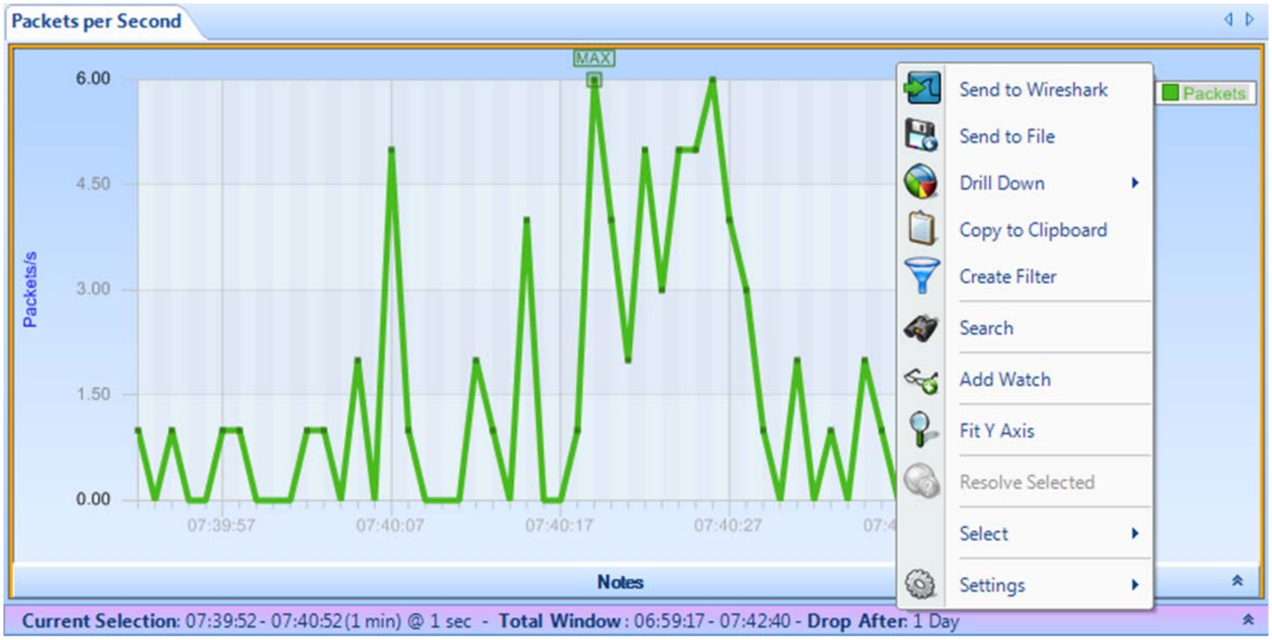
> *Note:* ***The Trigger Condition is checked at the underlying Sampling Time intervals, even if the chart is showing sub-sampled or aggregated data for larger intervals.***

For example, suppose that the View is Bandwidth Over Time with a Sampling Time of one second and the selected Chart within the View is Packet Bandwidth Over Time. This means that for every second, packets-per-second is computed over the packets that arrived during the previous Sampling Time – this is the quantity shown in the Chart. If a Watch were associated with this Chart, then the Trigger Condition would be checked every second using the computed packets-per-second.

The following sections show how Watches are created for Strip Charts and Bar Charts.

> *Note:* ***Watches can be applied to only Strip Charts and Single Bar Charts.***

Creating Watches on Strip Charts and Bar Charts



Current Selection: 07:39:52 - 07:40:52 (1 min) @ 1 sec - Total Window: 06:59:17 - 07:42:40 - Drop After: 1 Day

Figure 22 Strip Chart with Context Menu

Figure 22 shows the context menu associated with the Packets per Second strip chart within the Bandwidth Over Time View. Right-clicking in the Packets per Second chart displays the context menu. The *Add Watch* submenu item brings up the Watch Editor panel (Figure 26), which can create a Watch on the metric (Packets per Second) associated with the selected chart.

The user sets up the Watch by completing the necessary items in the Watch Editor panel (see Figure 26). Clicking “OK” in the Watch Editor panel causes the Watch to be associated with the View. The Watch appears in the Sources panel under the View.

Watch in Sources Panel

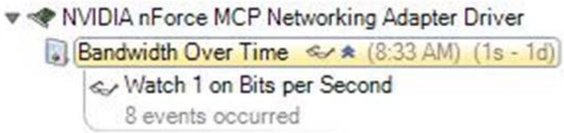

NVIDIA nForce MCP Networking Adapter Driver
Bandwidth Over Time (8:33 AM) (1s - 1d)
Watch 1 on Bits per Second
8 events occurred

Figure 23 Watch in Device Sources Panel

The Watch appears below its associated View in the sources panel. In this case the View has been applied to a live source. Watches can also be applied to trace files. The small arrows beside the watch icon are used to hide or show the list of watches.

Context Menu for Watch Applied to a Live Source

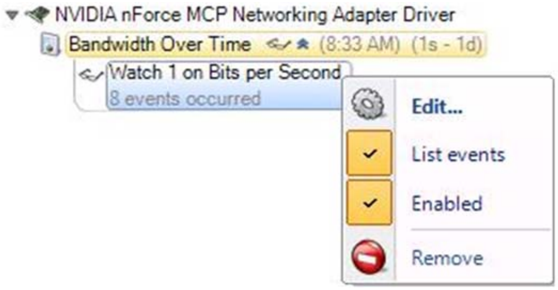

NVIDIA nForce MCP Networking Adapter Driver
Bandwidth Over Time (8:33 AM) (1s - 1d)
Watch 1 on Bits per Second
8 events occurred
Edit...
List events
Enabled
Remove

Figure 24:Context Menu For Watch Applied to Live Source

The context menu for a Watch associated with a live source contains the following menu items:

- *Edit*. This menu item brings up the Watch Editor Panel
- *List events*. Lists/Does Not List the events associated with the Watch in the Events panel
- *Enabled*. Enables/Disables the Watch
- *Remove*. The Watch is removed and all of the associated Events are removed from the Events panel

Context Menu for Watch Applied to a Trace File

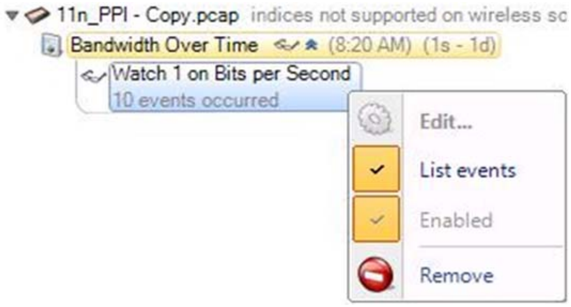
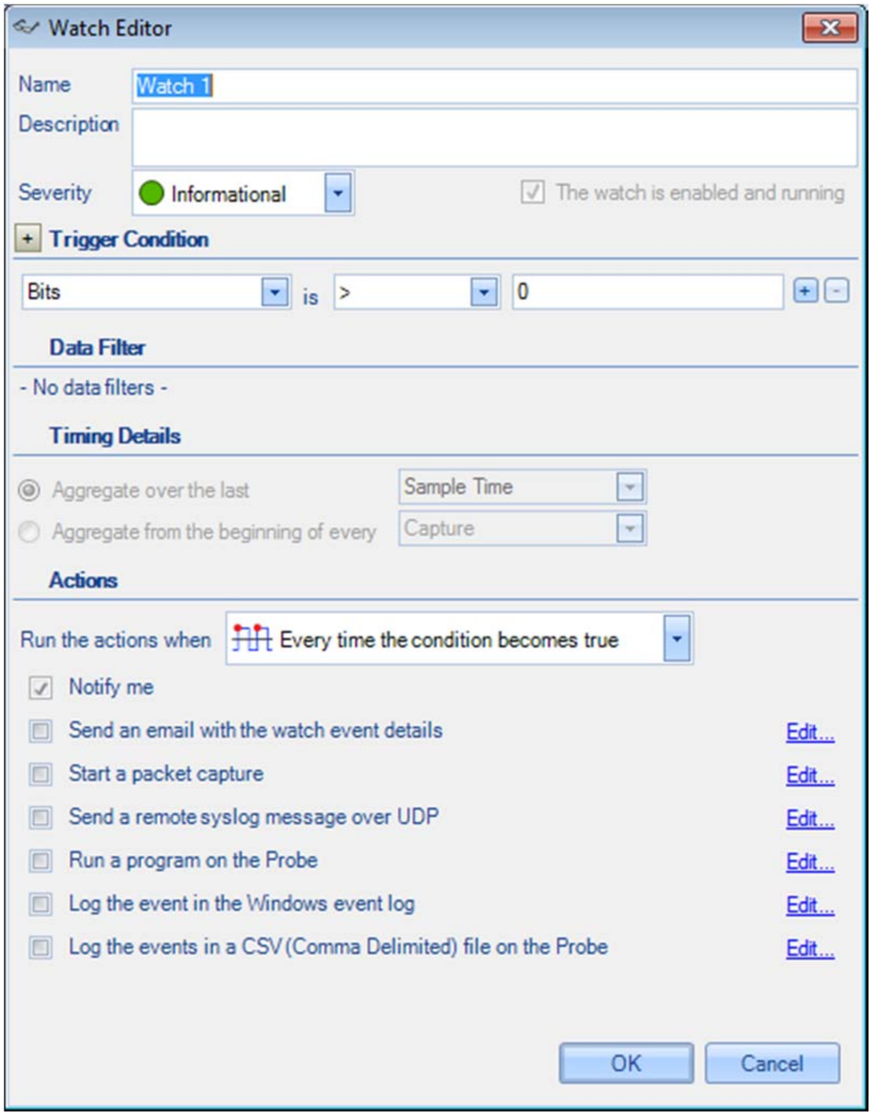

11n_PPI - Copy.pcap indices not supported on wireless sc
Bandwidth Over Time (8:20 AM) (1s - 1d)
Watch 1 on Bits per Second
10 events occurred
Edit...
List events
Enabled
Remove

Figure 25:Context Menu for Watch Applied to a Trace File

A Watch applied to a trace file cannot be edited, enabled, or disabled.

The Watch Editor

Figure 26 shows the Watch Editor. The following section describes the fields in the Watch Editor panel.



Watch Editor

Name: Watch 1

Description:

Severity: ● Informational

☑ The watch is enabled and running

Trigger Condition

Bits is > 0

Data Filter

- No data filters -

Timing Details

● Aggregate over the last: Sample Time

○ Aggregate from the beginning of every: Capture

Actions

Run the actions when: Every time the condition becomes true

☑ Notify me

☐ Send an email with the watch event details

☐ Start a packet capture

☐ Send a remote syslog message over UDP

☐ Run a program on the Probe

☐ Log the event in the Windows event log

☐ Log the events in a CSV (Comma Delimited) file on the Probe

Figure 26 Watch Editor Panel

Name and Description

The *Name* field is used to assign a name to the Watch and the *Description* field is used to provide specific details regarding the Watch.

Severity

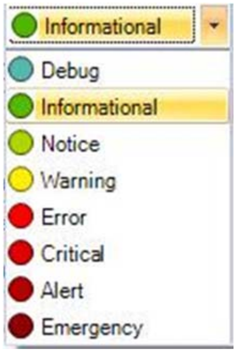


Figure 27 Watch Severity

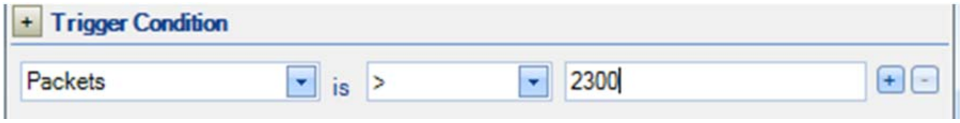
The *Severity* field contains a drop-down list (see Figure 27) with a number of different “severity” levels. These levels are mainly used to distinguish events (actions) from one another and can be used when searching for specific events.

Enabled

When *The Watch is Enabled and Running* checkbox is checked, the Watch, once it is created, is immediately active. Otherwise, if the box is not checked, the Watch can be created but the Trigger Condition is not activated until the Watch is enabled.

Trigger Conditions

The Trigger Condition elements are shown in Figure 28. Together they represent a Boolean condition; that is, an expression that evaluates to either True or False.



Packets is > 2300

Figure 28 Trigger Condition

The left-most box contains the value to be tested. Recall that in Figure 22 the Packets (per second) strip chart was selected when the New Watch submenu item was selected. This accounts for the Packets value in the left-most box. The middle box is a drop-down list that contains relational operators that can be selected (see Figure 29 for the list of operators.

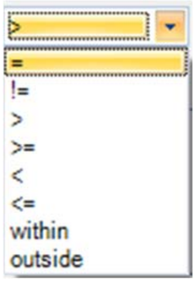
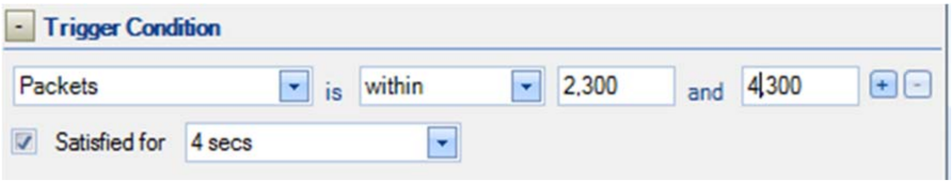


Figure 29 Relational Operators

Finally, there is the right-most box, which contains the comparison value. The Trigger Condition in the example shown in Figure 28 is true whenever Packets is greater than 2,300.



⊟ Trigger Condition

Packets is within 2,300 and 4300 ⊞ ⊟

☑ Satisfied for 4 secs

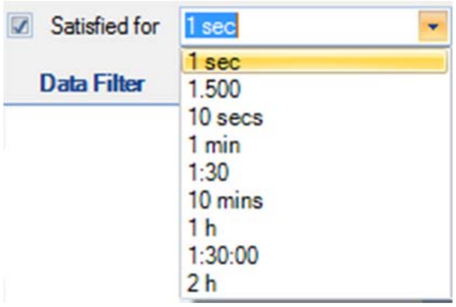
Figure 30 Trigger Condition Expanded

Figure 30 shows the “within” condition and what is shown when the Trigger Condition is expanded. The “within” condition requires two values, namely, lower and upper limits in that order. In this case, the Trigger Condition is True whenever the value (Packets per second) is less than or equal to the upper limit and greater than or equal to the lower limit. Similarly, the “outside” condition is specified with lower and upper limits and is true when the value falls out of the specified range.

Expanded Trigger Condition

Expanding the Trigger Condition reveals the “Satisfied for” check box. When the box is checked, then the Trigger Condition becomes the conjunction of the underlying relational expression and the “Satisfied for” condition. In other words, both must be true for the Trigger Condition to be true. In the above example (Figure 30), the ”Satisfied for” condition is true whenever the underlying relational expression is true for 4 consecutive seconds. If the Sampling Time is 1 second, then the Trigger Condition is true if the underlying relational expression (Packets is within 2,300 and 4,300 for 4 consecutive seconds).

The Expanded Trigger Condition is very useful when the user only wants to react to a condition if that condition is true for a minimum amount of time, in this case 4 seconds.



☑ Satisfied for 1 sec

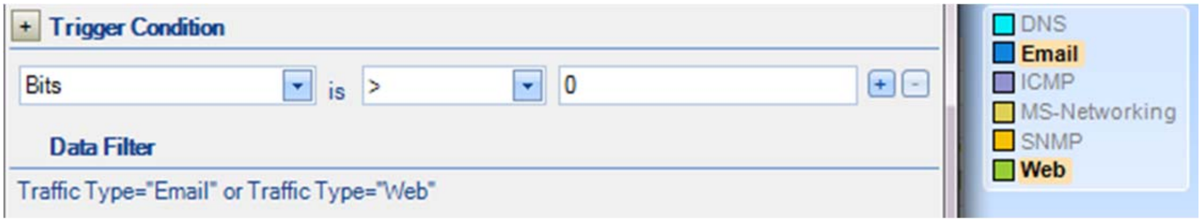
Figure 31 Sample Choices for Satisfied for

The figure above shows the contents of the drop-down box for the choice of durations for “Satisfied for.” The duration can be selected from this list or created from scratch using the formats shown in the list.

Multi-line Strip Charts

In the case of a single line strip chart as in Figure 22, the Trigger Condition is evaluated every Sample Time on the single value computed at each sample point. In the case of multi-line strip charts where multiple values are computed at each Sample Time, there are two cases: 1. Multiple characteristics are computed for each packet, or 2. The packets are partitioned into multiple categories and a single metric is computed for the packets in each category.

Single value, multiple packet types



Trigger Condition

Bits is > 0

Data Filter

Traffic Type="Email" or Traffic Type="Web"

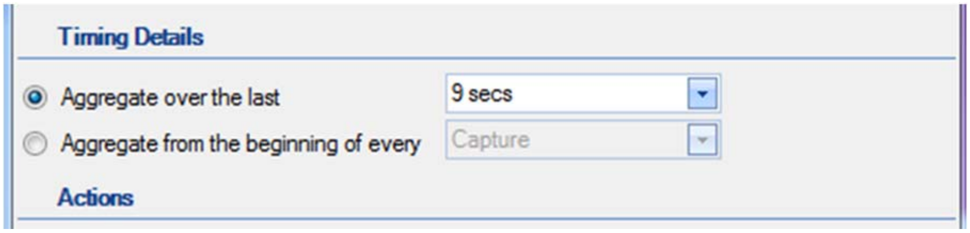
Figure 32 Multi-line Strip Chart with Filtering

Figure 32 depicts the case where the multi-line strip chart shows Traffic Type Over Time. Each packet is examined and partitioned according to its packet type and the bandwidth per second is computed for each packet type. In general, a Watch on this strip chart would check the Trigger Condition for each traffic type for each Sample Time and generate an event for each traffic type for which the Trigger Condition is met. This means that there could be as many events generated at each Sample Time as there are traffic types. If a line selection is made before the Watch is created, the Data Filter field will show the set of lines for which the packet bandwidth will be calculated. Figure 32 shows that two lines, Email and Web, have been selected. The Watch Editor acknowledges the line selection under the Data Filter section and automatically appears.

Multiple values, single packet type

Figure 34 shows another type of multi-line strip chart. This example comes from the Frame Size Over Time View in the Generic folder. In this case, the average, maximum, and minimum frame sizes are computed for *each* packet – there are three different values associated with each packet and the lines in the strip chart represent these values. Now different lines are represented as different "values" in the left-hand side of the Trigger Condition relational expression.

Timing Details for Bar Charts



Timing Details

● Aggregate over the last 9 secs

○ Aggregate from the beginning of every Capture

Actions

Figure 33 Timing Details

The section called "Timing Details" applies to aggregating charts such as Bar Charts. Strip Charts are not aggregating charts and therefore the Timing Details section is grayed out for strip charts.

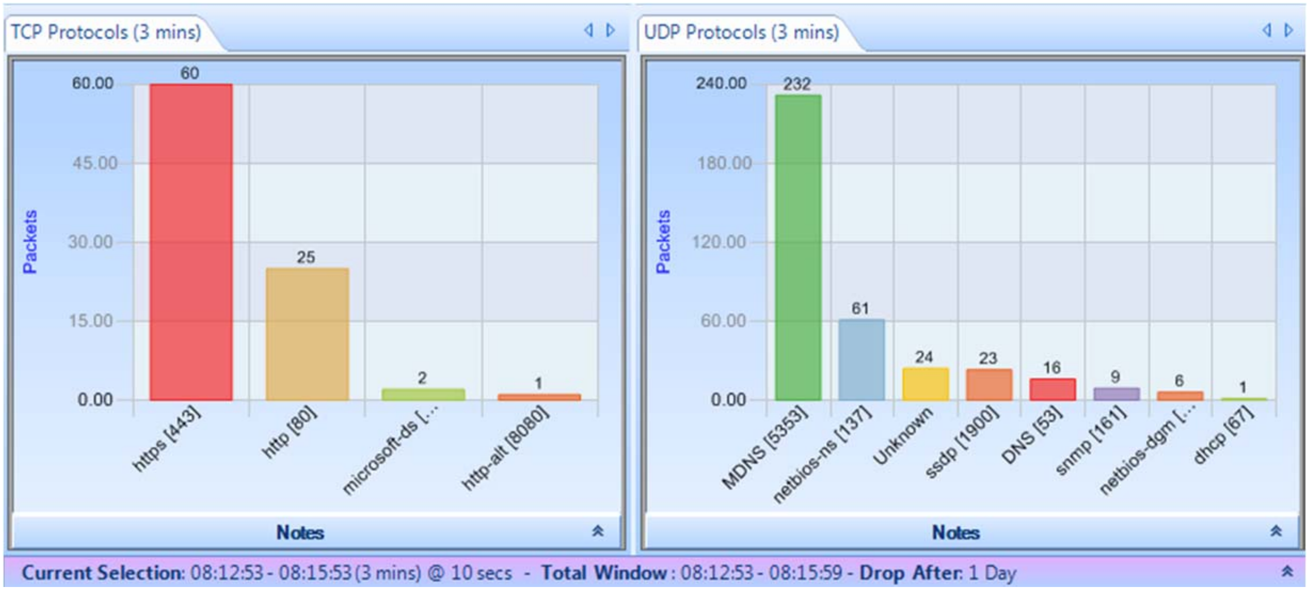


Figure 34 Aggregating Chart

The Current Selection interval in Figure 34 is equal to 3 minutes. The bar chart on the left partitions the incoming packets according to the TCP protocol and counts the number of packets for each protocol. For example, in the left-most chart, there are 60 packets carrying the https protocol. But there is more to the story. The Current Selection interval is 3 minutes, which means that the bars are the sums seen over a 3-minute interval. In the case of the above chart, the interval is from 08:12:53 to 08:15:53. The aggregation interval for the bar chart is, for convenience, also show in the chart’s tab.

Note: ***The Timing Details sets an aggregation interval for the Watch that is independent of the aggregation associated with the Current Selection interval.***

In setting up a Watch for an aggregating chart it is important to specify the interval over which the aggregation takes place. There are two radio buttons in the Timing Details section, and one or the other must be selected. The first one specifies the aggregation back in time from the current time. At each Sampling Time, the value of each bar is determined by aggregating over the aggregation interval specified. The aggregation intervals are overlapping.

The second radio button is for specifying non-overlapping aggregation intervals. For example, suppose a user wanted to aggregate the total packets over every hour for each TCP protocol. For each hour we would begin a new aggregation interval. This means that for each Sample Time, the aggregation interval extends back to the start of the current hour. Therefore the aggregation interval grows until it reaches one hour and then starts again.

In the bar chart example, the aggregation function is SUM. A number of other aggregation functions are used throughout Cascade Pilot, namely, MAX, MIN, AVG, TIME AVG, and others.

Actions

The Trigger Condition is an expression that is evaluated at each Sample Time. Even when the trigger is true, you may want some additional context before you execute the corresponding actions. For example, you may want to execute only the associated actions when the Trigger Condition makes a transition from False to True on successive Sample Times. These additional conditions are called *Transition Conditions*.

Transition Conditions

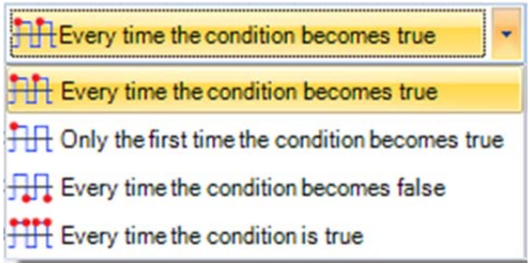

Every time the condition becomes true
Every time the condition becomes true
Only the first time the condition becomes true
Every time the condition becomes false
Every time the condition is true

Figure 35 Transition Condition List

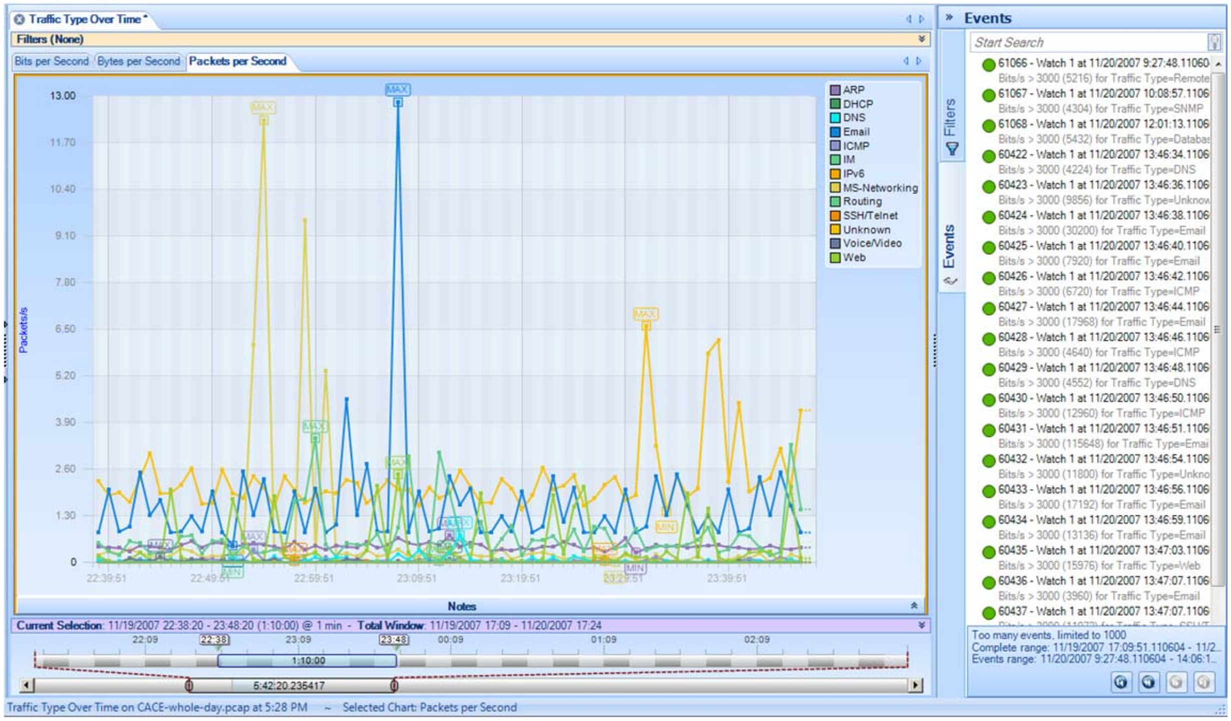
In Figure 35 we show the contents of the drop-down box. These are the Transition Conditions that are used, in conjunction with the Trigger Condition, to determine when the associated actions are to be executed. The icons are suggesting: leading edge, every time; leading edge, only once; trailing edge, every time; and every time.

- *Every time the condition becomes true.* Actions are executed whenever the Trigger Condition is true on the current Sample Time and was False on the previous Sample Time. The Actions are also executed if the Trigger Condition is True when the Watch is activated (i.e., before there is any history for the Watch).
- *Only the first time the condition becomes true*. Actions are executed the first time the Trigger Condition is true on a Sample Time and was False on the previous Sample Point. The Actions are also executed if the Trigger Condition is True when the Watch is activated (i.e., before there is any history for the Watch). The Actions are executed at most one time.
- *Every time the condition becomes false*. Actions are executed whenever the Trigger Condition is false on the current Sample Time and was true on the previous Sample Time. The Actions are also executed if the Trigger Condition is true when the Watch is activated (i.e., before there is any history for the Watch).
- *Every time the condition is true*. Actions are executed whenever the Trigger Condition is true.

Note: ***A Trigger Condition, along with its associated transition condition, is based on a View associated with the local system or with a remote Shark appliance. Accordingly, the actions associated with the trigger condition are initiated by the local system or the remote Shark appliance***

Notify Me

The Notify Me action is always executed and makes a record of the event on the strip chart and in the Events panel.



Current Selection: 11/19/2007 22:38:20 - 23:48:20 (1:10:00) @ 1 min - Total Window: 11/19/2007 17:09 - 11/20/2007 17:24

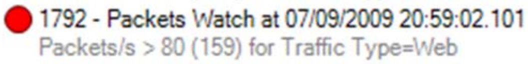
Traffic Type Over Time on CACE-whole-day.pcap at 5:28 PM ~ Selected Chart: Packets per Second

```
61066 - Watch 1 at 11/20/2007 9:27:48.11060
Bits/s > 3000 (5216) for Traffic Type=Remote
61067 - Watch 1 at 11/20/2007 10:08:57.1106
Bits/s > 3000 (4304) for Traffic Type=SNMP
61068 - Watch 1 at 11/20/2007 12:01:13.1106
Bits/s > 3000 (5432) for Traffic Type=Databas
60422 - Watch 1 at 11/20/2007 13:46:34.1106
Bits/s > 3000 (4224) for Traffic Type=DNS
60423 - Watch 1 at 11/20/2007 13:46:36.1106
Bits/s > 3000 (9856) for Traffic Type=Unknow
60424 - Watch 1 at 11/20/2007 13:46:38.1106
Bits/s > 3000 (30200) for Traffic Type=Email
60425 - Watch 1 at 11/20/2007 13:46:40.1106
Bits/s > 3000 (7920) for Traffic Type=Email
60426 - Watch 1 at 11/20/2007 13:46:42.1106
Bits/s > 3000 (6720) for Traffic Type=ICMP
60427 - Watch 1 at 11/20/2007 13:46:44.1106
Bits/s > 3000 (17968) for Traffic Type=Email
60428 - Watch 1 at 11/20/2007 13:46:46.1106
Bits/s > 3000 (4640) for Traffic Type=ICMP
60429 - Watch 1 at 11/20/2007 13:46:48.1106
Bits/s > 3000 (4552) for Traffic Type=DNS
60430 - Watch 1 at 11/20/2007 13:46:50.1106
Bits/s > 3000 (12960) for Traffic Type=ICMP
60431 - Watch 1 at 11/20/2007 13:46:51.1106
Bits/s > 3000 (115648) for Traffic Type=Emai
60432 - Watch 1 at 11/20/2007 13:46:54.1106
Bits/s > 3000 (11800) for Traffic Type=Unkno
60433 - Watch 1 at 11/20/2007 13:46:56.1106
Bits/s > 3000 (17192) for Traffic Type=Email
60434 - Watch 1 at 11/20/2007 13:46:59.1106
Bits/s > 3000 (13136) for Traffic Type=Email
60435 - Watch 1 at 11/20/2007 13:47:03.1106
Bits/s > 3000 (15976) for Traffic Type=Web
60436 - Watch 1 at 11/20/2007 13:47:07.1106
Bits/s > 3000 (3960) for Traffic Type=Email
60437 - Watch 1 at 11/20/2007 13:47:07.1106
```

Too many events, limited to 1000
Complete range: 11/19/2007 17:09:51.110604 - 11/2...
Events range: 11/20/2007 9:27:48.110604 - 14:06:1...

Figure 36 Event Notifications

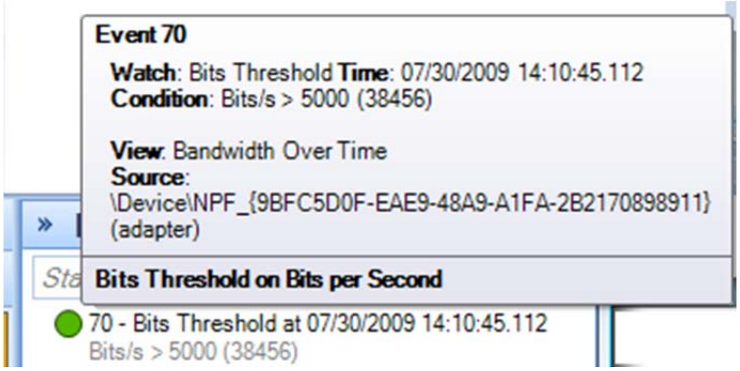
Figure 36 shows how the event notifications appear on a strip chart and in the Events panel. Notice that the event selected in the Events panel is highlighted in the strip chart and also on the Time Window. If a vertical line representing an event on the strip chart is selected, the corresponding event is shown as selected in the Events panel and in the Time Window. Moreover, if the event line is selected in the Time Window, it is shown as selected in both the Events panel and the strip chart.



● 1792 - Packets Watch at 07/09/2009 20:59:02.101
Packets/s > 80 (159) for Traffic Type=Web

Figure 37 Event Structure

The Event Structure begins with a circle with the color corresponding to the color of the Watch Severity. The following number is the event Unique ID followed by the name of the event. This is followed by the date and time at which the event occurred. The second line begins with the Trigger Condition and the value, in parentheses, that caused the Trigger Condition to be true followed by the line that was selected in the strip chart when the Watch was defined.



Event 70

Watch: Bits Threshold **Time**: 07/30/2009 14:10:45.112
Condition: Bits/s > 5000 (38456)

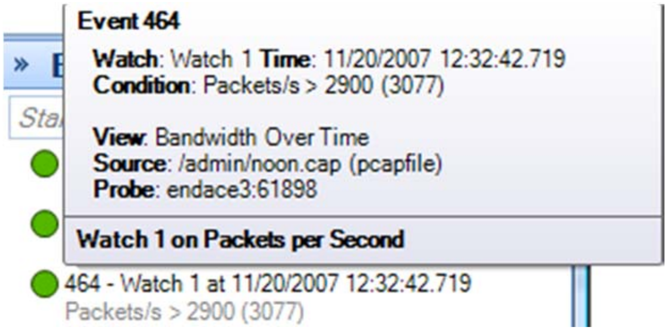
View: Bandwidth Over Time
Source:
\Device\NPF_{9BFC5D0F-EAE9-48A9-A1FA-2B2170898911}
(adapter)

Bits Threshold on Bits per Second

70 - Bits Threshold at 07/30/2009 14:10:45.112
Bits/s > 5000 (38456)

Tooltip 1 Tooltip for an Event

Moving the mouse over a severities icon in the Events panel displays a tooltip for the selected event. The tooltip contains the details regarding the Event.



Event 464

Watch: Watch 1 **Time**: 11/20/2007 12:32:42.719
Condition: Packets/s > 2900 (3077)

View: Bandwidth Over Time
Source: /admin/noon.cap (pcapfile)
Probe: endace3:61898

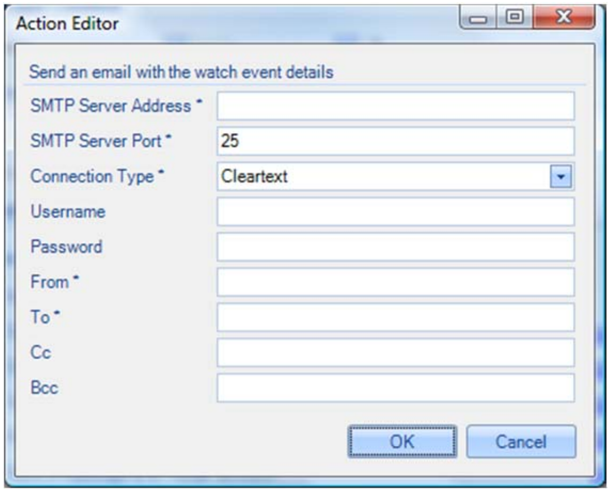
Watch 1 on Packets per Second

464 - Watch 1 at 11/20/2007 12:32:42.719
Packets/s > 2900 (3077)

Tooltip 2 Tooltip for a Remote Event

The tooltip for a Remote event also identifies the "name" of the Shark appliance and port number.

Send an email with the watch event details



Action Editor

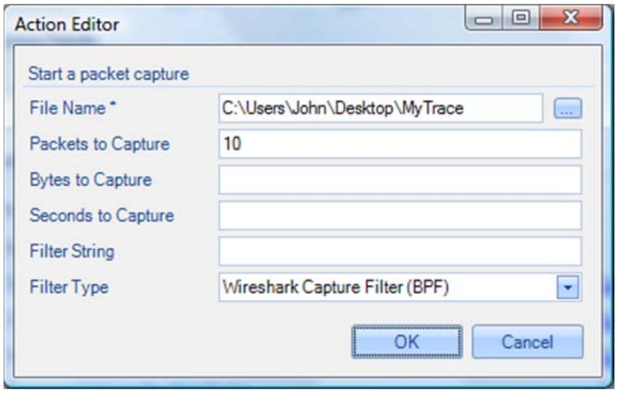
Send an email with the watch event details

SMTP Server Address *	
SMTP Server Port *	25
Connection Type *	Cleartext
Username	
Password	
From *	
To *	
Cc	
Bcc	

Figure 38 Email Action

If "Send email with the Watch event details" is selected, the Send Email Parameters Editor appears. This should be filled in with the mail server information, account, and destination email addresses. When the Action occurs, email is sent to the destination email addresses with the Event information.

Start a packet capture



Start a packet capture

File Name * C:\Users\John\Desktop\MyTrace

Packets to Capture 10

Bytes to Capture

Seconds to Capture

Filter String

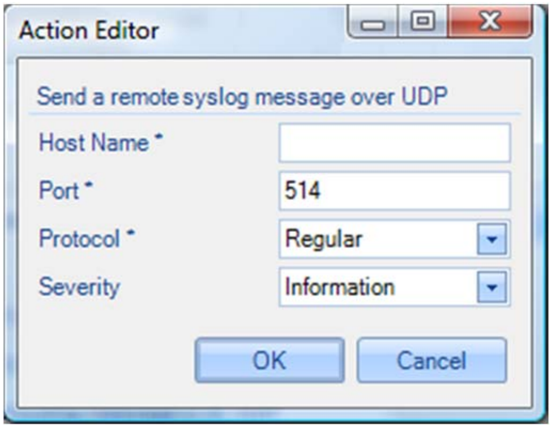
Filter Type Wireshark Capture Filter (BPF)

Figure 39 Capture Packets Panel

When “Start a packet capture” is selected, the panel in Figure 39 appears. The File name is a mandatory field and specifies the absolute path name of the capture file to be created. The “Packets to Capture,” “Bytes to Capture,” and “Seconds to Capture” are stopping conditions, whichever comes first. An optional Filter String can be specified along with the Filter Type. When the event occurs, a packet capture is initiated and terminated according to the stopping conditions.

> *Note:* ***If the Watch is associated with a remote probe, the browser assist for setting the File Name is not available. The capture file is placed in the My Files directory located on the remote probe.***

Send a remote syslog message over UDP



Send a remote syslog message over UDP

Host Name *

Port * 514

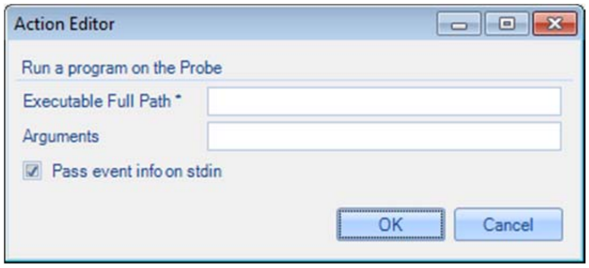
Protocol * Regular

Severity Information

Figure 40 Send to Remote Syslog

Send a syslog message using UDP to a remote host.

Run a program on the Pilot Probe



☑ Pass event info on stdin

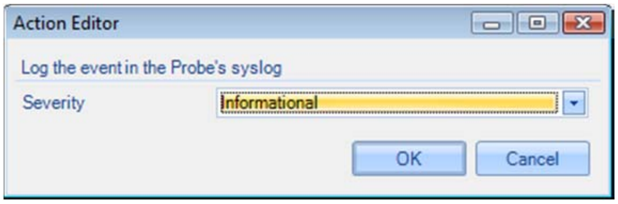
Figure 41 Run a Program

Enter the Program Name (complete path name) and any arguments. In this case the Watch is associated with a remote probe. The browser assist for setting the Program Name is not available.

If “Pass event info on stdin” option is selected, then once the program is run, informative details of the event are passed to the program on its standard input channel. For example:

```
UID: 6
Severity: INFORMATION
Time: Wednesday, 11 May 11 19:24:56 -0700
Condition: Bits/s > 0
Entities:
Watch Name: Watch 1
Watch Description:
Interface: Intel(R) 82577LM Gigabit Network Connection
Hostname: PX73HF-W7
```

Log the events in the Probe’s syslog

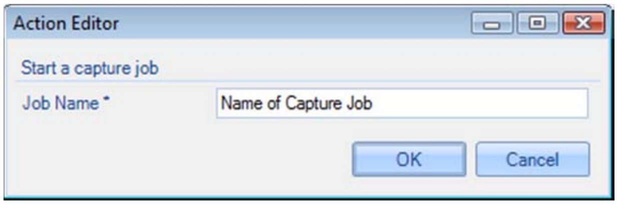


Severity: Informational

Figure 42 Send to Probe’s syslog

The event is entered into the Probe’s syslog with the indicated severity.

Start a Capture Job

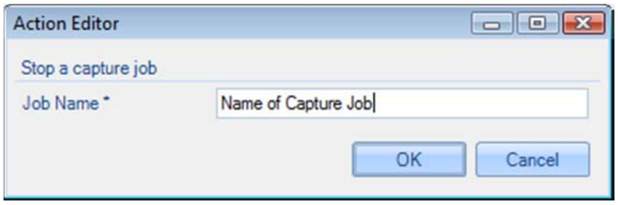


Job Name *: Name of Capture Job

Figure 43: Start a Capture Job

The event starts a currently stopped capture job. If the capture job is already started there is no change.

Stop a Capture Job



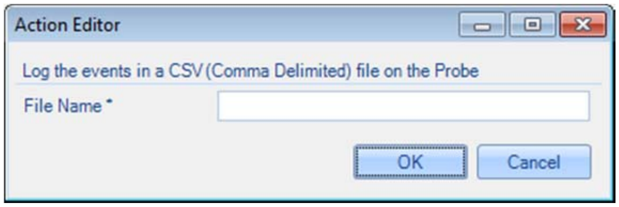
Stop a capture job

Job Name * Name of Capture Job

Figure 44: Stop a Capture Job

The event stops a currently running capture job. If the capture job is already stopped, there is no change.

Log the events in a CSV file on the Shark appliance



Log the events in a CSV (Comma Delimited) file on the Probe

File Name *

Figure 45 Send to CSV File

The event is written as a CSV file using the complete pathname provided in the Action Editor.

> *Note:* ***If the Watch is associated with a remote probe, the browser assist for setting the File Name is not available.***

Watches/Events Ribbon

The Watches/Events Ribbon is divided into a number of sections.

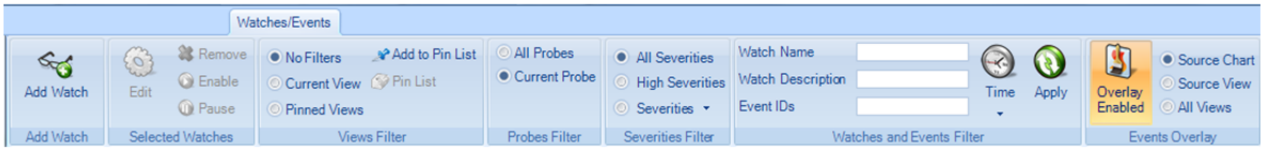


Figure 46 Watches and Events Ribbon

Add Watch

Figure 47 Add Watch

The *Add Watch* button is enabled when there is either a strip chart or bar chart selected within the current View. Clicking the Add Watch button brings up the Watch Editor panel for creating a new Watch for the selected chart within the current View.

Selected Watches

Edit Selected Watch

Figure 48 Edit Watch

With a Watch selected in the Sources panel, the *Edit* button brings up the Watch Editor. The Watch parameters can be modified with the Watch Editor.

Note: ***A Watch applied to a trace file cannot be edited.***

Remove Selected Watch

Figure 49 Remove Watch

With a Watch selected in the Sources panel, the *Remove* button is used to remove the Watch and all of the associated events in the Events panel

Enable Selected Watch

Figure 50 Enable Watch

With a disabled Watch selected in the Sources panel, the *Enable* button causes the Watch to become active.

Note: ***A Watch applied to a trace file cannot be enabled.***

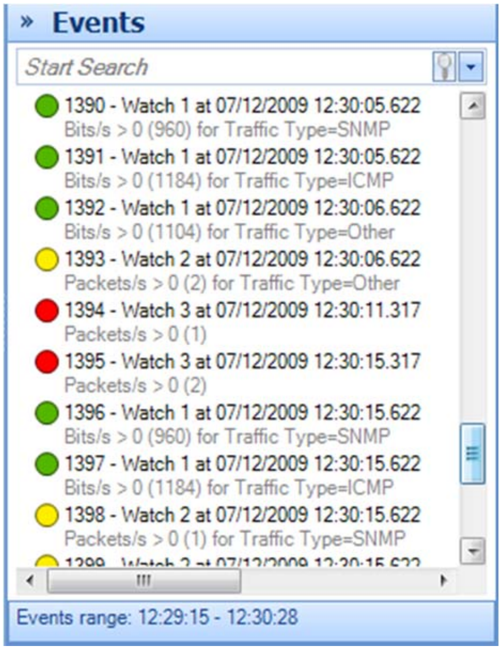
Pause Selected Watch

Figure 51 Pause Watch

With an enabled Watch selected in the Sources panel, the *Pause* button is used to disable the Watch. During the time the Watch is disabled, no events are generated.

Note: ***A Watch applied to a trace file cannot be disabled.***

Filtering Events Section



- 🟢 1390 - Watch 1 at 07/12/2009 12:30:05.622
  Bits/s > 0 (960) for Traffic Type=SNMP
- 🟢 1391 - Watch 1 at 07/12/2009 12:30:05.622
  Bits/s > 0 (1184) for Traffic Type=ICMP
- 🟢 1392 - Watch 1 at 07/12/2009 12:30:06.622
  Bits/s > 0 (1104) for Traffic Type=Other
- 🟡 1393 - Watch 2 at 07/12/2009 12:30:06.622
  Packets/s > 0 (2) for Traffic Type=Other
- 🔴 1394 - Watch 3 at 07/12/2009 12:30:11.317
  Packets/s > 0 (1)
- 🔴 1395 - Watch 3 at 07/12/2009 12:30:15.317
  Packets/s > 0 (2)
- 🟢 1396 - Watch 1 at 07/12/2009 12:30:15.622
  Bits/s > 0 (960) for Traffic Type=SNMP
- 🟢 1397 - Watch 1 at 07/12/2009 12:30:15.622
  Bits/s > 0 (1184) for Traffic Type=ICMP
- 🟡 1398 - Watch 2 at 07/12/2009 12:30:15.622
  Packets/s > 0 (1) for Traffic Type=SNMP
- 🟡 1399 - Watch 2 at 07/12/2009 12:30:15.622

Events range: 12:29:15 - 12:30:28

Figure 52 Events Panel

When there are multiple Watches, or even a single Watch, it is possible to generate a very large number of Events. Sorting through these looking for significant ones can be daunting. The Events panel has a search box that can be used to isolate events of interest.

Another possibility for filtering events can be found in the middle sections of the Watches/Events ribbon.

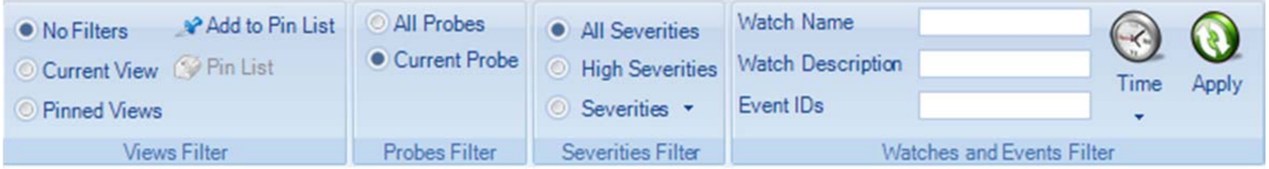


Figure 53 Event Filtering Section of the Watches/Events Ribbon

Figure 53 shows the sections on the Watches/Events ribbon that deal with locating Events by filtering on:

- Views Filter
- Severity Filter
- Watches and Events Filter

> Note: ***The events filter that results from these three filter sections is the conjunction of the filtering provided by the individual sections.***

Views Filter

This section of the ribbon deals with filtering Events based on their associated Views.

- *No Filters* is selected: Filtering on View is disabled.
- *Current View* is selected: The Views Filter selects only those Events that are associated with the Current View.
- *Pinned Views* is selected: The Pin List contains a list of Views that have been "Pinned." When Pinned Views is selected, the Views Filter selects only those Events that are selected with some View in the "Pin List."

Add to Pin List

Figure 54 Add to Pin List

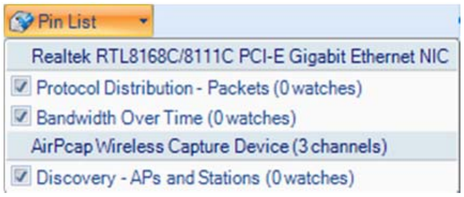
With a View selected in the Sources panel, clicking *Add to Pin List* adds the selected View to the Pin List.

(Show the) Pin List

Figure 55 (Show the) Pin List

The *Pin List* button is active whenever there is at least one View in the Pin List. Clicking the Pin List button (when it is active), shows the Pin List.

The Pin List



Pin List

Realtek RTL8168C/8111C PCI-E Gigabit Ethernet NIC

☑ Protocol Distribution - Packets (0 watches)

☑ Bandwidth Over Time (0 watches)

AirPcap Wireless Capture Device (3 channels)

☑ Discovery - APs and Stations (0 watches)

Figure 56 The Pin List

The *Pin List* itself shows the pinned views and their sources. The sources can be either live or a trace file. Views can be removed from the Pin List by clicking the corresponding check boxes.

Probes Filter

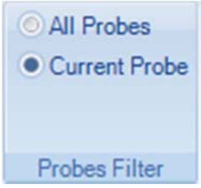


Figure 57 Probes Filter

There are two choices with the Probes Filter. Show the Events from all of the Shark appliances (including the Local System) in the Events panel, or only show the Events from the currently selected Shark appliance in the Sources panel.

Severities Filter

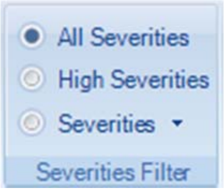


Figure 58 Severities Filter

The Severities Filter section allows you to add filters on the Event severities. The three choices are disjoint.

- *All Severities*. This is equivalent to no Severity filtering.
- *High Severities*. High severities are defined to be Error or higher – Error, Critical, Alert, and Emergency.
- *Severities (List)*. When this button is selected, the Events are filtered on the severity levels in this list. The list can be set/reset by clicking the down-arrow.

Severities Filter

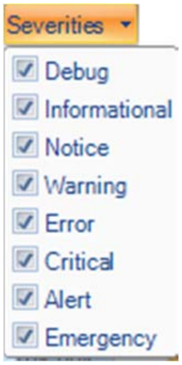


Figure 59 Severities List

The Severities List contains the severities used by the severities filter. The selected severities are those with the checks. Severities can be selected or deselected using the check boxes.

Watches and Events Filter

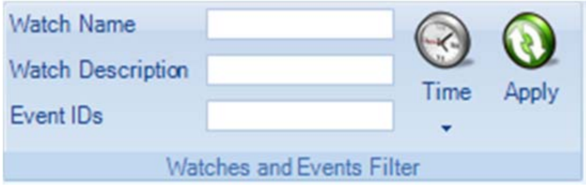


Figure 60 Watches and Events Filter

Event filtering based on the corresponding Watch Name, Watch Description, Event IDs, or Time Interval.

Time Filter

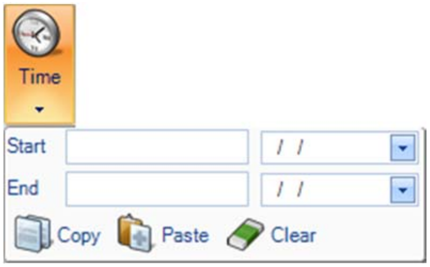


Figure 61: Time Selection

The Start and End times can be filled in manually, or the Paste operation can be used. Typically, the clipboard is carrying a time interval that was obtained using the copy operation in the Time Selection section of the Time Control ribbon. Conversely, if the time interval is available, the Copy operation can be used to save the interval to the clipboard for use in making time selections by pasting it into the Time Selection section of the Time Control ribbon.

Apply

Figure 62 Apply Button

Once all of the parameters in the Watches and Events Filter have been set, click the *Apply* button for the filter to take effect.

> *Note:* ***The Watches and Events Filter does not take effect until the user clicks the Apply button.***

Events Overlay

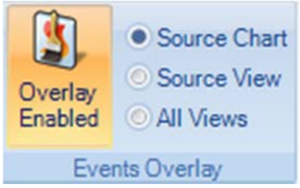


Figure 63 Events Overlay Section

By selecting the *Overlay Enabled* button, the radio buttons are enabled.

- *Source Chart*. Only show the events in a Chart of the Watches that are associated with the Chart. This is the usual case where you see the events only in the chart where the Watch was created.
- *Source View*. Show events associated with all of the Watches in a View in each Chart of a View. This is generally used when one of the charts in a View has a Watch and you want to see these events displayed in the other charts in the View.
- *All Views*. Show all the events of all the Watches in all of the charts of all of the Views. Is often used if only one chart has a Watch and you want to see where these events occur in the charts of all of the other Views.

Predefined Watches

Many of the View folders contain an initial subfolder containing predefined Watches. Figure 64 shows the expanded Bandwidth Usage folder. Its first subfolder is called the *Bandwidth Usage Watches*.

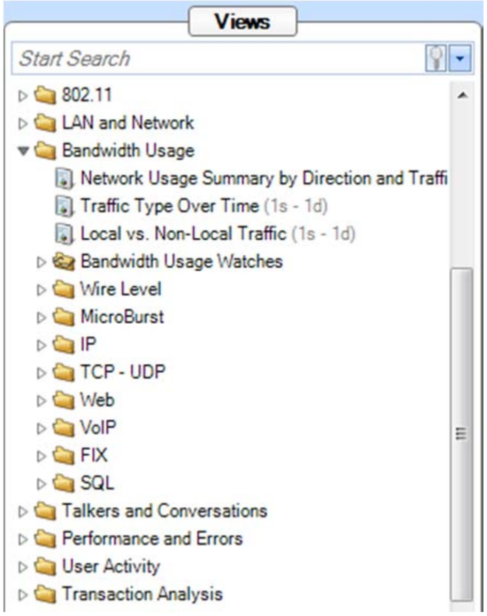


Figure 64 Predefined Watches

Opening the Bandwidth Usage Watches folder displays the following:

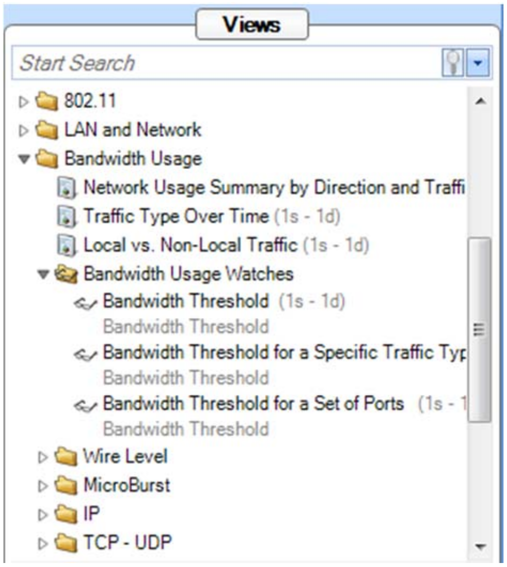
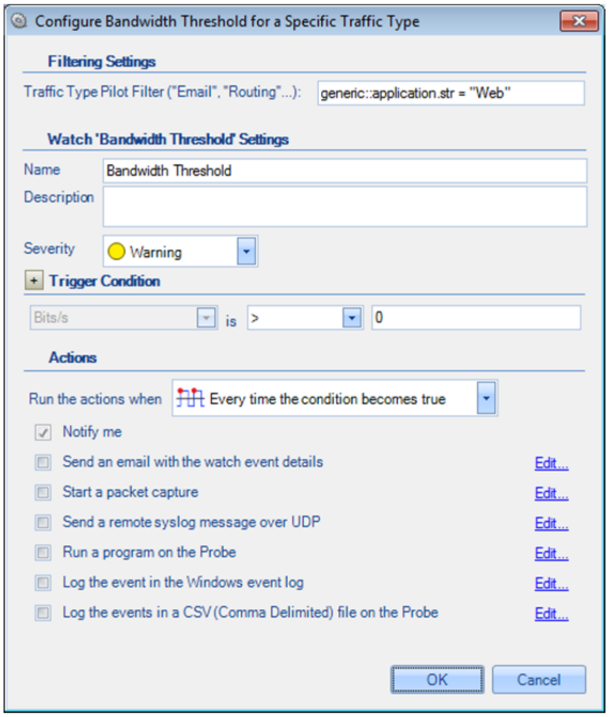

Views
Start Search
802.11
LAN and Network
Bandwidth Usage
Network Usage Summary by Direction and Traffi
Traffic Type Over Time (1s - 1d)
Local vs. Non-Local Traffic (1s - 1d)
Bandwidth Usage Watches
Bandwidth Threshold (1s - 1d)
Bandwidth Threshold
Bandwidth Threshold for a Specific Traffic Typ
Bandwidth Threshold
Bandwidth Threshold for a Set of Ports (1s - 1
Bandwidth Threshold
Wire Level
MicroBurst
IP
TCP - UDP

Figure 65 Expanded Bandwidth Usage Watches Folder

The expanded Bandwidth Usage Watches folder contains three entries. Each of these entries consists of a View and a Watch that is associated with the View. For Example, the *Bandwidth Threshold for a Specific Traffic Type* (in Figure 65) is a View with a *Bandwidth Threshold* Watch associated with the View. This View/Watch combination can be applied to either a live or off-line source just like any other View. However, when it is applied, the Watch Editor displayed to be filled in with the usual parameters. In this case a Filter Settings section is made available to further modify the Watch before applying the View/Watch combination.



Configure Bandwidth Threshold for a Specific Traffic Type

Filtering Settings

Traffic Type Pilot Filter ("Email", "Routing"...): generic::application.str = "Web"

Watch 'Bandwidth Threshold' Settings

Name: Bandwidth Threshold

Description:

Severity: Warning

Trigger Condition

Bits/s is > 0

Actions

Run the actions when: Every time the condition becomes true

- ☑ Notify me
- ☐ Send an email with the watch event details — Edit...
- ☐ Start a packet capture — Edit...
- ☐ Send a remote syslog message over UDP — Edit...
- ☐ Run a program on the Probe — Edit...
- ☐ Log the event in the Windows event log — Edit...
- ☐ Log the events in a CSV (Comma Delimited) file on the Probe — Edit...

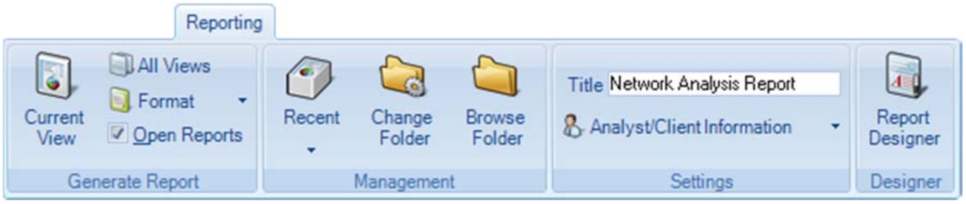
Figure 66 Watch Editor Panel with Filter Settings

Figure 66 shows the watch editor for the Bandwidth Threshold predefined Watch. In addition to the usual Watch settings, the user can specify Filter Settings to select specific traffic types.

> *Note:* ***Filters that appear in predefined View/Watch combinations are placed between the source and the View to filter out unwanted packets before being processed by the View. The Watch is subsequently applied to the metrics produced by the View.***

Once the combined View/Watch is applied, it behaves exactly the same as if the View and the Watch were each applied independently – the View to the source and the Watch to the View.

Reporting Ribbon



Title Network Analysis Report

☑ Open Reports

Figure 67 Reporting Ribbon

The *Reporting Ribbon* is used to create and manage reports created from Views. Certain sections and buttons of the ribbon are disabled by default. Reports can be made from one View or from all open Views. Reports can be generated for a number of different file formats in a single batch operation. Many things can be customized in a generated report. The ribbon is described below top-to-bottom and left-to-right, by section.

Generate Report

This section manages how the reports are generated.

Current View

Icon 20 Current View

The *Current View* button is used to generate a report using the current View, which requires that a View be the foremost tab. Under any other situation, this button is disabled. This button and the next button, “All Views” act differently depending on the settings of the final two buttons of the section, *Format* and *Open Reports*.

All Views

Icon 21 All Views

The *All Views* button is used to generate a report using all open Views. This button and the previous button, *Current View*, act differently depending on the settings of the final two buttons of the section, *Format* and *Open Reports*.

Format

Icon 22 Format

The *Format* button opens a submenu that specifies one or more export formats. These selections are saved in the global configuration file. By default, only the PDF option is selected.

The meaning of each check box is as follows:

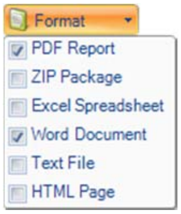
PDF Report

The *PDF Report* checkbox refers to a PDF 1.4 (Acrobat 5.x or newer) PDF document generated with all security turned off.

Zip Package

The *Zip Package* check box refers to a ZIP file with the following contents:

- Each trace file analyzed in the report.
- The MD5 cryptographic digests of the trace files (smaller than 50 MB).
- The PDF version of the report.



Format ▾

☑ PDF Report
□ ZIP Package
□ Excel Spreadsheet
☑ Word Document
□ Text File
□ HTML Page

Submenu 5 Format

Excel Spreadsheet

The *Excel Spreadsheet* check box refers to an Microsoft Excel spreadsheet with the tabular data of the report in a way that can be used to generate further graphs and charts with the spreadsheet graphing options that are available in Excel.

Word Document

The *Word Document* check box refers to a "Rich Text Formatted" (RTF) document that can be viewed in Microsoft Word.

Text File

The *Text File* check box refers to a plain text document. Naturally, no images are available, but the image data is made available in tabular form.

HTML Page

The *HTML Page* check box refers to a generated HTML page and a directory containing the images of the relevant charts in PNG format. The HTML is compatible with all major modern web browsers.

Open Reports

☑ Open Reports

Figure 68 Open Reports

The *Open Reports* check box, selected by default, works in the following way:

When On

Pressing the *Current View* or *All Views* button instantiates the appropriate helper applications to be open with the generated reports. For instance, when generating Word and HTML formatted reports, then the default word processor and web browser open and display the reports.

When Off

No programs are opened when a report is generated.

Management

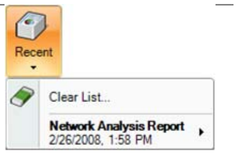
Generated reports are saved to a user-specified directory. The default directory is the "My Documents" directory in the user's "Documents and Settings" directory (or the language equivalent). This can be changed as desired. The *Management* section provides a convenient way to get to the directory, manage recently created reports, and change the report directory.

Recent

Icon 23 Recent

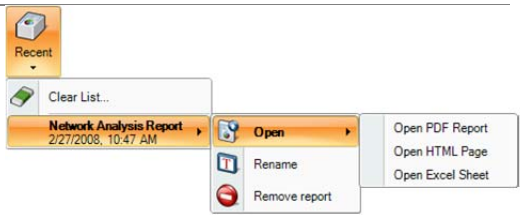
The *Recent* button opens a submenu to manage recently generated reports. By default, before reports are generated, the Recent button is disabled.

After a report is generated, a reference to it is placed in the Recent submenu list. The list holds the five most recently generated reports and can be cleared at any time. Note that the clear operation does not remove the file(s) from disk but simply clears the referential list inside of Cascade Pilot.



Submenu 6 Recent Reports

Each submenu item has in turn another submenu to open one of the formatted reports from the generated report package. Additionally, reports can be renamed and removed irrevocably from disk.



Submenu 7 Recent Reports (Detail)

Change Folder

Icon 24 Change Folder

The *Change Folder* button changes where future generated reports will be saved.

Browse Folder

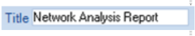
Icon 25 Browse Folder

The *Browse Folder* button opens a browser window to show the folder where future reports will be saved.

Settings

The *Settings* section manages what goes on the cover page of the report, if it is used. (See the section on the Report Designer about how to turn it off.)

Title



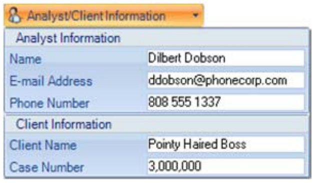
Title Network Analysis Report

Figure 69 Title

The *Title* edit box specifies what to call subsequently generated reports. The title goes on the cover page if the page is included in the report generation. See the section on the Report Designer Ribbon that follows for more information.

Analyst/Client Information

Icon 26 Analyst/Client Information



Analyst/Client Information

Analyst Information

Name	Dilbert Dobson
E-mail Address	ddobson@phonecorp.com
Phone Number	808 555 1337

Client Information

Client Name	Pointy Haired Boss
Case Number	3,000,000

Submenu 8 Analyst/Client Information

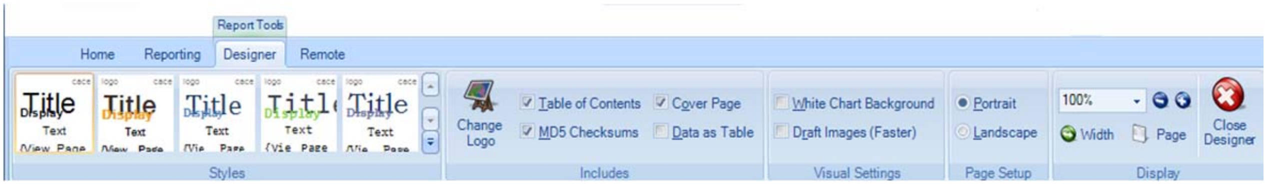
The *Analyst/Client Information* button presents a submenu that specifies what information appears on the cover page of a report. Each field is directly analogous to what appears on the cover page. Refer to the appendix on the example report for more information.

Report Designer

Icon 27 Report Designer

The *Report Designer* button opens a new tab in the ribbon bar to do specific design actions on subsequently generated reports. This ribbon is described below.

Report Designer Ribbon



☑ Table of Contents ☑ Cover Page
☑ MD5 Checksums □ Data as Table
□ White Chart Background
□ Draft Images (Faster)
● Portrait
○ Landscape

Figure 70 Report Designer Ribbon

The *Report Designer* ribbon is not always available. It is a contextual ribbon that appears only when reports are being designed. In order to get to it, click the *Report Designer* button at the end of the *Reporting* ribbon (described at the end of the previous section).

This displays a generic template report as a tabbed window that does not correspond to any specific data from a view. All changes made in the report designer take effect immediately and there is no need to save when exiting the designer.

Additionally, the designer can be left open while generating reports for quick changes. Note that any changes made to the template via the report designer will only affect how subsequent reports are generated, not any existing reports.

Styles

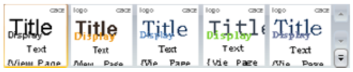


Figure 71 Styles

The *Styles* section controls the thematic look and feel of subsequent reports. There are five choices to choose from and each can be viewed by simply hovering over them with the mouse. A theme can be selected and set as the default by clicking it. In the depiction on the left for instance, the first style is selected.

Includes

The *Includes* section has options that determine what is presented inside a report.

Change Logo

Icon 28 Change Logo

The *Change Logo* button is used to specify the logo that goes in the upper right hand side of the cover page of all subsequent reports.

Table of Contents

☑ Table of Contents

Figure 72 Table of Contents

The *Table of Contents* check box (checked by default) is used to specify whether to include a table of contents in subsequent reports.

MD5 Checksums of Trace Files

☐ MD5 Checksums

Figure 73 MD5 Checksums

The *MD5 Checksums* check box (not checked by default) is used to specify whether MD5 cryptographic digests is generated for trace files in subsequent reports. These digests are printed on the reports and placed in a separate files when using the ZIP output format.

Cover Page

☑ Cover Page

Figure 74 Cover Page

The *Cover Page* check box (checked by default) is used to specify whether to include cover pages in subsequent reports.

Data as Table

☑ Data as Table

Figure 75 Data as Table

The *Data as Table* check box (checked by default) is used to specify whether to include quantitative data tables in subsequent reports.

Visual Settings

The *Visual Settings* section has options used to modify some technical aspects of the creation process of reports.

White Chart Background

☐ White Chart Background

Figure 76 White Chart Background

The *White Chart Background* check box (not checked by default) is used to specify whether the generated charts have a white background instead of the gradient one in Cascade Pilot. Turning this feature on:

- Increases the visual contrast on monochrome (black and white) printers.
- Marginally decreases the file size of generated reports by about 10%.

Draft Images (Faster)

Figure 77 Draft Images (Faster)

The *Draft Images (Faster)* check box (not checked by default) is used to specify the quality of the images in subsequent reports. Draft images are a suitable resolution for viewing on a computer while non-draft images are suitable for printing. Turning this feature on:

- Decreases the time needed to generate reports.
- Decreases the file size of the generated report.

Page Setup

The *Page Setup* section controls the page orientation of future generated reports.

Portrait

Figure 78 Portrait

The *Portrait* check box makes all subsequent reports generate in portrait orientation.

Landscape

Figure 79 Landscape

The *Landscape* check box makes all subsequent reports generate in landscape orientation.

Display

The *Zoom* section is used to control the magnification of the report template.

Zoom Amount

Figure 80: Zoom Amount

The *Zoom Amount* drop down specifies the magnification of the template in the report designer.

Decrease Zoom

Icon 29 Decrease Zoom

The *Decrease Zoom* button is the “minus” sign and it decreases the magnification level of the template in the report designer by 10%.

Increase Zoom

Icon 30 Increase Zoom

The *Increase Zoom* button is the “plus” sign and it increases the magnification level of the template in the report designer by 10%.

Width

Icon 31 Zoom Width

The *Screen Width* button changes the magnification level of the template in the report designer so the width of a page matches all that is available in the tab.

Page

Icon 32 Zoom Page

The *Page Height* button changes the magnification level of the template in the report designer so that an entire page can be viewed.

Close Designer

Icon 33 Close Designer

The *Close Designer* button closes the report designer ribbon and template view tab. Since all changes are immediate, there is no prompt to save for changes.

Remote Ribbon

Users and Groups play an important role in accessing remote probes. This section describes the remote probe Credential Manager.

Remote Probe Credential Manager

User and Group access control

All communication between the Cascade Shark appliances and the Cascade Pilot uses SSL-encrypted web communications and requires HTTP basic access authentication credentials (HTTP Authentication). The Cascade Shark appliance passes the authentication credentials to the Credential Manager, which determines whether the user has the permission to execute the requested operation. If not, the Cascade Shark appliance returns a *not enough privileges* error to the Cascade Pilot making the request.

Credential Manager

The Credential Manager running in Cascade Shark supports two types of authentication:

- Local authentication. The management of credentials is governed by the user configuration file co-located with the Cascade Shark appliance.
- Remote authentication. The management of credentials uses an external authentication/auditing server using either the Radius or Tacacs+ protocols.

Each user has ownership of the resources that the user created, including files, folders, and views that are applied to a traffic source. With the exception of administrators, users cannot see a file or a view created by another user, and a user cannot close a view or delete a file that was created by another user.

Resources, however, can be *shared* among one or more groups. For local authentication, a user can be a member of one or more groups, whereas for remote authentication, a user can be a member of only one group.

Members of a group share a common folder identified with the group name. This folder can be used for trace file sharing, and all the users in the group have read and write access to the folder. When a resource is dragged into this folder, all the other members of the group immediately have access to it.

Views can be shared with other groups by right-clicking on them and selecting **share with**. As soon as a view is shared, the selected group immediately sees it in their sources panel. Note: sharing views is supported only with local authentication.

User and groups are configured using the Cascade Shark web interface.

Privileges

The web interface is used to configure the privileges for users and groups. A privilege is a capability that can be granted or revoked, and is specified as an attribute of a group. The Cascade Shark appliance currently implements the following privileges:

- **IsAdministrator**. Gives members of a group full access to the Cascade Shark appliance. Administrators see all the resources in the system, including views, files and folders that have been created by other users. Administrators have full control of all these resources.
- **CanApplyViewsOnFiles**. Allows members of the group to apply views to traces files residing on the Cascade Shark appliance, capture jobs and trace clips. In order to apply a view to a capture job or trace clip, the privilege **CanAccessProbeFiles** is also required.
- **CanApplyViewsOnInterfaces**. Allows members of the group to apply views to the capture ports and job interfaces on the Cascade Shark appliance.
- **CanCreateFiles**. Allows members of the group to create files on the Cascade Shark appliance, by selecting **Send to File** in Cascade Pilot.
- **CanImportFiles**. Allows members of the group to import files into the Cascade Shark appliance through drag and drop or by clicking **Import Files Into Probes** in the Remote ribbon of Cascade Pilot.
- **CanExportFiles**. Allows members of the group to export files from the Cascade Shark appliance, and move them to Cascade Pilot or to another Cascade Shark appliance (assuming the user has sufficient privilege on the target Cascade Shark appliance to create a trace file). When this privilege is not granted, the user is not able to export a trace file to Wireshark, because that involves exporting packets out of the Cascade Shark appliance to Cascade Pilot.
- **CanShareViews**. Enables members of group to share the views created on the Cascade Shark appliance with any group on the same appliance. If this privilege is not granted, a user can share a view with only the groups to which he belongs.
- **CanAccessProbeFiles**. Enables members of the group to access capture jobs and trace clips located on the Cascade Shark appliance.
- **CanCreateJobs**. Enables members of the group to create and manage capture jobs from the Cascade Shark Web Interface.

Privilege policy

Since a user can be part of one or more groups, conflicts can arise between the privileges of the multiple groups to which a user belongs. To solve these conflicts, the Cascade Shark appliance grants a privilege if it is enabled for any group of which the user is a member.

The Remote Ribbon

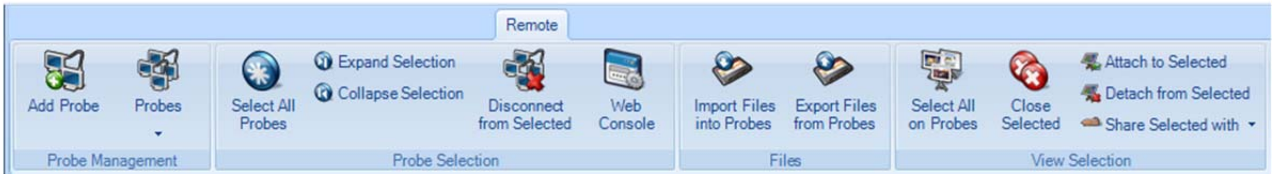


Figure 81 Remote Ribbon

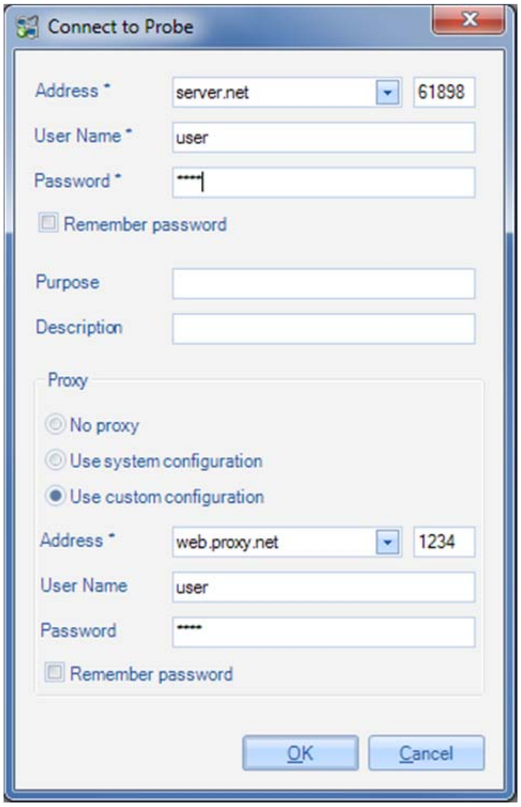
This section describes sections of the Remote Ribbon: Probe Management, Probe Selection, Files, and View Selection.

Probe Management

Add Probe

Icon 34 Add Probe

Clicking the *Add Probe* button brings up the *Connect to Probe* panel.



Connect to Probe

Address * server.net 61898

User Name * user

Password * ****

□ Remember password

Purpose

Description

Proxy

○ No proxy

○ Use system configuration

● Use custom configuration

Address * web.proxy.net 1234

User Name user

Password ****

□ Remember password

Figure 82 Connect to Probe Panel

The *Connect to Probe* panel is used to initiate a connection to a Shark appliance. The required parameters include the Shark appliance address (either a host name or IP address), Shark appliance port number (default is 61898), user name, and password. A descriptive comment for the Shark appliance is optional. The information regarding the Shark appliance is saved in the probe list, which is accessible using the *Probes* icon located in the Probe Management section of the Remote ribbon.

Proxy Support

Cascade Pilot can connect to Cascade Shark appliances via an HTTPS proxy server.

The Proxy section of the Connect to Probe panel has three options for the proxy settings. *Use system configuration* is the default option, and it causes Pilot to use the proxy settings that are specified in the system Control Panel. The *No Proxy* setting always connects directly to the Shark appliance, regardless of the system-wide setting. The *Use custom configuration* opens additional fields (shown in the Figure above) where the address, port, user name, and password are specified to connect to the proxy.

Note: ***The that remember password checkbox, if selected, causes the credentials to be stored in plain text in the Cascade Pilot configuration file.***

Probes

Icon 35 Probes

The *Probes* button brings up the probes panel containing, among other things, the list of probes that have been Added, but not Deleted, using the *Connect to Probe* panel.

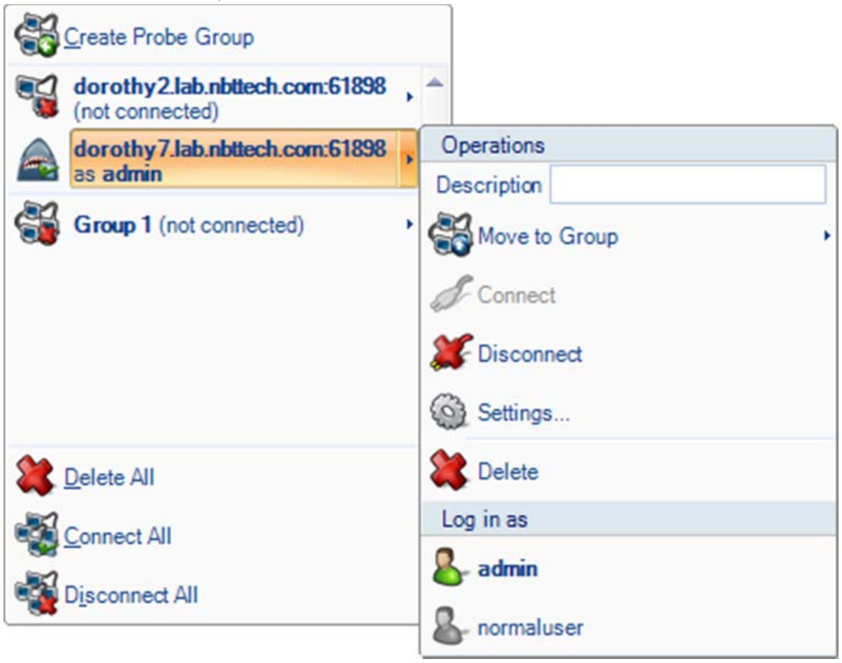


Figure 83 Probes Panel

The first item in the Probes Panel is the Create Probe Group. This selection is used to create a collection of probes that can be treated as a single group. A Shark appliance can be a member of at most one probe group. If a probe is member of a probe group, then it appears only within the probes group in the Probes Panel.

Below the Create Probe Group is a list of all of the probes that have been added using the Add Probe panel and have not been removed from this list. Clicking the icon to the left of one of the probes on the list disconnects Cascade Pilot from the probe if it is already connected. On the other hand, if the probe is initially disconnected, then clicking the icon reconnects the probe as the user shown in the Probes Panel.

The last three items on the main panel act on the list as a whole. Delete All, Connect All, and Disconnect All.

Selecting a Shark appliance on the list brings up a submenu for operations on the selected Shark appliance, enabling the user to edit the appliance description, move the appliance into a probe group, connect to or disconnect from the appliance, display the appliance settings, and delete the appliance from the list.

When Cascade Shark is configured for local authentication mode, the “Log in as” list includes the identity of all users having accounts on the selected Shark appliance. The item in bold is the identity of the user who is currently logged into the Shark appliance from Cascade Pilot. Selecting a user on this list initiates an attempt to connect to the Shark appliance on behalf of the selected user. When remote authentication is being used this list is not shown.

Probe Selection

Select All Probes

Icon 36 Select All Probes

The *Select All Probes* button highlights (selects) all probes in the Sources Panel (Devices and Files).

Expand Selection

Icon 37 Expand Selection

The *Expand Selection* button expands all the selected probes in the sources panel, thereby showing all their associated interfaces and file folders**.**

Collapse Selection

Icon 38 Collapse Selection

The *Collapse Selection* button collapses all the selected probes in the sources panel, hiding all their associated interfaces, files, and views.

Disconnect from Selected

Icon 39 Disconnect from Selected

The *Disconnect from Selected* button disconnects Cascade Pilot from the selected probes. The selected probes continue to process live views and maintain the views associated with trace files.

Web Interface

Icon 40 Web Interface

The *Web Interface* button opens the selected remote probe’s Web Interface.

Files

Import Files into Probes

Icon 41 Import Files into Probes

The *Import Files into Probes* button transfers trace files from the Local System to the selected remote probe. The trace files are transferred to the selected directory of the remote probe.

Export Files from Probes

Icon 42 Export Files from Probes

The *Export Files from Probes* button transfers files from the selected remote probe to the Local System. If a folder on a remote probe is included in the selection, then the folder and its contents are transferred to the Local System. If a file on a remote probe is in the selection, then just the file is transferred. Multiple selections are permitted as long as the selections are either all folders or all files.

View Selection

Select All on Probes

Icon 43 Select All on Probes

The *Select All on Probes* button highlights (selects) all the views on the selected probes.

Close Selected

Icon 44 Close Selected

The *Close Selected* button closes all the selected views.

Attach to Selected

Icon 45 Attach to Selected

The *Attach to Selected* button attaches to the selected views.

Detach from Selected

Icon 46 Detach from Selected

The *Detach from Selected* button detaches from the selected views.

Share Selected with

Icon 47 Share Selected with

The *Share Selected with* button brings up a panel to allow selected views on Shark appliances to be shared with other groups.

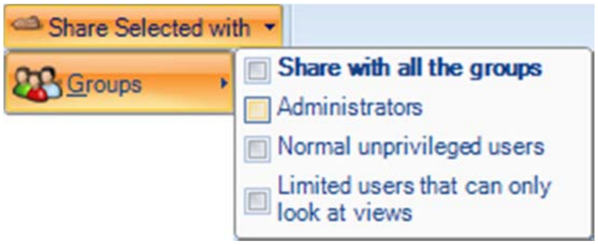

Share Selected with
Groups
□ Share with all the groups
□ Administrators
□ Normal unprivileged users
□ Limited users that can only look at views

Figure 84 Share Selected with Groups

Shark Packet Recorder

A traditional approach to capturing high-speed and/or long duration network traffic is to create a file rotation scheme, whereby the capture is divided into a collection of small trace files with names indicating the time intervals covered by the individual files. It is not difficult to see that this approach can lead to thousands of small files, which makes analysis and troubleshooting extremely tedious, especially when the traffic of interest spans multiple trace files.

The Cascade Shark appliance includes a facility called the *Shark Packet Recorder* that uses a new approach for dealing with high-speed and/or long-duration traffic capture scenarios. The Packet Recorder is based on an optimized *packet data store* called *SharkFS* - a novel approach that saves network traffic as objects called Job Traces. It also makes use of *time filters* to efficiently index the packet data, which eliminates the need for a cumbersome file rotation scheme.

Furthermore, a user can isolate specific and manageable portions of a Job Trace for analysis and visualization by creating Trace Clips, which correspond to arbitrary time intervals within a Job Trace. An important feature of a Trace Clip is that it does not require any additional storage beyond the underlying Job Trace. Trace Clips behave just like ordinary trace files for analysis and can be converted to ordinary pcap files on the Cascade Shark appliance.

Terminology

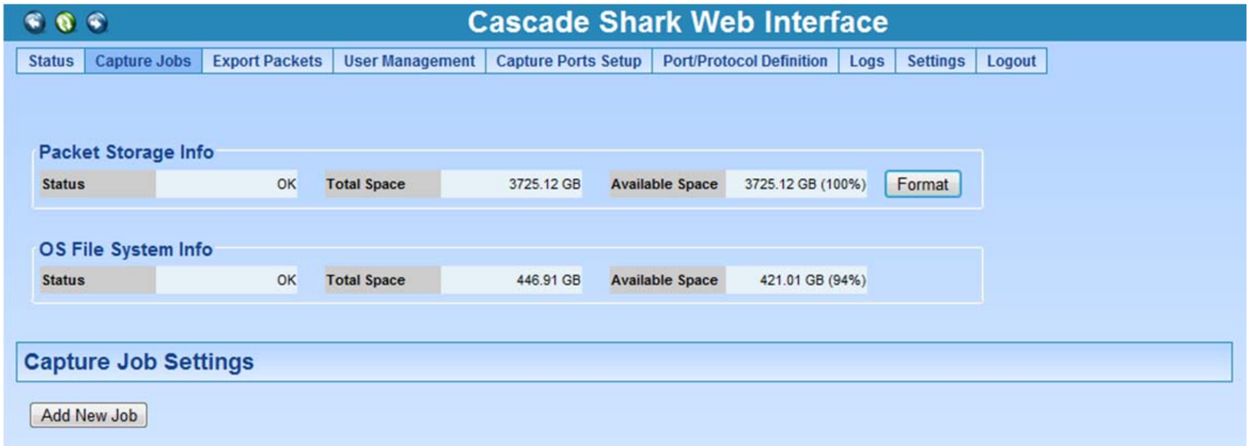
- **Capture Job**: A *Capture Job* refers to the specific parameters associated with at packet recording session. These parameters include the job name, the network interface, a BPF filter, start and stop criteria, and an upper bound on the amount of storage to be used by the Capture Job.
- **Job Trace**: The *Job Trace* represents the network traffic saved in the packet data store. Each Capture Job is associated with exactly one Job Trace, which has the same name as the Capture Job.
- **Trace Clips**: *Trace Clips* represent user-defined time intervals within a Job Trace.
- **Jobs Repository**: In Cascade Pilot, the Files panel for a Shark appliance contains a folder called the *Jobs Repository* that has an icon and the name for each Job Trace in the appliance.
- **Capture Job Interface**: In Cascade Pilot, the Devices panel for a Shark appliance contains an icon and the name for each *Capture Job Interface* representing the network interface associated with a Capture Job on the appliance. Views can be applied to these Capture Job Interfaces creating a visual analysis and representation of the corresponding Job Trace.

The Cascade Shark appliance includes two separate storage subsystems:

- The OS file system contains the Cascade Shark appliance file system, software, pcap trace files, View metrics, and Trending/Indexing data for Job Traces and pcap files.
- The Packet Storage subsystem contains the RAID Array used by the Shark Packet Recorder to store Job Traces. This storage system is optimized to provide high-speed writing to disk and fast read access for arbitrary time intervals within a Job Trace.

Capture Jobs

The Capture Jobs menu item takes you to a screen showing status and usage of the Packet Storage subsystem and OS file system, as well as any currently running capture jobs.



Packet Storage Info

Status	OK	Total Space	3725.12 GB	Available Space	3725.12 GB (100%)	Format

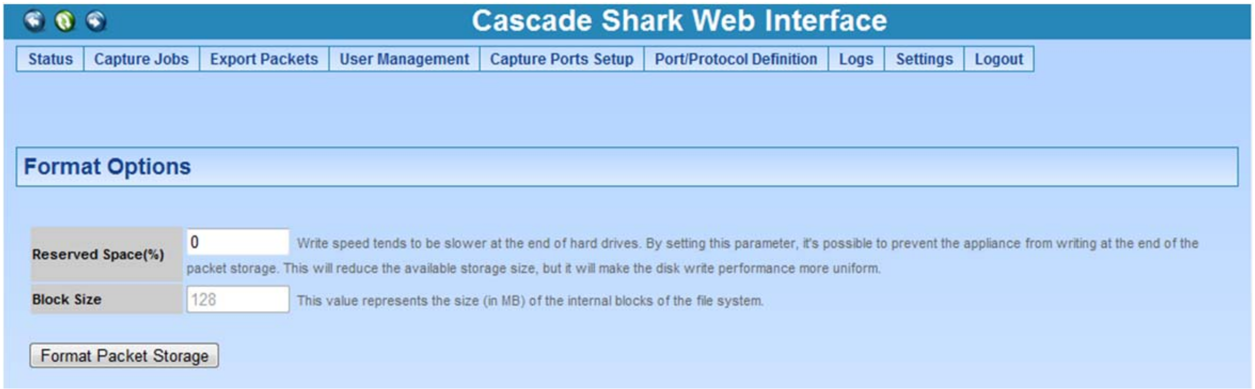
OS File System Info

Status	OK	Total Space	446.91 GB	Available Space	421.01 GB (94%)

Capture Job Settings

Figure 85: Cascade Shark appliance Packet Recorder – No Capture Jobs

Clicking the **Format** button displays the page shown in Figure 86. This panel shows the block size used by the Shark Packet Recorder and has the Format Storage button, which reformats the Packet Storage subsystem. Note that reformatting packet storage destroys all recorded packet data on the appliance and should be done only when instructed by Riverbed Support.



Format Options

Reserved Space(%)	0	Write speed tends to be slower at the end of hard drives. By setting this parameter, it's possible to prevent the appliance from writing at the end of the packet storage. This will reduce the available storage size, but it will make the disk write performance more uniform.
Block Size	128	This value represents the size (in MB) of the internal blocks of the file system.

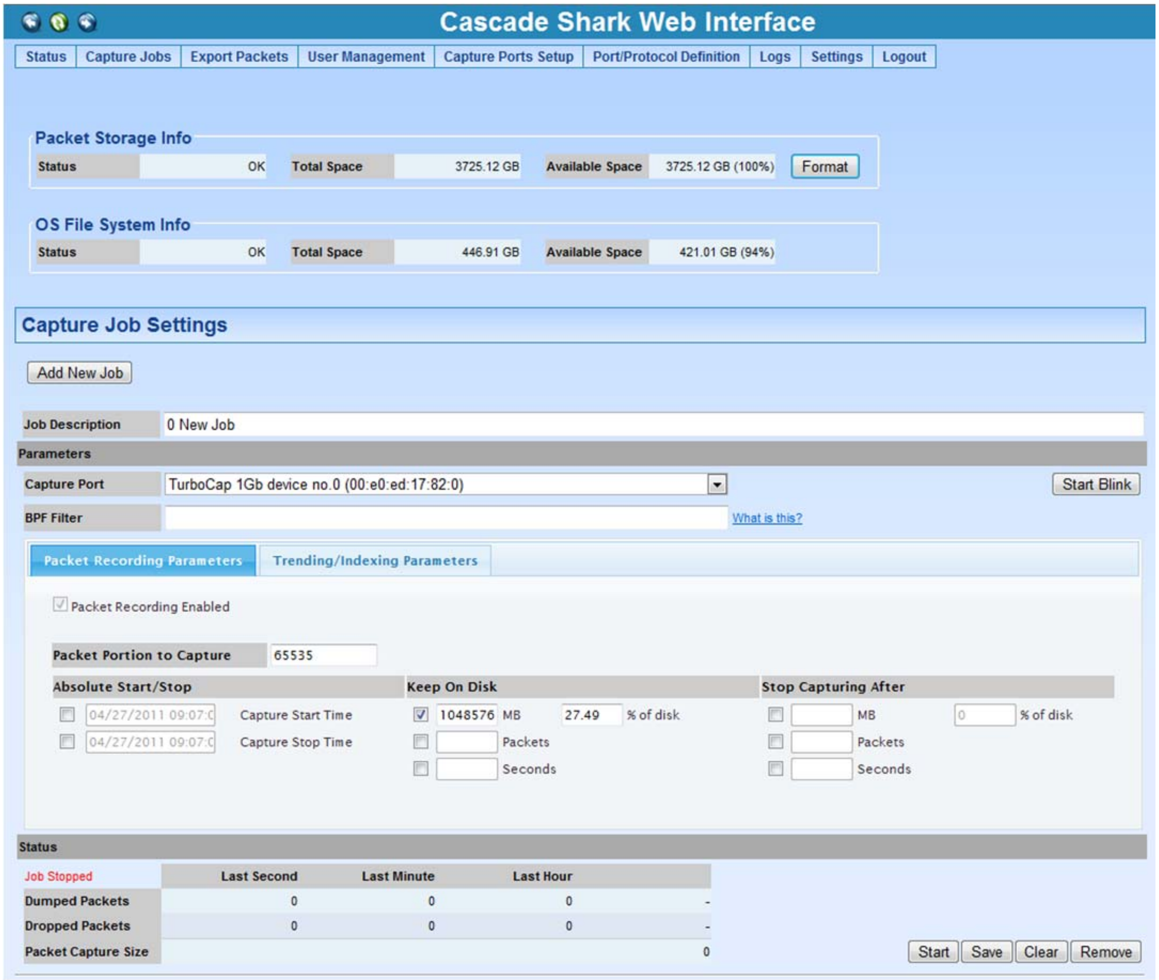
Figure 86: Storage format options

The Reserved Space field can be used to prevent use of the inner tracks of hard disks that can have slower transfer rates. Setting this value to something other than 0% can in some cases provide more uniform write-to-disk speeds although it reduces the amount of storage available for packet capture.

Add/Edit Capture Jobs

This section describes how to create a Capture Job and subsequently manage it. Multiple Capture Jobs can exist simultaneously.

Clicking **Add New Job** displays a new Capture Job form on the Capture Job page. This form is shown in Figure 87. The form has two tabs: Packet Recording Parameters and Trending/Indexing Parameters.



Packet Storage Info

Status	OK	Total Space	3725.12 GB	Available Space	3725.12 GB (100%)

OS File System Info

Status	OK	Total Space	446.91 GB	Available Space	421.01 GB (94%)

Capture Job Settings

Job Description: 0 New Job

Parameters

Capture Port: TurboCap 1Gb device no.0 (00:e0:ed:17:82:0)

BPF Filter:

☑ Packet Recording Enabled

Packet Portion to Capture: 65535

Absolute Start/Stop		Keep On Disk		Stop Capturing After	
□ 04/27/2011 09:07:0	Capture Start Time	☑ 1048576 MB	27.49 % of disk	□ MB	0 % of disk
□ 04/27/2011 09:07:0	Capture Stop Time	□ Packets		□ Packets	
		□ Seconds		□ Seconds	

Status

Job Stopped	Last Second	Last Minute	Last Hour	
Dumped Packets	0	0	0	-
Dropped Packets	0	0	0	-
Packet Capture Size				0

Figure 87: Adding a Capture Job

Packet recording parameters

There are a number of configuration parameters that need to be set when creating a Capture Job:

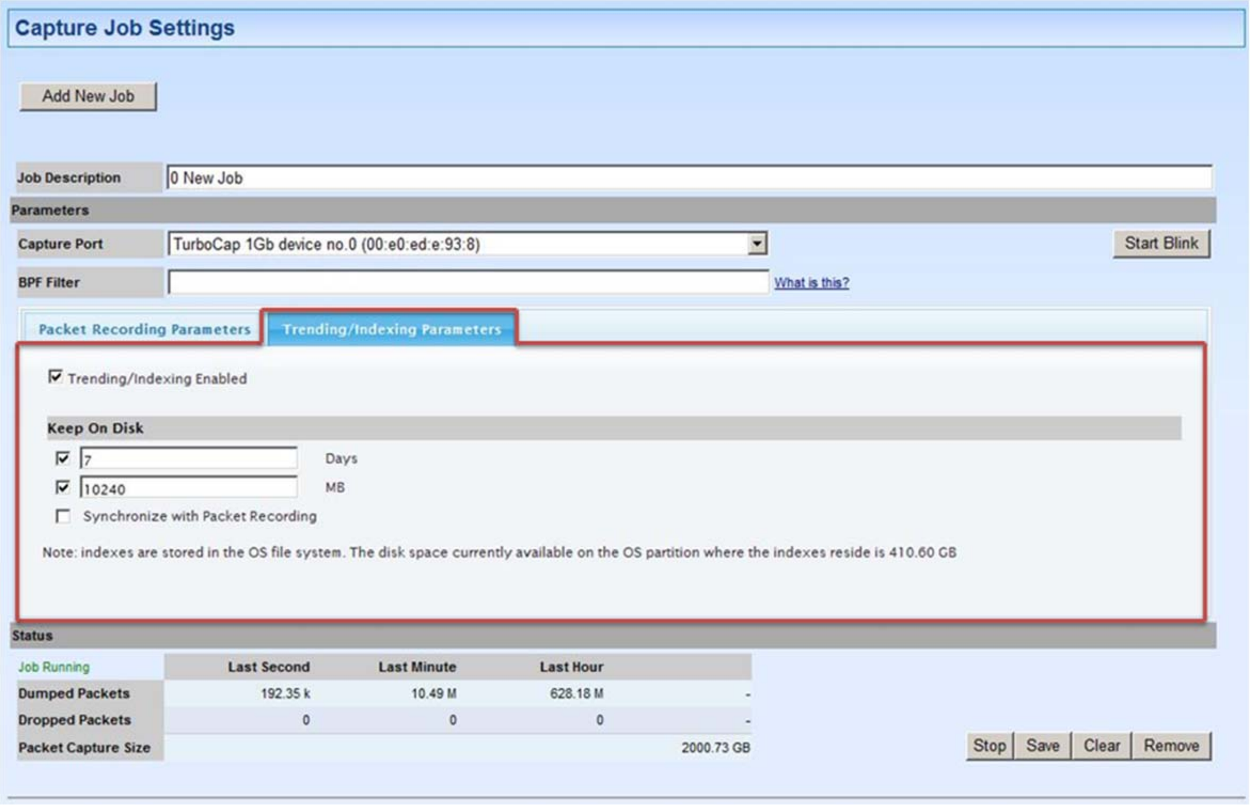
- *Job Description* is used to provide a descriptive name for the Capture Job and helps identify the Capture Job in the Cascade Pilot Devices and Files source panels.
- *Capture Port* shows the available network interfaces. The Capture Job takes traffic from the selected interface and records it to disk.
- *Start Blink* is used to quickly identify the hardware capture port on the Cascade Shark appliance by flashing the LED on the interface.
- *BPF filte*r can be provided to select a subset of the traffic for capturing. For example, the BPF filter `src host 172.18.5.4` captures only the packets with source IP address `172.18.5.4`.
- *Packet Portion to Capture* puts an upper bound on the number of bytes saved for each packet (the snaplen). The default value of 65535 captures the entire packet.

- The settings that affect the Start/Stop criteria for a Capture Job are:
  - **Absolute Start/Stop**: These fields specify absolute starting and stopping times for the job.
  - **Keep On Disk**: These fields limit the maximum amount of storage used by the Capture Job. They can be specified in terms of storage (either in megabytes or a percentage of the total packet store), a maximum number of packets, and/or a maximum time interval of packets. After the limit is reached, the oldest packets are discarded as new packets arrive.
  - **Stop Capturing After**: These fields specify conditions for stopping the job based on the consumed storage (in megabytes or a percentage of the total packet store), the number of packets, or the duration of the capture.

Note: When multiple conditions are selected, the most restrictive condition is the controlling condition. For example, if stop conditions for both the absolute stop time and a maximum number of captured packets are selected, then the first condition to be satisfied stops the capture job.

Trending/Indexing parameters

There are a number of trending/indexing parameters that need to be set when creating a Capture Job, as shown in Figure 88.



Job Description: 0 New Job

Parameters

Capture Port: TurboCap 1Gb device no.0 (00:e0:ed:e:93:8)

BPF Filter:

☑ Trending/Indexing Enabled

Keep On Disk

☑ 7 Days

☑ 10240 MB

☐ Synchronize with Packet Recording

Note: indexes are stored in the OS file system. The disk space currently available on the OS partition where the indexes reside is 410.60 GB

Status

Job Running	Last Second	Last Minute	Last Hour	
Dumped Packets	192.35 k	10.49 M	628.18 M	-
Dropped Packets	0	0	0	-
Packet Capture Size				2000.73 GB

Figure 88: Trending/Indexing Parameters

The following is a *simplified* version of the underlying computation performed by the Shark appliance when the Trending/Indexing feature is enabled.

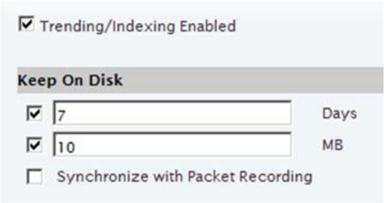
For each packet, the *Conversation Identifier* consists of the 5-tuple:

1. Source IP address
2. Source Port
3. Destination IP address
4. Destination Port
5. IP Protocol

When the Trending/Indexing feature is enabled, the Cascade Shark appliance computes the total bytes and number of packets for each unique conversation identifier in the traffic stream for each second. This information is stored in a file and is referred to as *Trending/Indexing data.*

The Trending/Indexing data is all that is needed to compute many of the View metrics associated with the traffic stream. For example, Bandwidth Over Time, Network Usage By Traffic Type, IP Conversations, and Protocol Distribution are just a few of the Views that can take advantage of the existence of Trending/Indexing data.

Parameters



☑ Trending/Indexing Enabled

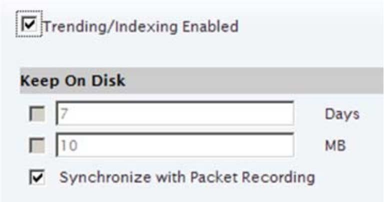
Keep On Disk

☑ 7 Days

☑ 10 MB

□ Synchronize with Packet Recording

Figure 89: Trending/Indexing Enabled



☑ Trending/Indexing Enabled

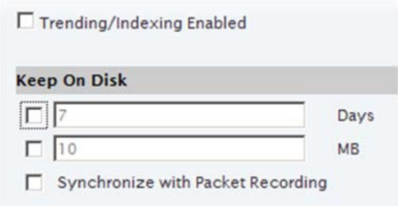
Keep On Disk

□ 7 Days

□ 10 MB

☑ Synchronize with Packet Recording

Figure 90: Synchronized Trending



□ Trending/Indexing Enabled

Keep On Disk

□ 7 Days

□ 10 MB

□ Synchronize with Packet Recording

Figure 91: Trending/Indexing Disabled

- Trending/Indexing Enabled – With the **Trending/Indexing Enabled** checkbox selected and the **Synchronize** checkbox not selected, the Keep on Disk parameters control the size and duration of the Conversation Index.
  - If the Days checkbox is selected, then the duration of the Trending/Indexing data is limited in duration by the number of days entered in the field
  - If the MB checkbox is selected, then the size in megabytes of the Trending/Indexing data is bounded by the value in the MB field.

  Note: The duration of Trending/Indexing is typically set to be significantly longer than the duration of the Packet Recording since it consumes much less storage.

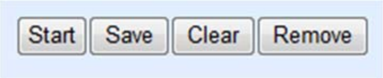
- Synchronized Trending/Indexing – When both **Trending** and **Synchronize with Packet Recording** are selected, then the duration of the Trending/Indexing data is kept synchronized with the duration of the corresponding Capture Job. This ensures that all views (both those that use only the index and those that require the packet data) are available for the same time period, although it likely limits the amount of index that can be retained.

- No Trending/Indexing – If the **Trending/Indexing Enabled** checkbox is not selected, then the Trending/Indexing data are not created for this Capture Job. In general, disabling indexing is not recommended, and this should be done only in cases where the index computation impacts the performance of the packet capture.

Note: The Capture Job Recording is stored in the Packet Storage and the Trending/Indexing data are stored on the OS File System storage.

Capture Job control buttons

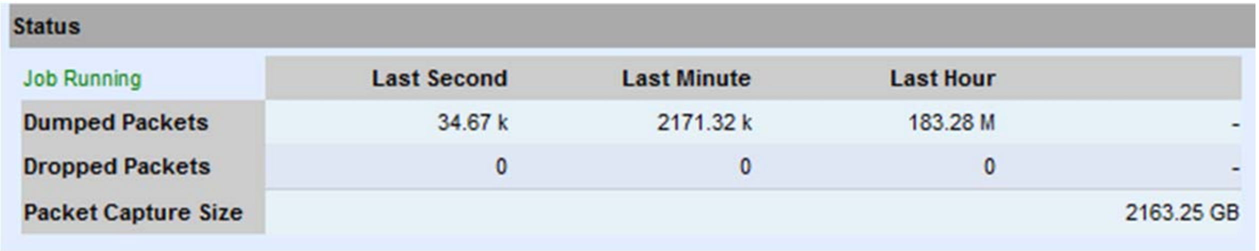
There are four buttons that are used to control a Capture Job.



Buttons 1: Capture Job Control Buttons

- **Start/Stop**: If the Capture Job is running then the **Stop** button stops the job, and if it is not running then the **Start** button starts it. When a Capture Job is stopped both the packet recording and the calculation of the Trending/Indexing data are stopped.
- **Save**: After the parameters of a Capture Job have been edited, they can be saved using the **Save** button. The parameters are also automatically saved when the user clicks the **Start** button to start the job.
- **Clear**: The **Clear** button removes all the data associated with the Capture Job, including the Packet Recording and the Trending/Indexing data storage. This should be used only when the Capture Job is in the Stopped state. The definition and configuration of the job remain and the job can be restarted later.
- **Remove**: The **Remove** button removes all of the data and configuration associated with the Capture Job. The **Remove** button should be used only when the Capture Job is in the Stopped state.

Figure 92 shows a configured Capture Job that is running as indicated by the status display. The page also shows statistics regarding the number of Dumped (Captured) and Dropped Packets for the last second, minute, and hour. The Packet Capture Size shows the amount of storage currently used by the Capture Job.



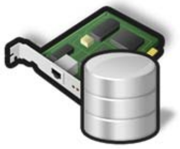
Status

Job Running	Last Second	Last Minute	Last Hour	
Dumped Packets	34.67 k	2171.32 k	183.28 M	-
Dropped Packets	0	0	0	-
Packet Capture Size				2163.25 GB

Figure 92: Managing a Capture Job

Capture Jobs in the Cascade Pilot Devices panel

Each Capture Job appears as a *Job Interface* in the Devices panel.



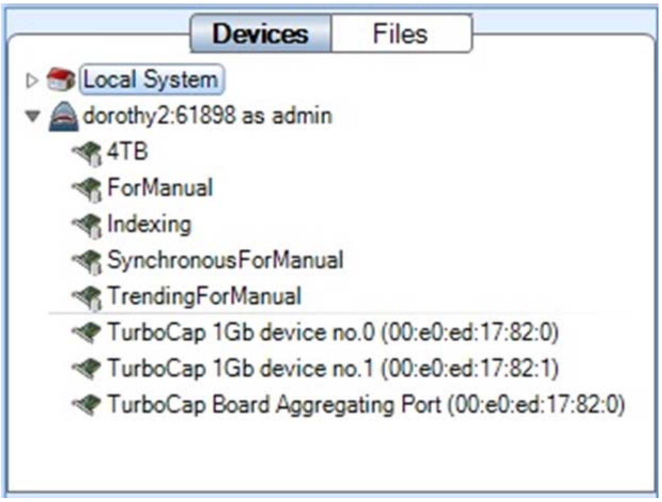
Job Interface icon

Each Capture Job has an associated live interface, which corresponds to the Capture Port of the Job. When a Capture Job is created, an icon appears in the Devices panel representing the Job Interface. The name of the interface is the same as the name of the Capture Job.

Figure 93 shows five Job Interfaces:

- 4TB
- ForManual
- NoIndexing
- SynchronousForManual
- TrendingForManual

These interfaces behave as ordinary live traffic sources. The actual physical interface corresponds to the Capture Port setting in the corresponding Capture Job.



- Local System
- dorothy2:61898 as admin
  - 4TB
  - ForManual
  - Indexing
  - SynchronousForManual
  - TrendingForManual
  - TurboCap 1Gb device no.0 (00:e0:ed:17:82:0)
  - TurboCap 1Gb device no.1 (00:e0:ed:17:82:1)
  - TurboCap Board Aggregating Port (00:e0:ed:17:82:0)

Figure 93: Job Interface in Devices panel

Cascade Pilot Operations on Job Interfaces

All the operations that are available for live interfaces can be applied to a Capture Job Interface.

Capture Jobs in the Cascade Pilot Files panel

The Files panel for a Cascade Shark appliance contains a *Jobs Repository Folder*. The Jobs Repository folder contains a *Job Trace* for each Capture Job. The Job Trace has the same name as the Capture Job and represents the network traffic recording. Each Job Trace has an associated icon that represents the extent to which the Trending/Indexing data is available, as follows.

Job Trace without Trending/Indexing

Denotes a Capture Job without Trending/Indexing data

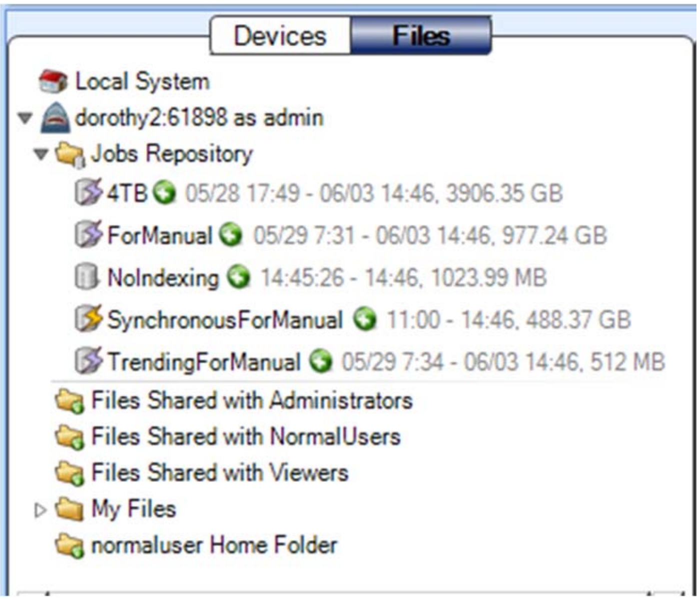
Job Trace with Trending/Indexing

Denotes a Capture Job with Trending/Indexing enabled in which the Trending/Indexing data and the Job Trace packet recording durations are the same.

Job Trace with Mixed Trending/Indexing

Denotes a Capture Job with Trending/Indexing enabled, but for which the duration of Trending/Indexing data duration is longer than the duration of the Job Trace recording.

Figure 94 shows the contents of the Jobs Repository folder in the Devices Panel of Cascade Pilot. It contains five Job Traces with varying options for Trending/Indexing as shown by the icons.



Devices | Files

- Local System
- dorothy2:61898 as admin
  - Jobs Repository
    - 4TB 05/28 17:49 - 06/03 14:46, 3906.35 GB
    - ForManual 05/29 7:31 - 06/03 14:46, 977.24 GB
    - NoIndexing 14:45:26 - 14:46, 1023.99 MB
    - SynchronousForManual 11:00 - 14:46, 488.37 GB
    - TrendingForManual 05/29 7:34 - 06/03 14:46, 512 MB
  - Files Shared with Administrators
  - Files Shared with NormalUsers
  - Files Shared with Viewers
  - My Files
  - normaluser Home Folder

Figure 94: Jobs Repository folder in the Files panel

Cascade Pilot Operations on Job Traces – Trace Clips

It is not unusual for a Job Trace to be multiple terabytes in size, making direct operations inefficient and slow. These potentially massive network traffic recordings can be divided into time intervals within a Job Trace that are called Trace Clips. There are a number of simple and visually oriented ways in which Trace Clips can be created using the Cascade Pilot. Trace Clips do not require any additional storage and behave exactly like ordinary trace files.

A Trace Clip identifies a time interval within a Job Trace. Trace Clips are found in the Files panel and located under the corresponding Job Trace. They are identified by the icons shown below.

Trace Clip

Trace Clip with packets and no Trending/Indexing data

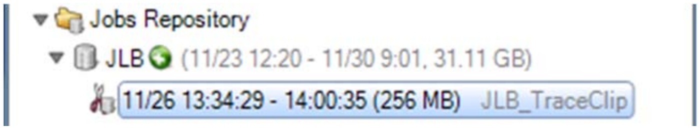
Trace Clip with Index

Trace Clip with packets and Trending/Indexing data available throughout the time interval

Trace Clip with Trending

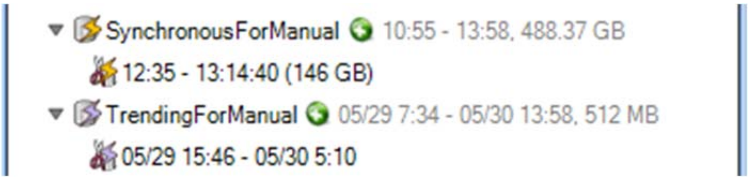
Trace Clip with packets for some or none of the interval, and Trending/Indexing data throughout the interval

Figure 95 shows a Trace Clip named JLB_TraceClip for which there is no Trending/Indexing data available. Figure 96 shows two trace clips that have associated Trending/Indexing data.



Jobs Repository
JLB (11/23 12:20 - 11/30 9:01, 31.11 GB)
11/26 13:34:29 - 14:00:35 (256 MB) JLB_TraceClip

Figure 95: Trace Clip for JLB

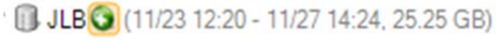


SynchronousForManual 10:55 - 13:58, 488.37 GB
12:35 - 13:14:40 (146 GB)
TrendingForManual 05/29 7:34 - 05/30 13:58, 512 MB
05/29 15:46 - 05/30 5:10

Figure 96: Trace Clips with Trending and Indexes

Creating Trace Clips

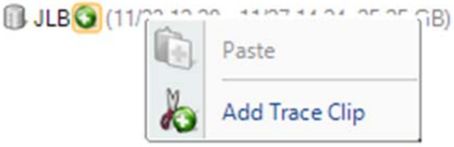
There are two ways to display the Time Control panel for creating a Trace Clip.



JLB (11/23 12:20 - 11/27 14:24, 25.25 GB)

Figure 97: Creating a Trace Clip

Figure 97 shows the Job Trace named JLB. Clicking the **plus** icon to the right of the name displays the Time Control panel shown in Figure 99.



JLB (11/...GB)

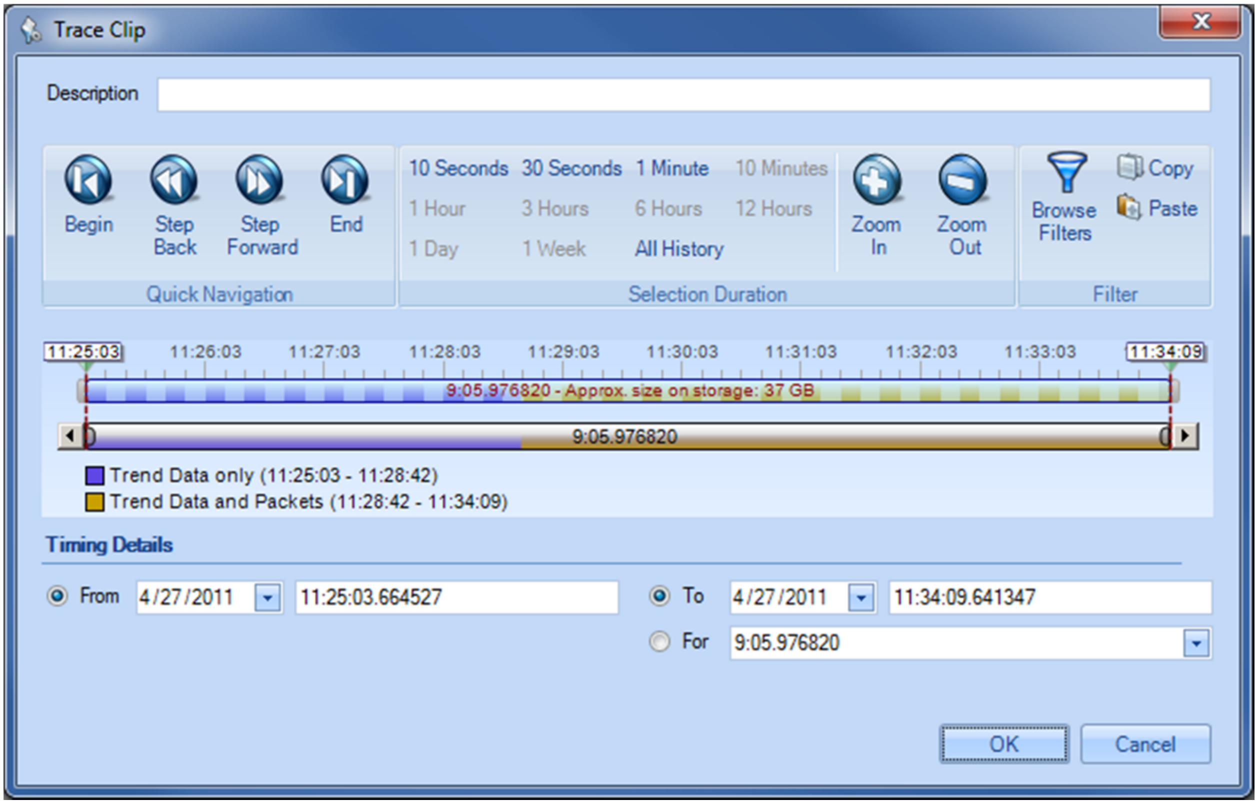
Figure 98: Add a Trace Clip

Right clicking the **Job Trace** displays a context menu (Figure 98) with the menu item Add Trace Clip. Selecting this menu item displays the Time Control Panel.

A Trace Clip identifies a time interval within a Job Trace. If the clipboard contains a time interval, then the Paste menu item can be used to create a Trace Clip corresponding to the time interval on the clipboard.

Time Control panel for creating Trace Clips

It is also possible to create trace clips using the time control panel of Cascade Pilot. Figure 99 shows the Time Control panel for creating a Trace Clip. This is the process of selecting a time interval (time filter) and an optional filter (see the Browse Filters button in the upper-right side of the panel). The Trace Clip can be named using the Description text field. The rest of the options in the Time Control panel provide various ways of selecting a time interval and optional filter. After the selections are made, clicking **OK** creates a Trace Clip corresponding to the selections.



🟪 Trend Data only (11:25:03 - 11:28:42)
🟨 Trend Data and Packets (11:28:42 - 11:34:09)

● From 4/27/2011 11:25:03.664527

● To 4/27/2011 11:34:09.641347

○ For 9:05.976820

Figure 99: Time Control panel for creating Trace Clips

There are multiple ways to create a Trace Clip using the Time Control Panel. The most common approach for networking issues identified by a particular onset time is to specify the **From** time in the Timing Details section. Then specify either the **To** time or the **For** duration.

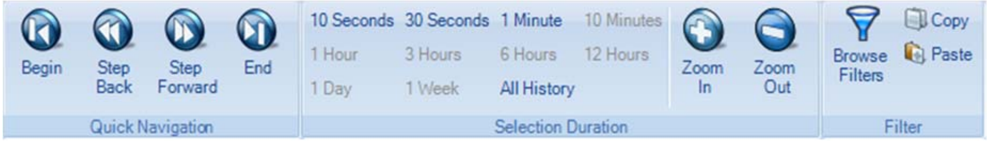


Figure 100: Trace Clip time selection

Another set of options use the multi-level zoom scroll bars to select a time interval. This has the advantage of making it clear whether the selected time interval contains packets and/or trending/indexing data.

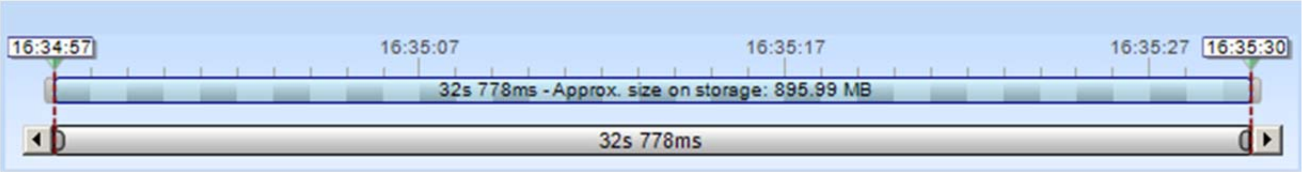


Figure 101: Packets Only

Here, the upper bar is a graphical representation of the duration of the Job Trace, and the lower scroll bar enables zooming in and out over the duration.

In cases where the Job Trace contains both packets and trending/indexing data, the duration of the upper bar represents the *maximum* of the packet capture duration and the duration of the index data. A trace clip can be selected by moving the triangular markers on top on the upper bar.

The following are a series of images representing the various configurations of packets and trending/indexing data.

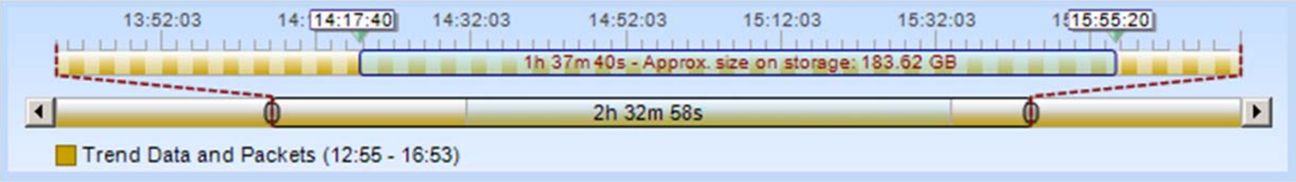

13:52:03
14:
14:17:40
14:32:03
14:52:03
15:12:03
15:32:03
1
15:55:20
1h 37m 40s - Approx. size on storage: 183.62 GB
2h 32m 58s
🟨 Trend Data and Packets (12:55 - 16:53)

Figure 102: Packets plus Trending/Indexing Data

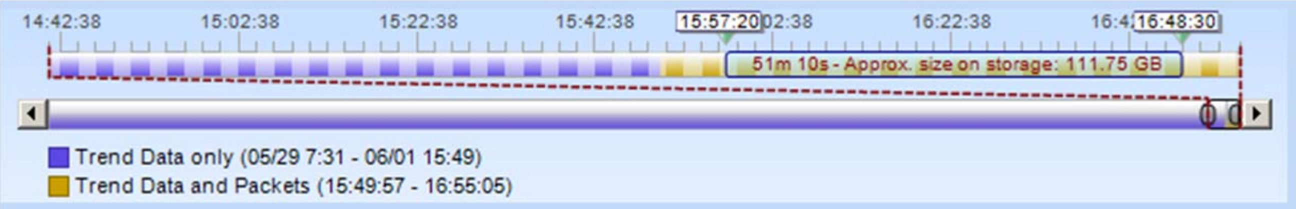

14:42:38
15:02:38
15:22:38
15:42:38
15:57:20
02:38
16:22:38
16:4
16:48:30
51m 10s - Approx. size on storage: 111.75 GB
🟪 Trend Data only (05/29 7:31 - 06/01 15:49)
🟨 Trend Data and Packets (15:49:57 - 16:55:05)

Figure 103: Packets plus Trending/Indexing Data

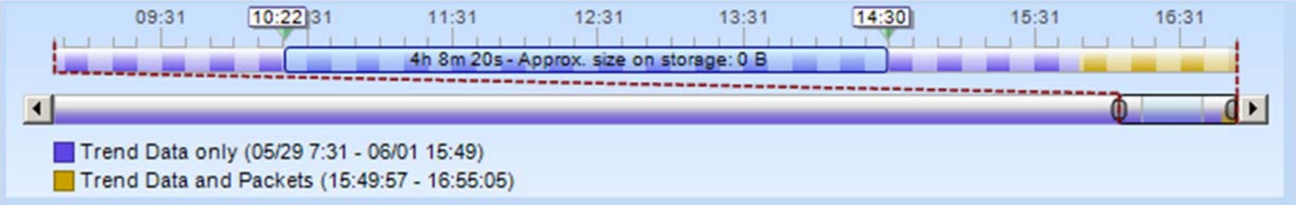

09:31
10:22
31
11:31
12:31
13:31
14:30
15:31
16:31
4h 8m 20s - Approx. size on storage: 0 B
🟪 Trend Data only (05/29 7:31 - 06/01 15:49)
🟨 Trend Data and Packets (15:49:57 - 16:55:05)

Figure 104: Trending/Indexing Data Only

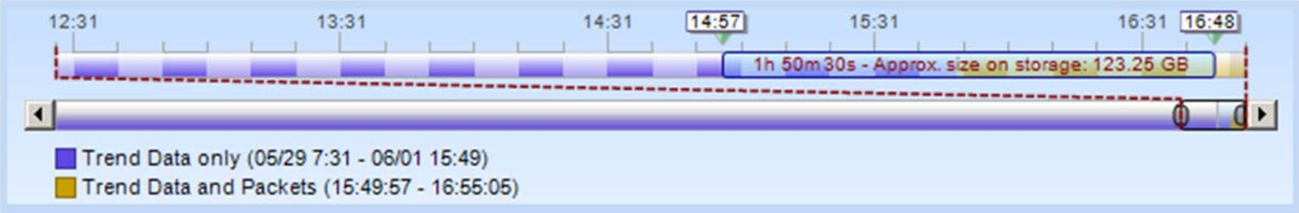

12:31
13:31
14:31
14:57
15:31
16:31
16:48
1h 50m 30s - Approx. size on storage: 123.25 GB
🟪 Trend Data only (05/29 7:31 - 06/01 15:49)
🟨 Trend Data and Packets (15:49:57 - 16:55:05)

Figure 105: Combination Trending/Indexing Data Only and Packets plus Trending/Indexing Data

Figure 106 shows the Browse Filters button that displays the Filter Editor for selecting a filter in addition to the time interval. Thus the Trace Clip not only represents a time interval, but also contains a packet filter. It is important to select a filter that is compatible with the trending/indexing data.

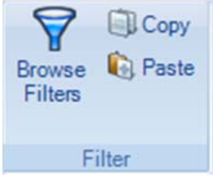
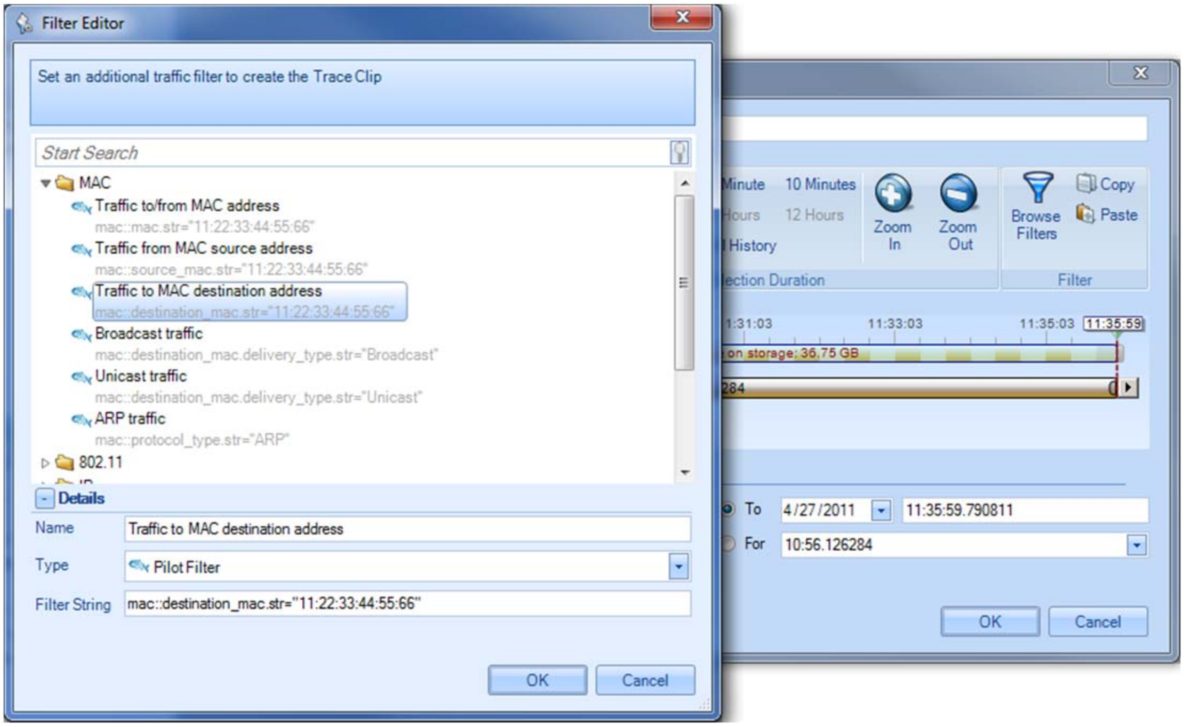


Figure 106: Show Filter Editor

Figure 107 shows the Filter Editor. Note that nearly all of the filters in the default set are Trending/Indexing-compatible Pilot Filters.


Filter Editor

Set an additional traffic filter to create the Trace Clip

Start Search

- MAC
  - Traffic to/from MAC address
    mac::mac.str="11:22:33:44:55:66"
  - Traffic from MAC source address
    mac::source_mac.str="11:22:33:44:55:66"
  - Traffic to MAC destination address
    mac::destination_mac.str="11:22:33:44:55:66"
  - Broadcast traffic
    mac::destination_mac.delivery_type.str="Broadcast"
  - Unicast traffic
    mac::destination_mac.delivery_type.str="Unicast"
  - ARP traffic
    mac::protocol_type.str="ARP"
- 802.11

Details

Name: Traffic to MAC destination address

Type: Pilot Filter

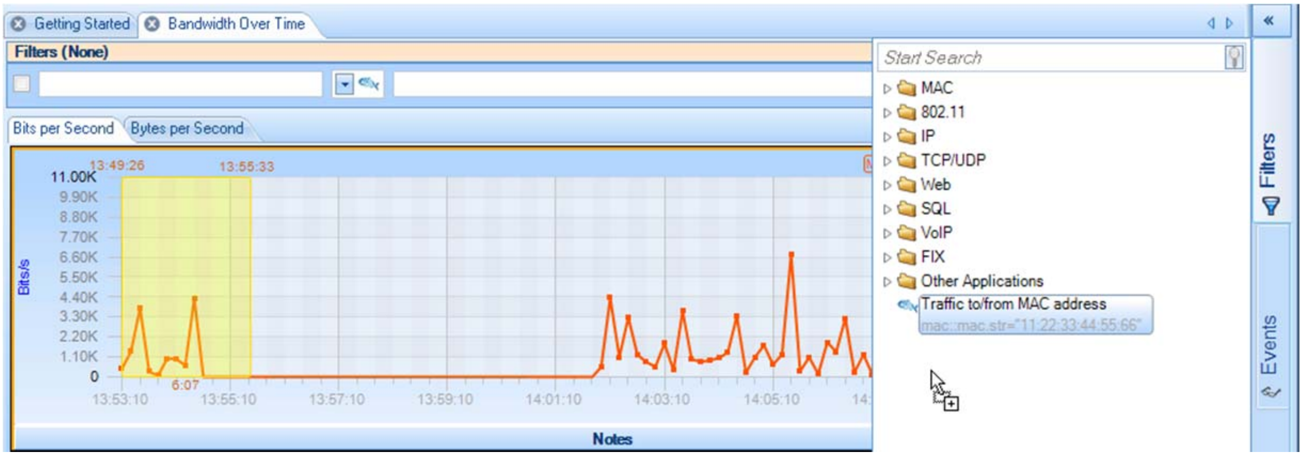
Filter String: mac::destination_mac.str="11:22:33:44:55:66"

To: 4/27/2011 11:35:59.790811

For: 10:56.126284

Figure 107: Filter Editor

You can also drag a selection from the chart area to the Filter panel to create an entry in the filter collection. Drag the selection to the Filter tab to open the panel and drop the selection, as shown in Figure 107.



Start Search

- MAC
- 802.11
- IP
- TCP/UDP
- Web
- SQL
- VoIP
- FIX
- Other Applications
- Traffic to/from MAC address
  mac::mac.str="11:22:33:44:55:66"

Figure 108: Time Selection dragged to Filter panel to create an entry

Using Time Selection to create a Trace Clip

Figure 109 shows a time selection in a strip chart. The strip chart was obtained by applying the Bandwidth Over Time view to the JLB Job Interface. Figure 110 switches from the Devices panel to the Files panel, showing the corresponding JLB Job Trace. The trace clip was created by clicking and dragging the selected time interval (in the strip chart) over the Job Trace. This automatically created the Trace Clip shown below the JLB Job Trace. Note that the Job Trace is over 30 GB, but the Trace Clip is only 256 MB.

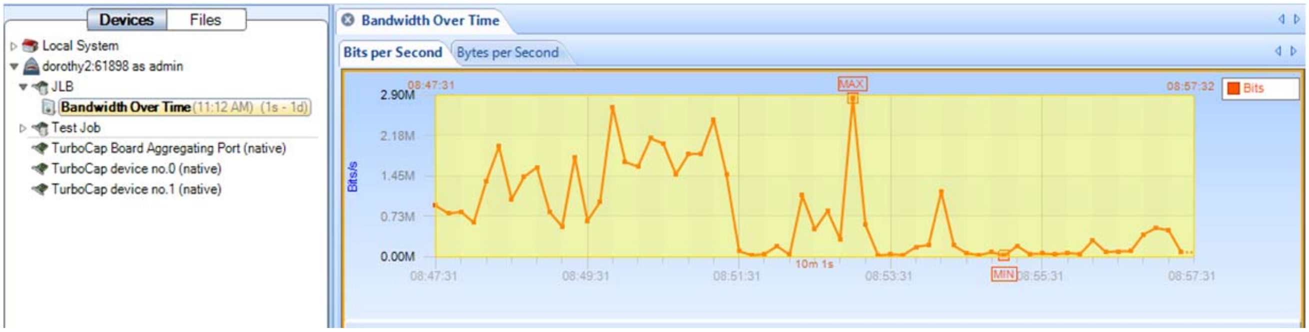


Figure 109: Time Selection in a Strip Chart

In Figure 110 the Bandwidth Over Time view is applied to the Trace Clip below JLB. Note the similarity to the view in Figure 109.

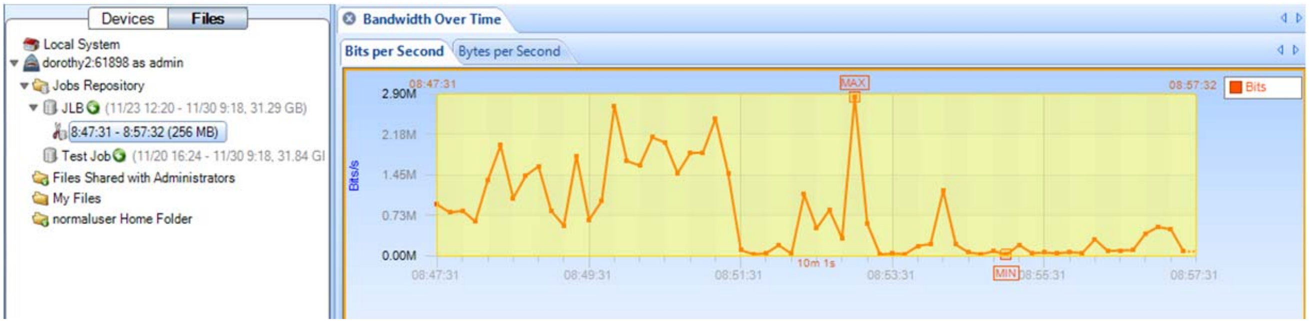


Figure 110: Time Selection dragged over Job Trace to create a Trace Clip

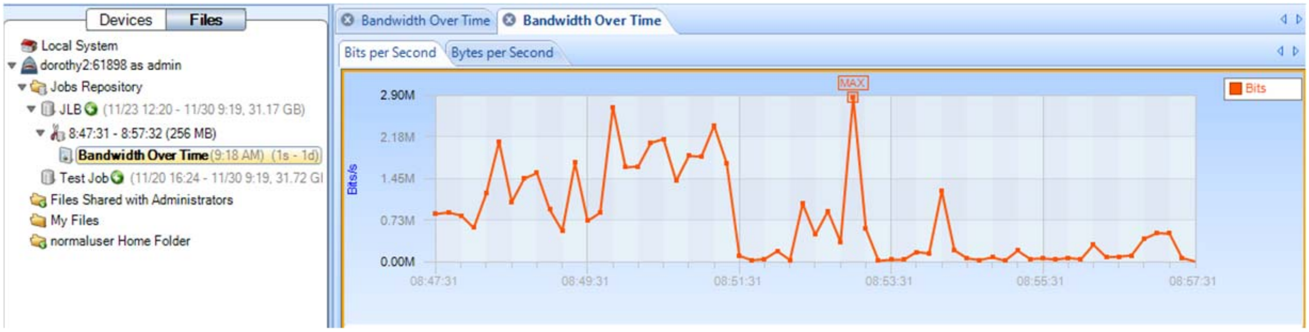


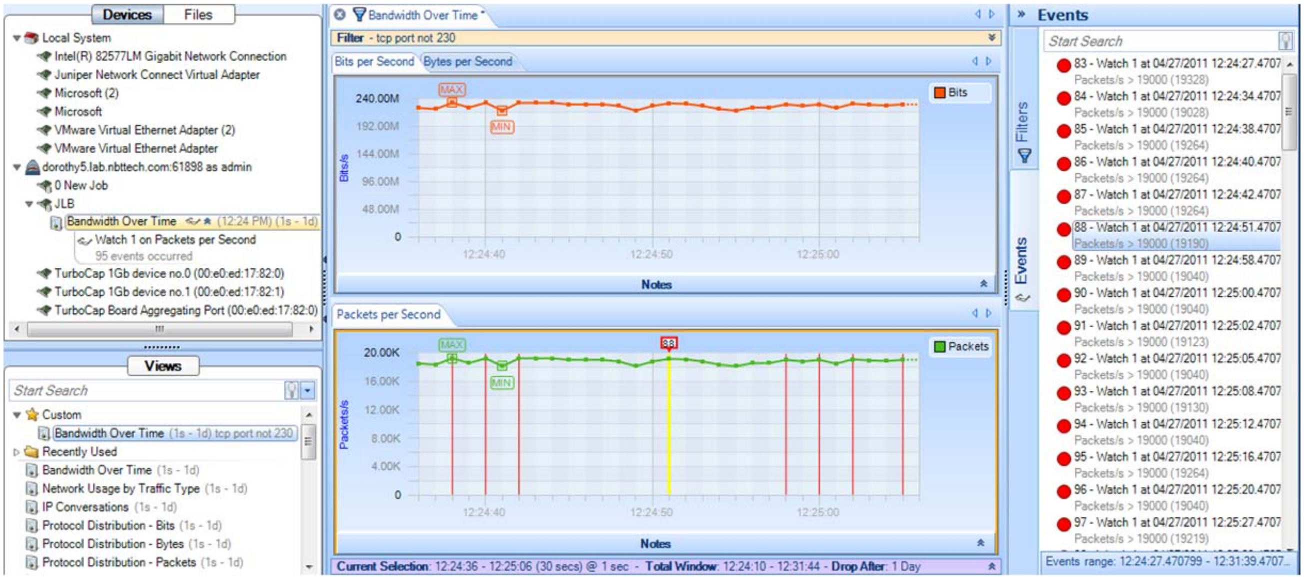
Figure 111: View applied to a Trace Clip

Note: The view in Figure 34 was obtained through the analysis of a live source, while the view in Figure 35 was obtained by applying the same analysis to the packets saved in the Trace Clip. Trace Clips have all of the properties of ordinary trace files and can be analyzed using all of the capabilities of Cascade Pilot.

Using Events to create Trace Clips

It is important to be able to easily isolate network traffic associated with an event for troubleshooting and diagnostics. This is easily accomplished by dragging the event in question over the Job Trace. A Trace Clip is automatically created that contains traffic occurring before and after the event.

Figure 112 shows the Event List and a particular event (88) that has been highlighted both in the Event List and on the Strip Chart. The events were created using a Watch on the live traffic corresponding to the JLB Capture Job. Creating a Trace Clip around the (temporal) location of the event is as easy as dragging the event from the Event List to the JLB Job Trace. Dragging Event 88 from the Event List and dropping it on the JLB Job Trace displays the Time Control panel for creating the Trace Clip. See Figure 113.


Devices
Files
Local System
Intel(R) 82577LM Gigabit Network Connection
Juniper Network Connect Virtual Adapter
Microsoft (2)
Microsoft
VMware Virtual Ethernet Adapter (2)
VMware Virtual Ethernet Adapter
dorothy5.lab.nbttech.com:61898 as admin
0 New Job
JLB
Bandwidth Over Time (12:24 PM) (1s - 1d)
Watch 1 on Packets per Second
95 events occurred
TurboCap 1Gb device no.0 (00:e0:ed:17:82:0)
TurboCap 1Gb device no.1 (00:e0:ed:17:82:1)
TurboCap Board Aggregating Port (00:e0:ed:17:82:0)
Views
Start Search
Custom
Bandwidth Over Time (1s - 1d) tcp port not 230
Recently Used
Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)
IP Conversations (1s - 1d)
Protocol Distribution - Bits (1s - 1d)
Protocol Distribution - Bytes (1s - 1d)
Protocol Distribution - Packets (1s - 1d)
Bandwidth Over Time
Bits per Second
Bytes per Second
Bits/s
240.00M
192.00M
144.00M
96.00M
48.00M
0
MAX
MIN
Bits
12:24:40
12:24:50
12:25:00
Notes
Packets per Second
Packets/s
20.00K
16.00K
12.00K
8.00K
4.00K
0
88
Packets
Filters
Events
Start Search

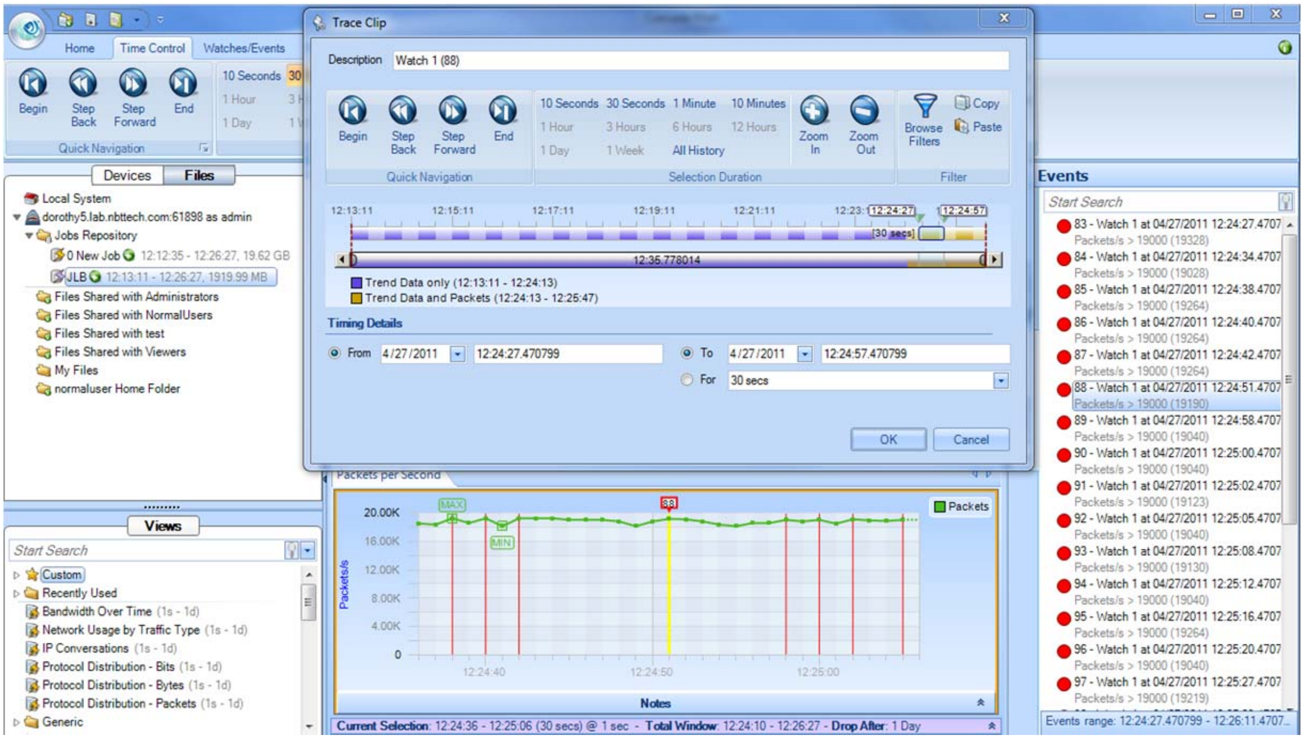
Filter - tcp port not 230

83 - Watch 1 at 04/27/2011 12:24:27.4707
Packets/s > 19000 (19328)
84 - Watch 1 at 04/27/2011 12:24:34.4707
Packets/s > 19000 (19028)
85 - Watch 1 at 04/27/2011 12:24:38.4707
Packets/s > 19000 (19264)
86 - Watch 1 at 04/27/2011 12:24:40.4707
Packets/s > 19000 (19264)
87 - Watch 1 at 04/27/2011 12:24:42.4707
Packets/s > 19000 (19264)
88 - Watch 1 at 04/27/2011 12:24:51.4707
Packets/s > 19000 (19190)
89 - Watch 1 at 04/27/2011 12:24:58.4707
Packets/s > 19000 (19040)
90 - Watch 1 at 04/27/2011 12:25:00.4707
Packets/s > 19000 (19040)
91 - Watch 1 at 04/27/2011 12:25:02.4707
Packets/s > 19000 (19123)
92 - Watch 1 at 04/27/2011 12:25:05.4707
Packets/s > 19000 (19040)
93 - Watch 1 at 04/27/2011 12:25:08.4707
Packets/s > 19000 (19130)
94 - Watch 1 at 04/27/2011 12:25:12.4707
Packets/s > 19000 (19040)
95 - Watch 1 at 04/27/2011 12:25:16.4707
Packets/s > 19000 (19264)
96 - Watch 1 at 04/27/2011 12:25:20.4707
Packets/s > 19000 (19040)
97 - Watch 1 at 04/27/2011 12:25:27.4707
Packets/s > 19000 (19219)

Current Selection: 12:24:36 - 12:25:06 (30 secs) @ 1 sec - Total Window: 12:24:10 - 12:31:44 - Drop After: 1 Day

Events range: 12:24:27.470799 - 12:31:39.4707...

Figure 112: Event List



Description: Watch 1 (88)

🟦 Trend Data only (12:13:11 - 12:24:13)
🟨 Trend Data and Packets (12:24:13 - 12:25:47)

Timing Details

● From 4/27/2011 12:24:27.470799
● To 4/27/2011 12:24:57.470799
○ For 30 secs

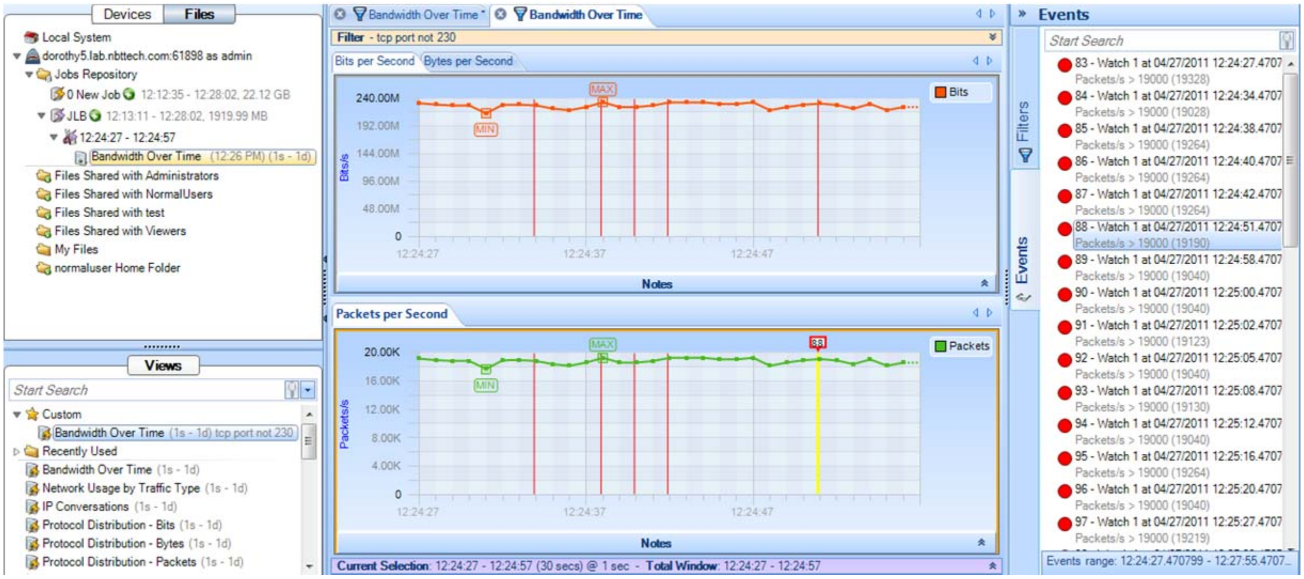
83 - Watch 1 at 04/27/2011 12:24:27.4707
Packets/s > 19000 (19328)
84 - Watch 1 at 04/27/2011 12:24:34.4707
Packets/s > 19000 (19028)
85 - Watch 1 at 04/27/2011 12:24:38.4707
Packets/s > 19000 (19264)
86 - Watch 1 at 04/27/2011 12:24:40.4707
Packets/s > 19000 (19264)
87 - Watch 1 at 04/27/2011 12:24:42.4707
Packets/s > 19000 (19264)
88 - Watch 1 at 04/27/2011 12:24:51.4707
Packets/s > 19000 (19190)
89 - Watch 1 at 04/27/2011 12:24:58.4707
Packets/s > 19000 (19040)
90 - Watch 1 at 04/27/2011 12:25:00.4707
Packets/s > 19000 (19040)
91 - Watch 1 at 04/27/2011 12:25:02.4707
Packets/s > 19000 (19123)
92 - Watch 1 at 04/27/2011 12:25:05.4707
Packets/s > 19000 (19040)
93 - Watch 1 at 04/27/2011 12:25:08.4707
Packets/s > 19000 (19130)
94 - Watch 1 at 04/27/2011 12:25:12.4707
Packets/s > 19000 (19040)
95 - Watch 1 at 04/27/2011 12:25:16.4707
Packets/s > 19000 (19264)
96 - Watch 1 at 04/27/2011 12:25:20.4707
Packets/s > 19000 (19040)
97 - Watch 1 at 04/27/2011 12:25:27.4707
Packets/s > 19000 (19219)

Current Selection: 12:24:36 - 12:25:06 (30 secs) @ 1 sec - Total Window: 12:24:10 - 12:26:27 - Drop After: 1 Day

Events range: 12:24:27.470799 - 12:26:11.4707...

Figure 113: Creating a Trace Clip from an Event

The Time Control panel can be used to enlarge or shrink the time interval of the Trace Clip around the event. The Trace Clip is shown in Figure 114.


Devices
Files
Local System
dorothy5.lab.nbttech.com:61898 as admin
Jobs Repository
0 New Job 12:12:35 - 12:28:02, 22.12 GB
JLB 12:13:11 - 12:28:02, 1919.99 MB
12:24:27 - 12:24:57
Bandwidth Over Time (12:26 PM) (1s - 1d)
Files Shared with Administrators
Files Shared with NormalUsers
Files Shared with test
Files Shared with Viewers
My Files
normaluser Home Folder
Views
Start Search
Custom
Bandwidth Over Time (1s - 1d) tcp port not 230
Recently Used
Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)
IP Conversations (1s - 1d)
Protocol Distribution - Bits (1s - 1d)
Protocol Distribution - Bytes (1s - 1d)
Protocol Distribution - Packets (1s - 1d)
Bandwidth Over Time *
Bandwidth Over Time
Bits per Second
Bytes per Second
240.00M
192.00M
144.00M
96.00M
48.00M
0
Bits/s
MAX
MIN
Bits
12:24:27
12:24:37
12:24:47
Notes
Packets per Second
20.00K
16.00K
12.00K
8.00K
4.00K
0
Packets/s
MAX
MIN
88
Packets
12:24:27
12:24:37
12:24:47
Notes
Filters
Events
Events
Start Search

Filter - tcp port not 230

Current Selection: 12:24:27 - 12:24:57 (30 secs) @ 1 sec - Total Window: 12:24:27 - 12:24:57

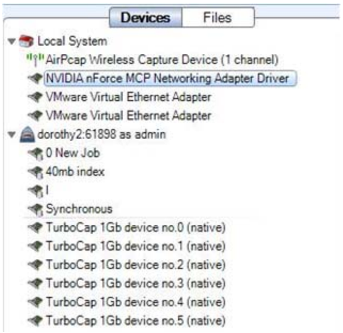
83 - Watch 1 at 04/27/2011 12:24:27.4707
Packets/s > 19000 (19328)
84 - Watch 1 at 04/27/2011 12:24:34.4707
Packets/s > 19000 (19028)
85 - Watch 1 at 04/27/2011 12:24:38.4707
Packets/s > 19000 (19264)
86 - Watch 1 at 04/27/2011 12:24:40.4707
Packets/s > 19000 (19264)
87 - Watch 1 at 04/27/2011 12:24:42.4707
Packets/s > 19000 (19264)
88 - Watch 1 at 04/27/2011 12:24:51.4707
Packets/s > 19000 (19190)
89 - Watch 1 at 04/27/2011 12:24:58.4707
Packets/s > 19000 (19040)
90 - Watch 1 at 04/27/2011 12:25:00.4707
Packets/s > 19000 (19040)
91 - Watch 1 at 04/27/2011 12:25:02.4707
Packets/s > 19000 (19123)
92 - Watch 1 at 04/27/2011 12:25:05.4707
Packets/s > 19000 (19040)
93 - Watch 1 at 04/27/2011 12:25:08.4707
Packets/s > 19000 (19130)
94 - Watch 1 at 04/27/2011 12:25:12.4707
Packets/s > 19000 (19040)
95 - Watch 1 at 04/27/2011 12:25:16.4707
Packets/s > 19000 (19264)
96 - Watch 1 at 04/27/2011 12:25:20.4707
Packets/s > 19000 (19040)
97 - Watch 1 at 04/27/2011 12:25:27.4707
Packets/s > 19000 (19219)

Events range: 12:24:27.470799 - 12:27:55.4707...

Figure 114: Trace Clip corresponding to an Event

Sources Panel

The Sources Panel has two tabs: Devices and Files.



- Local System
  - AirPcap Wireless Capture Device (1 channel)
  - NVIDIA nForce MCP Networking Adapter Driver
  - VMware Virtual Ethernet Adapter
  - VMware Virtual Ethernet Adapter
- dorothy2:61898 as admin
  - 0 New Job
  - 40mb index
  - I
  - Synchronous
  - TurboCap 1Gb device no.0 (native)
  - TurboCap 1Gb device no.1 (native)
  - TurboCap 1Gb device no.2 (native)
  - TurboCap 1Gb device no.3 (native)
  - TurboCap 1Gb device no.4 (native)
  - TurboCap 1Gb device no.5 (native)

Figure 115 Sources Panel

The *Sources Panel* contains representations of Shark appliances, live interfaces, trace files, and Capture Jobs and is one of the most important parts of Cascade Pilot.

Clicking the tabs switches between displaying the devices and the trace files.

Devices
: Shows local interfaces under the Local System icon and Shark appliances with their associated interface offering live sources of network traffic to Cascade Pilot.

Files
: Shows local folders and trace files under Local System and Shark appliances with their associated folders and trace files.

Devices

Cascade Pilot supports two basic classes of networking devices:

- Wired Ethernet
- Wireless (802.11)

Wired Ethernet Adapters

Icon 48 Wired Ethernet Adapter

Icon 49: Wired Ethernet Adapter associated with a Capture Job

Most wired Ethernet network interface cards work in Cascade Pilot. There are two types of adapters. One presented by the actual interface -- Icon 48, and one presenting the interface corresponding to a Capture Job -- Icon 49.

Wireless Adapters

Icon 50 Wireless Adapter

Normal wireless adapters in Windows are not designed to do packet capture and analysis. Riverbed Technology AirPcap adapters are made specifically to do packet capture and network analysis and are currently the only wireless adapters supported.

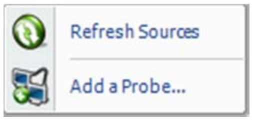
Additionally, multiple AirPcap Adapters are shown as a single device because the wireless adapters share the same airspace and, all adapters being equal, any one adapter can receive the same traffic as any other. Therefore, Cascade Pilot internally breaks up tasks among multiple adapters so that many channels can be scanned and locked without having to worry about which channel a particular physical adapter scans and locks on.

> *Note:* ***Wireless adapters are only available on the local Cascade Pilot system, not on the Shark appliance.***

Context Menus in the Devices Panel

There are five types of *Context Menus* in the Devices panel that will appear under the five conditions below:

With Nothing Selected



Context Menu 1 Devices Panel (No Selection)

With nothing selected, the options are as follows:

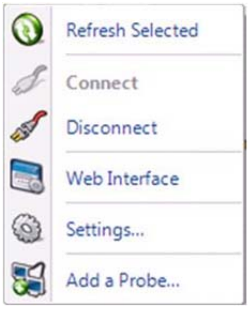
Refresh Sources

The *Refresh Sources* menu option causes Cascade Pilot to rescan the available interfaces on the local system and all connected Shark appliances to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected Shark appliances are rescanned and updated to reflect whether files have been removed or modified.

Add a Probe

The *Add a Probe* menu item opens the Connect to Probe panel.

With a Shark appliance Selected



Context Menu 2 Devices Panel (Shark appliance Selected)

With a Shark appliance selected:

Refresh Selected

The *Refresh Selected* menu option rescans the selected Shark appliance and displays the currently available interfaces. Additionally, the trace folders associated with the selected Shark appliance are rescanned and updated to reflect whether files have been removed or modified.

Disconnect

The *Disconnect* menu option disconnects the selected Shark appliance from Cascade Pilot. The selected Shark appliance remains in the Probes list in the Remote ribbon.

Web Interface

The *Web Interface* menu opens the selected remote probe’s Web Interface Settings.

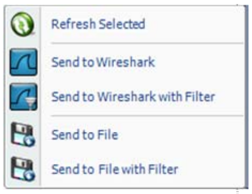
Settings

The *Settings* menu item opens the “Connect to Probe” panel showing the values used to connect to the selected Shark appliance.

Add a Probe

The *Add a Probe* menu item opens the Connect to Probe panel.

With an Interface Selected (Local System or Shark appliance)



Context Menu 3 Devices Panel (Interface Selected)

With an interface selected, the options are as follows:

Refresh Selected

The *Refresh Selected* menu option causes Cascade Pilot to rescan the available interfaces on the local system and all connected Shark appliances to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected Shark appliances are rescanned and updated to reflect whether files have been removed or modified.

Send to Wireshark

The *Send to Wireshark* menu option instructs Cascade Pilot to start up Wireshark and send all traffic from the selected interface to Wireshark.

Send to Wireshark with Filter

The *Send to Wireshark with Filter* menu option instructs Cascade Pilot to start up Wireshark and send traffic that matches a user-defined filter from the selected device to Wireshark. The filter is specified using the *Filter Dialog Box*, which is explained in a later section.

Send to File

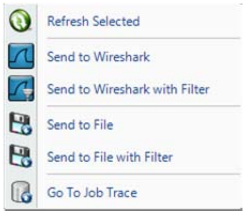
The *Send to File* menu option instructs Cascade Pilot to send all traffic from the selected device to a user-specified trace file.

Send to File with Filter

The *Send to File with Filter* menu option instructs Cascade Pilot to send traffic that matches a user-defined filter from the selected device to a user-specified trace file. The filter is specified using the filter dialog box, which appears first and is explained in a later section.

With a Capture Job Interface Selected (Shark appliance)

Icon 51: Capture Job Interface



Context Menu 4: Capture Job Interface Selected

With a Capture Job interface selected, the options are the same as the previous section, with one additional option to Go To Job Trace. Selecting this option takes the user directly to the corresponding Job Trace in the Jobs Repository folder.

With a View Selected

With a View Selected (Shark appliance and Local System):

Generate Report

The *Generate Report* menu option generates a report from the selected View.

Create Interactive View

The *Create Interactive View* menu option (available only on a drill-down view) generates an Interactive View by connecting charts of one or more views applied via drill-down.

Share the View with

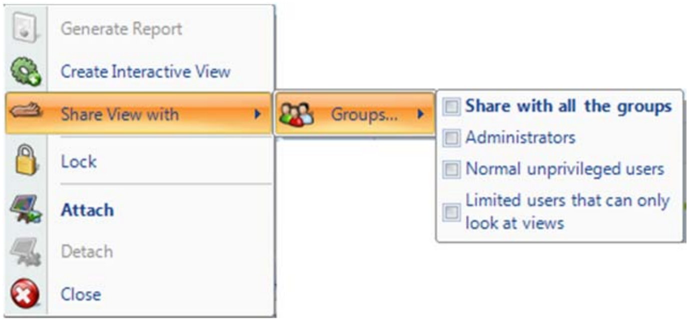
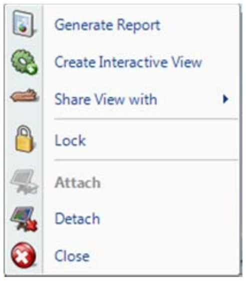


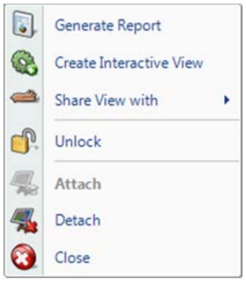
Figure 116 Sharing Views

Views applied to Shark appliance interfaces on one Cascade Pilot can be shared with groups located at other Cascade Pilot instances. The privileges associated with each group are determined on a probe-by-probe basis. Except for the Administrators, a user cannot close a View or delete a file that has been created by another user. However, Views can be shared with single groups using the Share View with menu item. As soon as a View is shared, the selected group will immediately see the View in their Sources Panel.

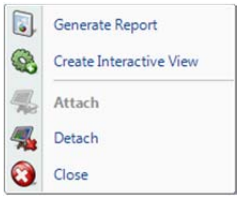
Note: The *Share the View with* menu item only applies to Shark appliances.



Context Menu 5 Unlocked View in the Devices Panel



Context Menu 6 Locked View in the Devices Panel



Context Menu 7 Devices Panel (View Selection, Local System)

Lock

If Lock is selected, then a small padlock image is added to the View icon. When the View is in the "Locked" state, it cannot be closed. When the View is in the "Locked" state, the Context menu shows an Unlock menu item. The View must be "unlocked" before it can be closed.
NOTE: The *Lock* menu item applies to only Shark appliances.

Attach

If the selected View is Detached, then the *Attach* menu item attaches Cascade Pilot to the View.
NOTE: The *Attach* menu item applies to only Shark appliances.

Detach

If the selected View is currently Attached, the *Detach* menu option detaches the selected View.
NOTE: The *Detach* menu item applies to only Shark appliances.

Close

If the user is the creator of the selected View, then the *Close* menu option closes the selected View. This implies that the corresponding Shark appliance will terminate the View and it will no longer be available to other users.

Files

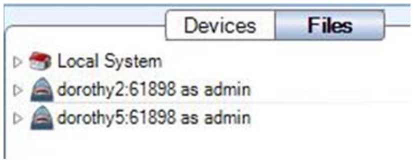
Cascade Pilot can analyze trace files of arbitrary size in the PCAP capture format with the following restrictions:

802.11 Wireless trace files must have either a RadioTap[2] or PPI[3] header.

All wired trace files must have an Ethernet header. For instance, trace files created through software loopback devices, software tunnels, software based aggregators, and from non-Ethernet devices (ex. tun[4], lo[5], ppp[6]) are not readable. In most of these instances, the traffic passing through these interfaces will eventually pass through an Ethernet interface.

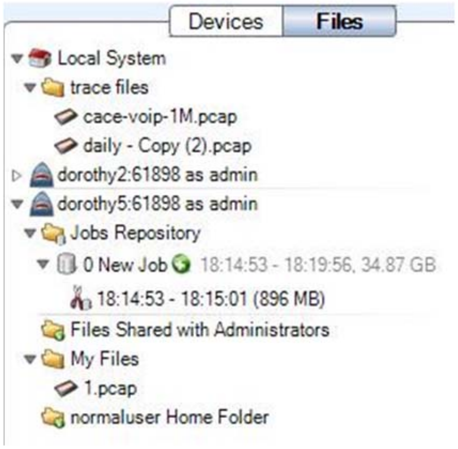
[2] NetBSD: http://netbsd.gw.com/cgi-bin/man-cgi?ieee80211_radiotap+9+NetBSD-current
[3] CACE Technologies: http://www.cacetech.com/documents/PPI_Header_format_1.0.1.pdf
[4] FreeBSD: http://www.freebsd.org/cgi/man.cgi?query=tun&manpath=FreeBSD+7.0-RELEASE&format=html
[5] FreeBSD: http://www.freebsd.org/cgi/man.cgi?query=lo&manpath=FreeBSD+7.0-RELEASE&format=html
[6] FreeBSD: http://www.freebsd.org/cgi/man.cgi?query=ppp&manpath=FreeBSD+7.0-RELEASE&format=html

Capture Jobs running on remote Shark appliances create network traffic recordings called Job Traces. Although Job Traces (and their derivatives, called Trace Clips) are not PCAP files, they can be analyzed by Cascade Pilot exactly as if they were PCAP files. Trace Clips that exist on a Shark appliance can be converted to PCAP format using the Send-to-File feature of Cascade Pilot. The resultant PCAP file will be stored in the Shark appliance's local file system.



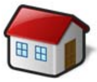
- Local System
- dorothy2:61898 as admin
- dorothy5:61898 as admin

Figure 117: Files Panel (closed)

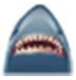


- Local System
  - trace files
    - cace-voip-1M.pcap
    - daily - Copy (2).pcap
- dorothy2:61898 as admin
- dorothy5:61898 as admin
  - Jobs Repository
    - 0 New Job 18:14:53 - 18:19:56, 34.87 GB
      - 18:14:53 - 18:15:01 (896 MB)
  - Files Shared with Administrators
  - My Files
    - 1.pcap
  - normaluser Home Folder

Figure 118: Files Panel (expanded)



Icon 52: Local System



Icon 53: Shark appliance

Icon 54: Jobs Repository

Icon 55: Job Trace

Icon 56: Trace Clip

Icon 57: Trace File (PCAP)

The Files Panel contains an item for the Local System and one for each attached Shark appliance.

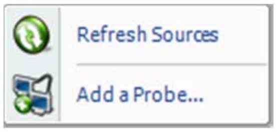
The figures show an example file panel with all the items closed and one with all of the items expanded.

They also show the icons for each type of object depicted in the Files panel

Context Menus in the File Panel

The context menus for the File Panel are described below:

With Nothing or Local System Selected



Context Menu 8 Files Panel (No Selection)

The options are as follows:

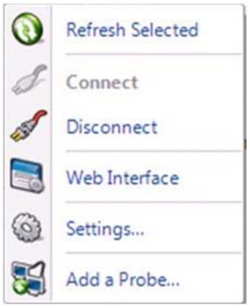
Refresh Sources

The *Refresh Sources* menu option causes Cascade Pilot to rescan the available interfaces on the local system and all connected Shark appliances to display the currently available devices. Additionally, the trace folders associated with the Local System and the connected Shark appliances are rescanned and updated to reflect whether files have been removed or modified.

Add a Probe

The *Add a Probe* menu item opens the Connect to Probe panel.

With a Shark appliance Selected



Context Menu 9 Files Panel (Probe Selected)

The options are as follows:

Refresh Selected

The *Refresh Selected* menu option rescans the selected Shark appliance and displays the currently available interfaces. Additionally, the trace folders associated with the selected Shark appliance are rescanned and updated to reflect whether files have been removed or modified.

Disconnect

The *Disconnect* menu option disconnects the selected Shark appliance from Cascade Pilot and removes it from the Devices and Files panels. The selected Shark appliance remains in the Probes list.

Web Interface

The *Web Interface* menu opens the selected remote probe's Web Interface Settings.

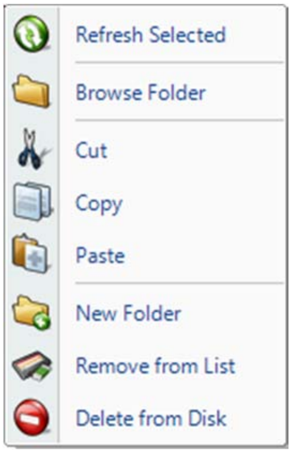
Settings

The *Settings* menu item opens the "Connect to Probe" panel showing the values used to connect to the selected Shark appliance.

Add a Probe

The *Add a Probe* menu item opens the Connect to Probe panel

With A Trace Folder Selected on Local System



Context Menu 10 Files Panel (Trace Folder Selected on Local System)

With a trace folder selected, the options are as follows:

Refresh Selected

The *Refresh Selected* menu option rescans a folder for new trace files and updates the status of those already added.

Browse Folder

The *Browse Folder* menu option opens an explorer window pointed to the selected folder.

Cut

The *Cut* menu option obtains a reference to the “to-be-cut” folder. When the Paste operation is invoked, the folder and its contents are copied to the “paste” location and removed from the original location only if the source and destination are on the same system. If the source and destination are on different systems, then Cut behaves like a Copy operation.

Copy

The *Copy* menu option obtains a reference to the “to-be-copied” folder. When the Paste operation is invoked, the folder is copied to the “paste” location and is NOT removed from the original location.

Paste

The *Paste* menu option copies a previously Cut or Copied file to the selected Paste location.

New Folder

The *New Folder* menu option creates a new folder in the selected one: The user is asked to enter the name of the folder to create.

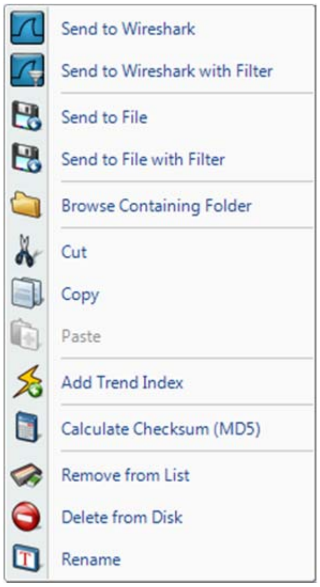
Remove from List

The *Remove from List* menu option removes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

Delete Trace Files

The *Delete Trace Files* menu option irrevocably deletes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

With A Trace File Selected on Local System



Context Menu 11 Files Panel (Trace File Selected on Local System)

With a trace file selected, the options are as follows:

Send to Wireshark

The *Send to Wireshark* menu option starts up Wireshark and sends all traffic from the selected trace file there.

Send to Wireshark with Filter

The *Send to Wireshark with Filter* menu option instructs Cascade Pilot to start up Wireshark and send traffic that matches a user-defined filter from the selected file to Wireshark. The filter is specified using the *Filter Dialog Box,* which is explained in a later section.

Send to File

The *Send to File* menu option sends all traffic from the selected trace file to a user specified trace file. This is a useful function because it allows for the decryption of traffic to be exported as a decrypted trace file.

Send to File with Filter

The *Send to File with Filter* menu option sends traffic from the selected trace file through a filter to a new trace file. This is a useful function because it can greatly reduce the size of a trace file to only those packets of interest. The *Filter Dialog* is explained in a later section.

Browse Containing Folder

The *Browse Containing Folder* menu option opens a Windows Explorer window pointed to the folder of the selected trace file.

Cut

The *Cut* menu option obtains a reference to the “to-be-cut” trace file. When the Paste operation is invoked, the file is copied to the “paste” location and removed from the original location only if the paste location references the same system as the Cut operation.

Copy

The *Copy* menu option obtains a reference to the “to-be-copied” trace file. When the Paste operation is invoked, the file is copied to the “paste” location and is NOT removed from the original location.

Paste

The *Paste* menu option will copy a previously Cut or Copied file to the selected Paste location.

Add/Remove Trend Index

Please refer to the

Interactive Views section for further details.

Calculate Checksum (MD5)

The *Calculate Checksum (MD5)* menu option calculates the MD5 cryptographic digest of the selected trace file and presents it in a window. This value is stored and will be used later in tooltips and reports if applicable.

Delete

The *Delete* menu option removes the selected trace file from disk. The trace file is not sent to the recycle bin.

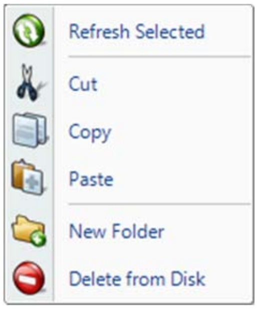
Remove from List

The *Remove from List* menu option removes the selected trace file's reference from the Files List, but not from the local file system.

Rename

The selected trace file can be renamed using the *Rename* menu option. The file name is renamed in the Files Panel and also on the local file system.

With A Trace Folder Selected on a Remote Shark appliance



Context Menu 12 Files Panel (Trace Folder Selected on Remote Shark appliance)

With a trace folder selected, the options are as follows:

Refresh Selected

The *Rescan Folder* menu option rescans a folder for new trace files and updates the status of those already added.

Cut

The *Cut* menu option obtains a reference to the "to-be-cut" folder. When the Paste operation is invoked, the folder and its contents are copied to the "paste" location and removed from the original location only if the source and destination are on the same system. If the source and destination are on different systems, then Cut behaves like a Copy operation.

Note: ***This option is not available for permanent folders such as "My Files" and "Jobs Repository"***

Copy

The *Copy* menu option obtains a reference to the "to-be-copied" folder. When the Paste operation is invoked, the folder is copied to the "paste" location and is NOT removed from the original location.

Paste

The *Paste* menu option will copy a previously Cut or Copied file to the selected Paste location.

New Folder

The *New Folder* menu option removes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

Delete

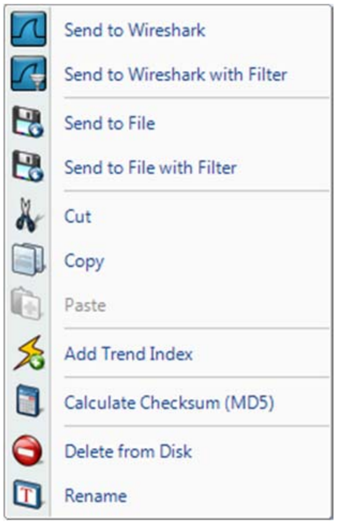
The *Delete* menu option irrevocably deletes the folder and all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

Note: ***This option is not available for permanent folders such as "My Files" and "Jobs Repository"***

Delete Trace Files

The *Delete Trace Files* menu option irrevocably deletes all trace files from the Files panel with respect to the selected folder that do not have a view open on them.

With A Trace File Selected on a Remote Shark appliance



Context Menu 13 Files Panel (Trace File Selected on Remote Shark appliance)

With a trace file selected, the options are as follows:

Send to Wireshark

The *Send to Wireshark* menu option starts up Wireshark and sends all traffic from the selected trace file there.

Send to Wireshark with Filter

The *Send to Wireshark with Filter* menu option instructs Cascade Pilot to start up Wireshark and send traffic that matches a user-defined filter from the selected file to Wireshark. The filter is specified using the *Filter Dialog Box*, which is explained in a later section.

Send to File

The *Send to File* menu option sends all traffic from the selected trace file to a user specified trace file. This is a useful function because it allows for the decryption of traffic to be exported as a decrypted trace file.

Send to File with Filter

The *Send to File with Filter* menu option sends traffic from the selected trace file through a filter to another trace file. This is a useful function because it can greatly reduce the size of a trace file to only those packets of interest. The *Filter Dialog* is explained in a later section.

Cut

The *Cut* menu option obtains a reference to the “to-be-cut” trace file. When the Paste operation is invoked, the file is copied to the “paste” location and removed from the original location only if the paste location references the same system as the Cut operation.

Copy

The *Copy* menu option obtains a reference to the “to-be-copied” trace file. When the Paste operation is invoked, the file is copied to the “paste” location and is NOT removed from the original location.

Paste

The *Paste* menu option will copy a previously Cut or Copied file to the selected Paste location.

Add/Remove Trend Index

Please refer to the

Interactive Views section for further details.

Calculate Checksum (MD5)

The *Calculate Checksum (MD5)* menu option calculates the MD5 cryptographic digest of the selected trace file and presents it in a window. This value is remembered and will be used later in tooltips and reports if applicable.

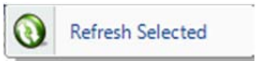
Delete

The *Delete* menu option removes the selected trace file from disk. The trace clip cannot be deleted if there is one or more Views currently applied to the trace clip.

Rename

The selected trace file can be renamed using the *Rename* menu option.

With The Jobs Repository Folder Selected on a Remote Shark appliance

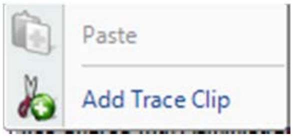


Context Menu 14: Jobs Repository Folder

Refresh Selected

The *Rescan Folder* menu option rescans a folder for new trace files and updates the status of those already added.

With A Job Trace Selected on a Remote Shark appliance



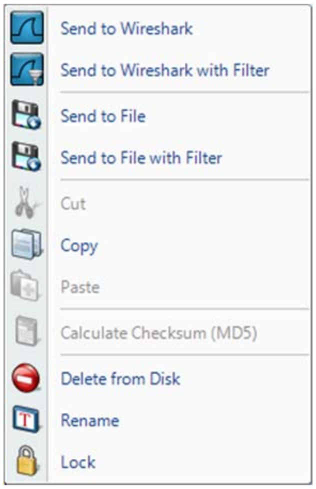
Context Menu 15: Job Trace

With a Job Trace selected, the options are as follows:

Add Trace Clip

The *Add Trace Clip* menu option brings up the Trace Clip time selection panel.

With A Trace Clip Selected on a Remote Shark appliance



Context Menu 16: Trace Clip

With a Trace Clip selected, the options are as follows:

Send to Wireshark

The *Send to Wireshark* menu option starts up Wireshark and sends all traffic from the selected trace clip there.

Send to Wireshark with Filter

The *Send to Wireshark with Filter* menu option instructs Cascade Pilot to start up Wireshark and send traffic that matches a user-defined filter from the selected trace clip to Wireshark. The filter is specified using the *Filter Dialog Box*, which is explained in a later section.

Send to File

The *Send to File* menu option sends all traffic from the selected trace clip to a user specified trace file. This is a useful function because it allows for the decryption of traffic to be exported as a decrypted trace file.

Send to File with Filter

The *Send to File with Filter* menu option sends all traffic from the selected trace clip in a user specified trace file with a filter to be defined in the filter dialog box, which appears first. This is a useful function because it can greatly reduce the size of a trace file to only those packets of interest. The *Filter Dialog* is explained in a later section.

Copy

The *Copy* menu option obtains a time filter corresponding to the time interval associated with the trace clip.

Delete

The *Delete* menu option removes the selected trace clip.

Rename

The selected trace file can be renamed using the *Rename* menu option.

Lock

By selecting the *Lock* menu option, the remote Shark appliance will lock the clip on disk, ensuring that the packet data is retained even as more traffic arrives on the system.

With a View Selected

The context menu for a view applied on a file is the same as the context menu of view applied on a device. Please refer to the paragraph: "With a View Selected" in the Device Panel section.

Views Panel

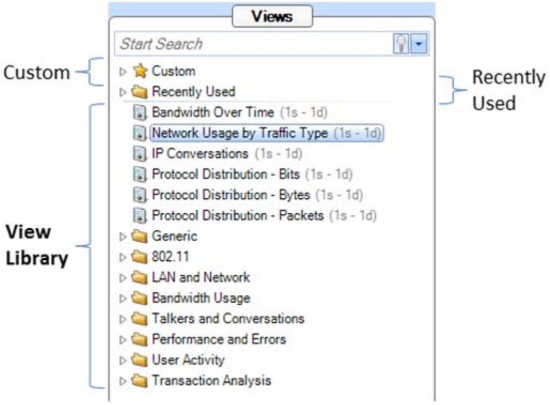

Views
Start Search
Custom
Custom
Recently Used
Recently Used
Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)
IP Conversations (1s - 1d)
Protocol Distribution - Bits (1s - 1d)
Protocol Distribution - Bytes (1s - 1d)
Protocol Distribution - Packets (1s - 1d)
View Library
Generic
802.11
LAN and Network
Bandwidth Usage
Talkers and Conversations
Performance and Errors
User Activity
Transaction Analysis

Figure 119 Views Library

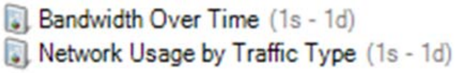

Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)

Figure 120 Instance of a View

A Cascade Pilot View represents a specific set of calculations that can be applied to both live and off-line (trace files) sources. The calculations associated with a View are called the View metrics. These metrics are visually presented to the user in terms of Charts. Graphical elements within a Chart are selectable such as bars within a bar chart and time intervals within a strip chart, etc.

Each view is depicted in the following format:

[Icon] [Name] ([Sampling Time] - [Data Retention Time])

For example, in Figure 120:

The Icon denotes the link type(s) of the source to which the View applies, which in this case is:

all link types

Other possible icons for the link type include:

wired Ethernet

802.11 link type

The View's name is "Bandwidth Over Time"

The Sampling Time is 1 second and so the associated metric (average bandwidth over time) is computed for every second.

The Data Retention Time is 1 day (1d), which means that once a day's worth of samples are calculated, the oldest samples will be dropped as new samples are calculated. This parameter is only used for live sources. In the case of trace files, all of the samples over the duration of the trace file are retained.

These parameters can be changed, and multiple instances of a view can exist with different parameters by utilizing the custom views feature, as explained below.

The Views panel above has four sections, which are (from top to bottom):

Search Text Box
Custom Views
Recently Used
View Library

Using Views

Views can be applied to one of the following:

- Devices, Trace Files, or Trace Clips
- Selections within Charts (also known as Drill Down)

Note: ***Not all Views can be applied to all devices, trace files, trace clips, or selections, as they are not applicable in certain contexts. For instance, a wired Ethernet device does not have signal to noise ratio of 802.11 channels.***

Applying a View (Local or Remote Sources)

Views can be applied to a device, trace file, or trace clip in the following ways:

Double Clicking on a View

When double clicking on a view, it is applied to the currently selected device or file, depending on which tab is open.

Pressing Enter on a View

Same as the double click previously described.

Dragging the View on to the Device, File, or Selection within a Chart

A view can be dragged on to any device or file, which opens the view on that source, similar to the above. Additionally, after performing a selection within a chart, a view can be dragged on to the selection, and the view will be applied to the subset of data that is selected.
When a view is dragged onto a source or selection two different icons can be displayed on the cursor:

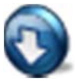


Figure 121: Apply Icon

- Figure 121 means the view metric can be applied to the source

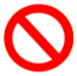


Figure 122:Do Not Apply Icon

- Figure 122 means that the view metric cannot be applied to the source.

Drill Down button in the Home Ribbon and Chart context menu option

Every chart has a "Drill Down" context menu option that lists the Custom, Recently Used, and View Library. This option is enabled when a selection is made in the chart, and selecting one of the views results in the view being applied to the subset of data selected. The drill-down menu button works identically.

Note: ***When drill down is applied to a live view, the new view shows results from the time the view was applied. Also, drill down cannot be applied to time selections in a live view. These limitations apply to the live Interfaces only.***

Applying a View with a Filter

It is possible to enable a filter when applying a view to limit the view to a subset of the original data. When holding down the control key and applying a view either by pressing enter, or dragging and dropping, a filter dialog box opens, enabling a filter to be specified. The Filter Dialog is explained further below.

Note: ***Application of a View with a Filter does not apply to the drill down operation. The reason for this is that the basis for the drill-down is the visual selection within a Chart, which intrinsically represents a filtering operation.***

When a view is dragged onto a source with a filter two different icons can be displayed on the cursor:

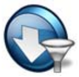


Figure 123: Apply Icon

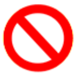


Figure 124:Do Not Apply Icon

- Figure 123 means the view metric can be applied with filter to the source
- Figure 124 means that the view metric cannot be applied to the source.

View Library

The *View Library* is the main repository of all the views available in Cascade Pilot.

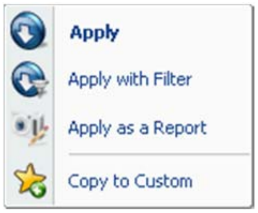
Views are divided into folders that are, in some cases, further subdivided.

Context Menus

The view library has two types of context menus. They are triggered when right clicking on either of the following:

- Folder
- View

Folder



Context Menu 17 View Library Folder

The context menu for a folder in the view library section has the following options:

Apply

The *Apply* menu option applies all the views in the currently selected folder to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies all the views in the currently selected folder to the selected device or file in the Devices and Files panel with a specified filter. The Filter Dialog (described later) pops up when this option is selected.

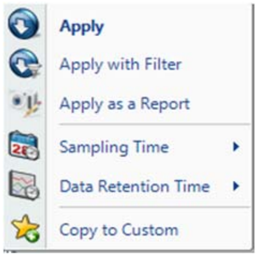
Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the “All Views” option as all the views in the currently selected folder applied to file selected in the Files panel. This menu option is disabled when a device is selected.

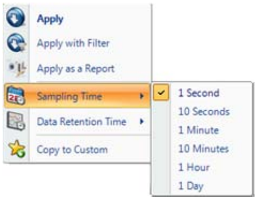
Copy to Custom

The *Copy to Custom* menu option copies the currently selected folder to the Custom folder (described later).

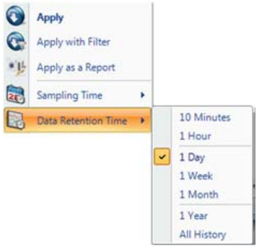
View



Context Menu 18 View Library View



Context Sub Menu 1 Sampling Time



Context Sub Menu 2 Data Retention Time

The context menu for a view in the view library section has the following options:

Apply

The *Apply* menu option applies the selected view to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies the selected view to the selected device or file in the Devices and Files panel with a specified filter. The Filter Dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the “All Views” option to the selection view applied to the file selected in the Files panel. Apply as a Report cannot be applied to a live interface.

Sampling Time

The *Sampling Time* menu option specifies the time granularity of the calculation for the corresponding View metric. The view calculations and time control options are performed with a specific time sampling interval, which typically defaults to one second. This context menu enables changing this interval, and the selected value is shown at the end of the textual representation of the view in the Views Library (along with the Data Retention Time value, described next).

Data Retention Time

The *Data Retention Time* value specifies the time period for the View metric history that is retained for a View applied to a live source. Once the Data Retention Time is reached, the oldest metrics are discarded as new sample points are calculated. The Data Retention time has no effect on the duration of the View metrics retained for trace files, since the complete View metric history over the duration of the trace file is retained.

Copy to Custom

The *Copy to Custom* menu option copies all the views in the currently selected folder to the Custom section (described later).

Tooltips

Tooltips are enabled for each of the views, and display a summary of the calculated view metrics and the various charts that comprise the view. They are made visible by hovering over the icon for a view or folder.

Recently Used

The Recently Used folder contains the five most recently used views. The Recently Used folder is not shown when the folder is empty, as is the case when Cascade Pilot is started.

Context Menus

The Recently Used section has two types of context menus. They are triggered by right clicking on either of the following:

- Recently Used Folder
- View within the Recently Used Folder

Recently Used Folder

**Context Menu 19
Recently Used Folder**

The context menu for a folder in the recently used section has the following options:

Apply

The *Apply* menu option applies all the views in the recently used folder to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies all the views in the recently used folder to the selected device or file in the Devices and Files panel with a specified filter. The filter dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option will automatically create a report with the "All Views" option as all the views in the recently used folder applied to the file selected in the Files panel. Apply as a Report cannot be applied to a device.

The Context menus for Views within the Recently Used Folder are identical to those when applied to Views in the View Library.

Custom Views

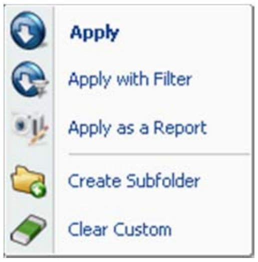
Custom Views are the views in the views library that have been saved with different settings. At the view level, the chart window positions and sizes are saved. At the chart level it varies. In the description of the charts it is noted whether the option is saved or not in a custom view.

Context Menus

The Custom section has two types of context menus. They are triggered when right clicking on either of the following:

- Folder (including the root "Custom" folder with the star icon)
- View

Custom Folder



Context Menu 20
Custom Folder

The context menu for the Custom folder has the following options:

Apply

The *Apply* menu option applies all the views in the selected folder in the custom section to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies all the views in the selected folder in the custom section to the selected device or file in the Devices and Files panel with a specified filter. The filter dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the "All Views" option as all the views in the selected folder in the custom section applied to the file selected in the Files panel. The *Apply as a Report* menu option cannot be applied to a device.

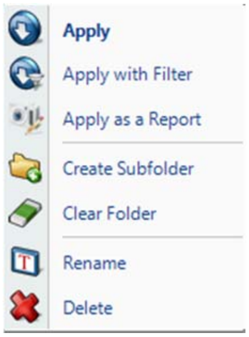
Create Subfolder

The *Create Subfolder* opens a dialog that prompts for the name of a to-be created subfolder in the custom section.

Clear Custom

The *Clear Custom* menu option removes the references to all of the views in the selected folder in the custom section.

Folder within the Custom Folder



Context Menu 21
Custom Folder

The context menu for a folder within the Custom folder has the following options:

Apply

The *Apply* menu option applies all the views in the selected folder in the custom section to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies all the views in the selected folder in the custom section to the selected device or file in the Devices and Files panel with a specified filter. The filter dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the "All Views" option as all the views in the selected folder in the custom section applied to the file selected in the Files panel. The *Apply as a Report* menu option cannot be applied to a device.

Create Subfolder

The *Create Subfolder* opens a dialog that prompts for the name of a to-be created subfolder in the custom section.

Clear Folder

The *Clear Custom* menu option removes the references to all of the views and sub folders in the selected folder in the custom section.

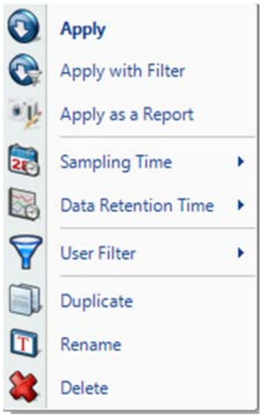
Rename

The Rename menu option prompts for the new name for the folder.

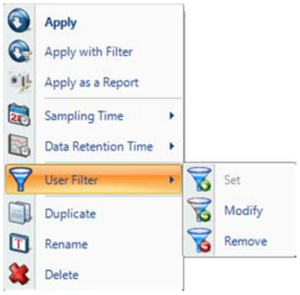
Delete

The Delete menu option will delete the folder and all of its contents.

View within Custom Folder (or Sub Folder)



Context Menu 22 Custom View



Context Sub Menu 3 User Filter

The context menu for a view in the Custom section has the following options:

Apply

The *Apply* menu option applies the selected view to the selected device or file in the Devices and Files panel.

Apply with Filter

The *Apply with Filter* menu option applies the selected view to the selected device or file in the Devices and Files panel with a specified filter. The filter dialog (described later) pops up when this option is selected.

Apply as a Report

The *Apply as a Report* menu option automatically creates a report with the “Current View” option as the selected view for the file selected in the Files panel. The *Apply as a Report* menu option cannot be applied to a device.

Sampling Time

As described above, this context menu option enables modification of the underlying sampling time used in the view calculations.

Data Retention Time

As described above, this context menu option enables modification of the duration that data is retained for a live view.

User Filter

The *User Filter* menu option applies a permanent filter to the view so that it does not need to be specified each time. Clicking on *Set* brings up the *Filter Dialog*, which is described below. After a filter is set, the menu options of *Modify* and *Remove* are enabled, and their functions are self-explanatory.

Duplicate

The *Duplicate* menu option duplicates the reference to a view so that different options can be saved for a view.

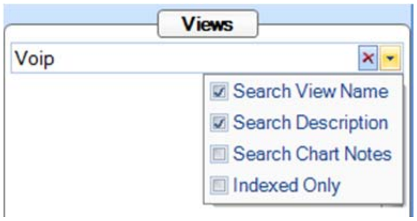
Rename

The *Rename* menu option allows the view to be renamed.

Delete

The *Delete* menu option deletes the selected view in the Custom section. All settings for the custom view are lost.

Search Text Box



Voip

☑ Search View Name
☑ Search Description
☐ Search Chart Notes
☐ Indexed Only

Context Menu 23 View Panel Search

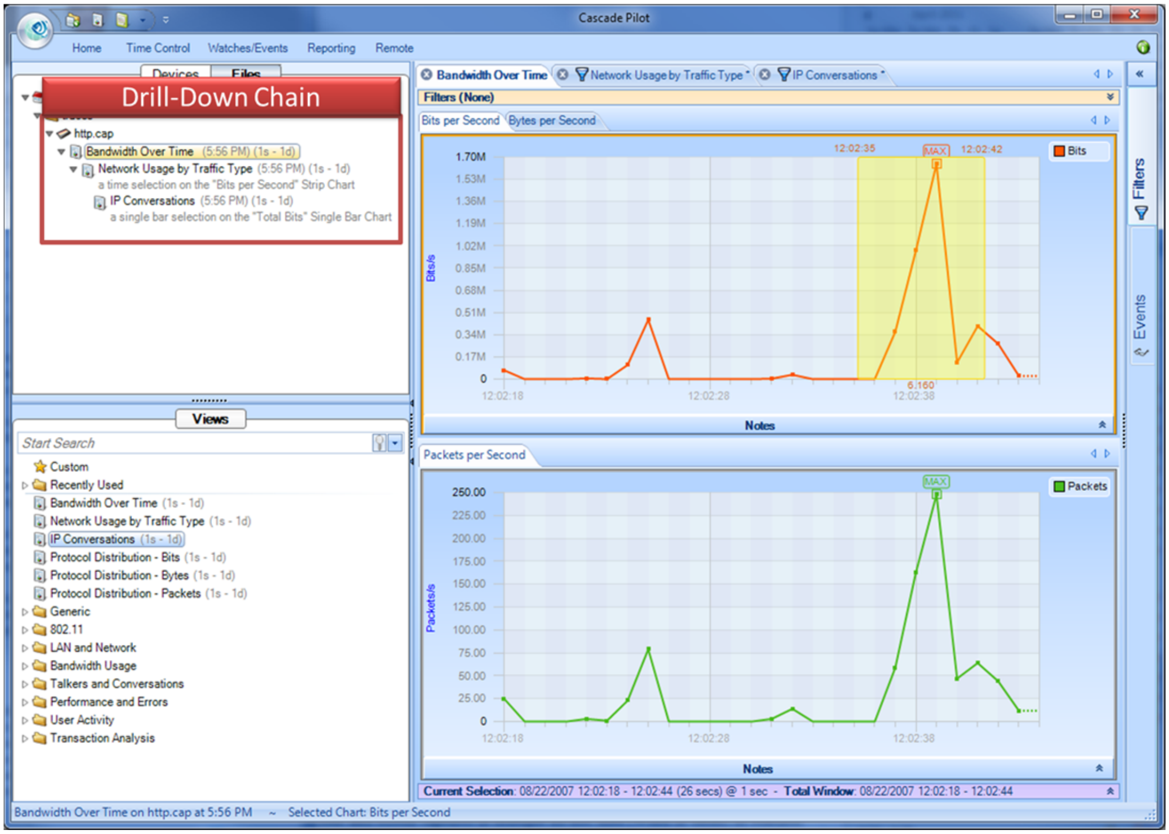
The Search Box is used to locate Views for specific purposes. For example, if VoIP is entered, the search will find all of the Views that have "VoIP" in either the View Name or the View Description. The drop-down check box also allows searches over the Chart Notes of all the charts that are part of a View.

The Search box is a convenient way to find the View that you are looking for. In a sense, it provides an alternative ways of organizing the View Library.

Interactive Views

As discussed previously, one of the most powerful features of Pilot is Drill-down, which enables a user to select a subset of the data in one view and apply a second view for an alternative metric or more details about the selected data, and perhaps a third or fourth view for additional details. This chain can then be converted into an Interactive View, which means that as the user changes selections in the first view(s), the subsequent views are automatically updated.

In the following example, a Bandwidth Over Time view is applied to the trace file http.cap, a time selection in the strip chart is used to drill-down using the Network Usage by Traffic Type view, and finally, the Web bar is selected to drill-down with the IP Conversations view.

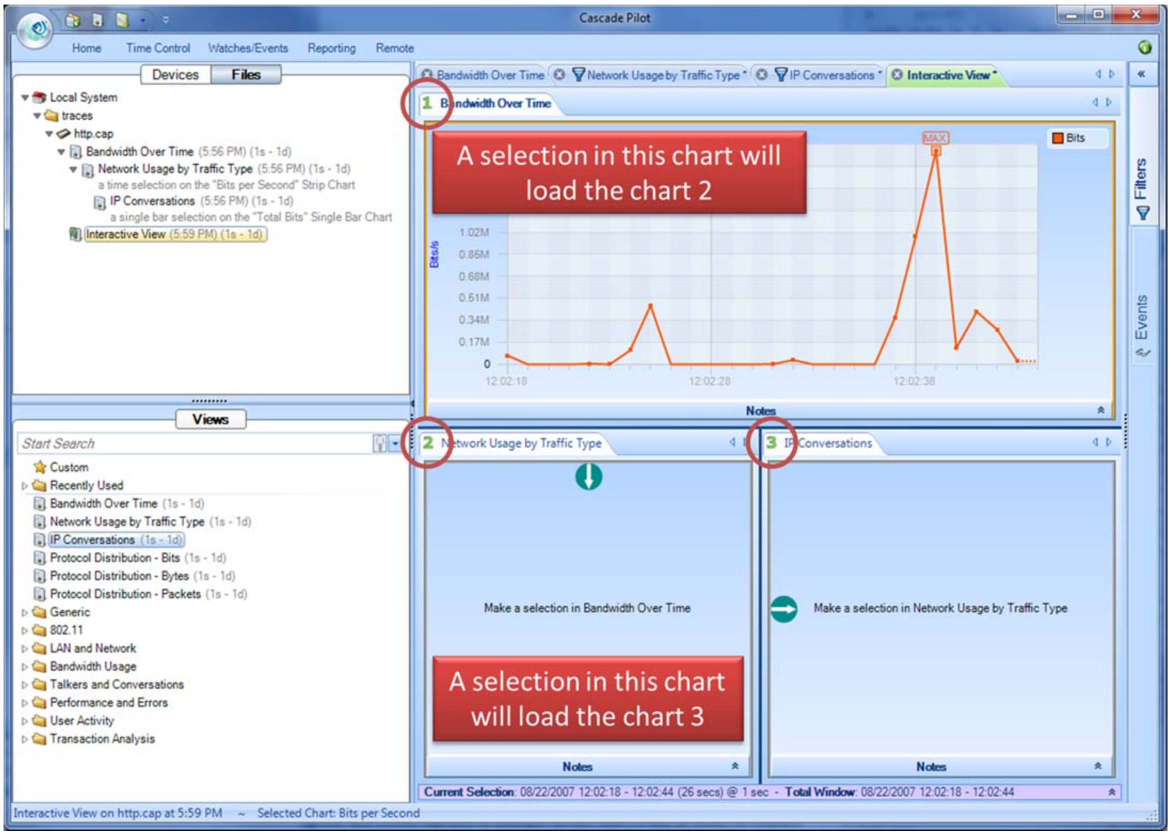


Current Selection: 08/22/2007 12:02:18 - 12:02:44 (26 secs) @ 1 sec - Total Window: 08/22/2007 12:02:18 - 12:02:44

Bandwidth Over Time on http.cap at 5:56 PM ~ Selected Chart: Bits per Second

Figure 125: Drill-down chain

To create an Interactive View, right-click the last drill-down view in the chain (*IP Conversations* in this example) and choose *Create Interactive View*. A new Interactive View is generated with the selected charts from the views in the drill-down chain.


Cascade Pilot
Home
Time Control
Watches/Events
Reporting
Remote
Devices
Files
Local System
traces
http.cap
Bandwidth Over Time (5:56 PM) (1s - 1d)
Network Usage by Traffic Type (5:56 PM) (1s - 1d)
a time selection on the "Bits per Second" Strip Chart
IP Conversations (5:56 PM) (1s - 1d)
a single bar selection on the "Total Bits" Single Bar Chart
Interactive View (5:59 PM) (1s - 1d)
Views
Start Search
Custom
Recently Used
Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)
IP Conversations (1s - 1d)
Protocol Distribution - Bits (1s - 1d)
Protocol Distribution - Bytes (1s - 1d)
Protocol Distribution - Packets (1s - 1d)
Generic
802.11
LAN and Network
Bandwidth Usage
Talkers and Conversations
Performance and Errors
User Activity
Transaction Analysis
Bandwidth Over Time
Network Usage by Traffic Type
IP Conversations
Interactive View
1 Bandwidth Over Time
MAX
Bits
Bits/s
1.02M
0.85M
0.68M
0.51M
0.34M
0.17M
0
12:02:18
12:02:28
12:02:38
Notes
2 Network Usage by Traffic Type
3 IP Conversations
Filters
Events

A selection in this chart will load the chart 2

Make a selection in Bandwidth Over Time

Make a selection in Network Usage by Traffic Type

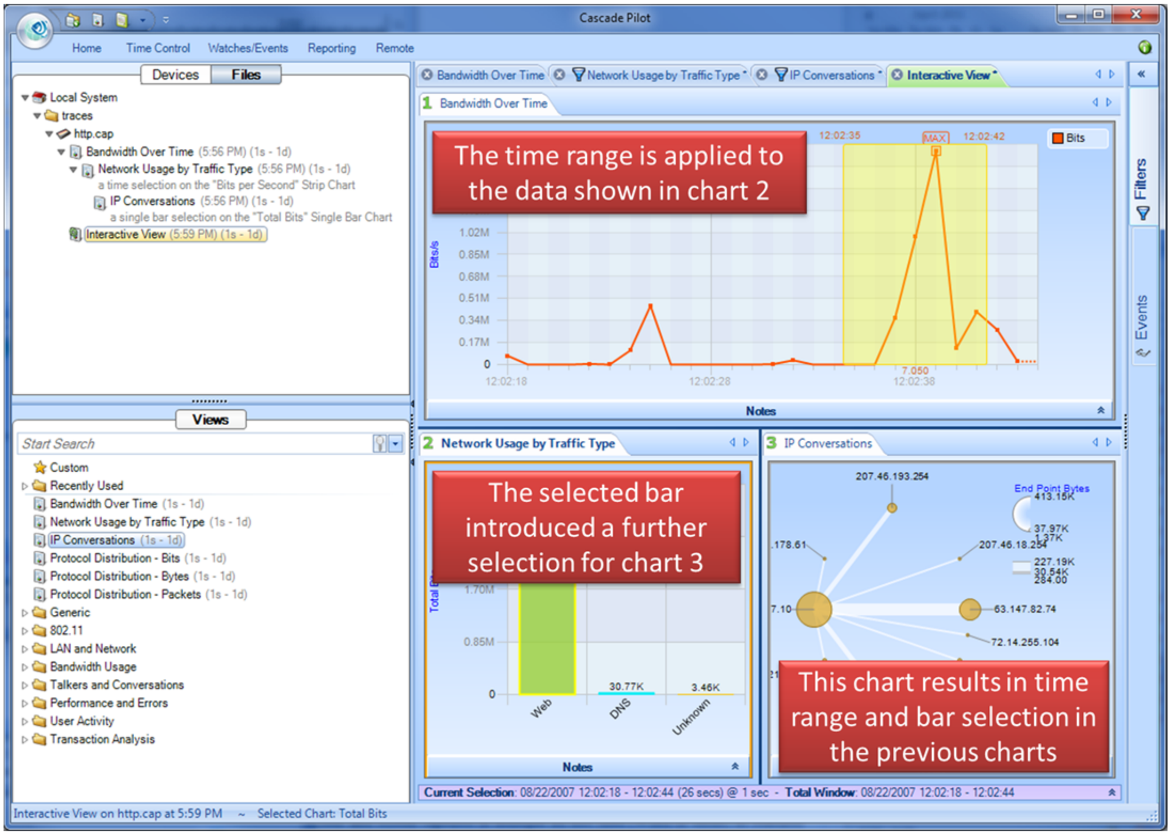
A selection in this chart will load the chart 3

Current Selection: 08/22/2007 12:02:18 - 12:02:44 (26 secs) @ 1 sec - Total Window: 08/22/2007 12:02:18 - 12:02:44

Interactive View on http.cap at 5:59 PM ~ Selected Chart: Bits per Second

Figure 126: Steps for drilling down

The numbers in the chart titles, arrows and instructions illustrate how to enable each chart. Once a time range has been selected in the Bandwidth Over Time chart, the selection result is applied to the Network Usage by Traffic Type chart for the time range selected in the first chart. A further selection in the Network Usage by Traffic Type chart shows the IP conversations ring, constrained to the time selection in the first chart and the traffic type selected in the second chart.



The time range is applied to the data shown in chart 2

The selected bar introduced a further selection for chart 3

This chart results in time range and bar selection in the previous charts

Current Selection: 08/22/2007 12:02:18 - 12:02:44 (26 secs) @ 1 sec - Total Window: 08/22/2007 12:02:18 - 12:02:44

Interactive View on http.cap at 5:59 PM ~ Selected Chart: Total Bits

Figure 127: Drill-down example

Regular Views, Fast Views, and Forbidden Views

When some Views are applied to Sources that have associated Trending/Indexing Data, they can make use of the index to run very quickly, even on large data sets. When a source is selected, the icons for the Views change to indicate whether they run as regular views (no lightning icon), fast views (lightning icon), or forbidden (red "X"). The forbidden views are those that cannot be run with the Trending/Indexing data alone. The ordinary views are those that cannot be run with the Trending/Indexing data alone, but the actual packets are available for the View calculation.

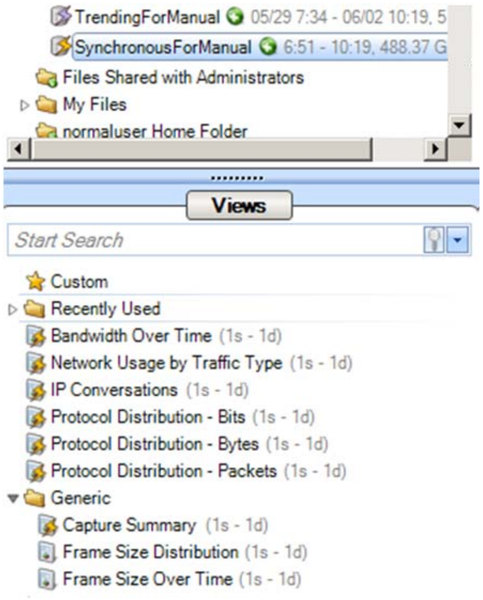

TrendingForManual 05/29 7:34 - 06/02 10:19, 5
SynchronousForManual 6:51 - 10:19, 488.37 G
Files Shared with Administrators
My Files
normaluser Home Folder
Views
Start Search
Custom
Recently Used
Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)
IP Conversations (1s - 1d)
Protocol Distribution - Bits (1s - 1d)
Protocol Distribution - Bytes (1s - 1d)
Protocol Distribution - Packets (1s - 1d)
Generic
Capture Summary (1s - 1d)
Frame Size Distribution (1s - 1d)
Frame Size Over Time (1s - 1d)

Figure 128: Fast Views

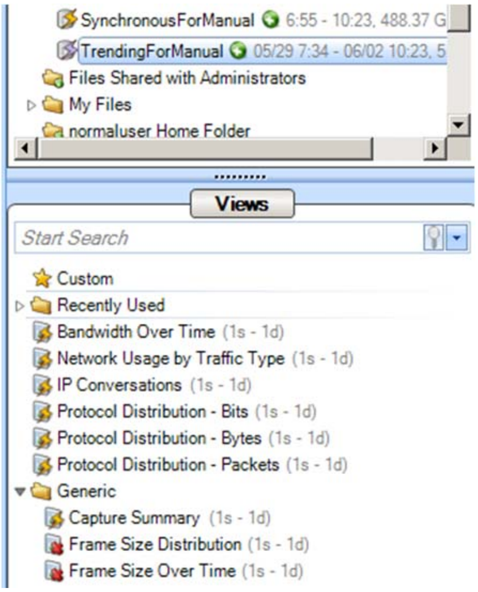

SynchronousForManual 6:55 - 10:23, 488.37 G
TrendingForManual 05/29 7:34 - 06/02 10:23, 5
Files Shared with Administrators
My Files
normaluser Home Folder
Views
Start Search
Custom
Recently Used
Bandwidth Over Time (1s - 1d)
Network Usage by Traffic Type (1s - 1d)
IP Conversations (1s - 1d)
Protocol Distribution - Bits (1s - 1d)
Protocol Distribution - Bytes (1s - 1d)
Protocol Distribution - Packets (1s - 1d)
Generic
Capture Summary (1s - 1d)
Frame Size Distribution (1s - 1d)
Frame Size Over Time (1s - 1d)

Figure 129: Disallowed Views

Indexing

Indexing a Trace File

Indexing a trace file can improve the performance of several views by a factor of 100x to 1000x. Creating an index does not take much more time than loading a single view, thus it is often more efficient to create an index on a large file and then apply multiple views on the indexed file.

Indexes can be applied to all types of trace files except Wi-Fi capture files. When an index is successfully created, the indexed file shows a small yellow lightning icon on it. If, for any reason, the index is not completely loaded, a red lighting arrow appears on the top of the trace file icon. When an indexed file is selected in the source panel, all the views supporting that index show a small yellow lighting icon on the top of them.

Apply an Index to a Trace File

An Index can be applied to a trace file using the *Add Trend Index* button in the trace file context menu option.

Context Menu

Add Trend Index

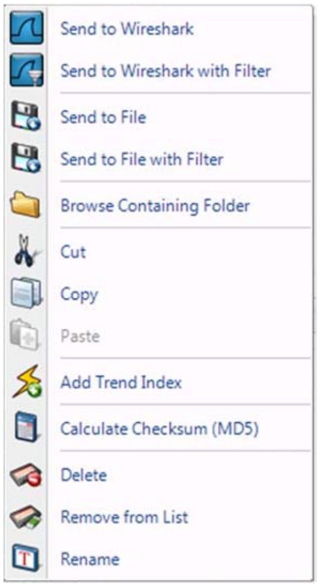


Figure 130: Add Trace Index context menu

The context menu for a Trace File without index shows:

Add Trend Index

The *Add Trend Index* menu option creates an Index on the selected file.

Figure 131: Add Trend Index

Interrupt Trend Index

The context menu while the index on a Trace File is created shows:

Interrupt Indexing

The *Interrupt Trend Index* menu option interrupts the creation of an Index while it is being created

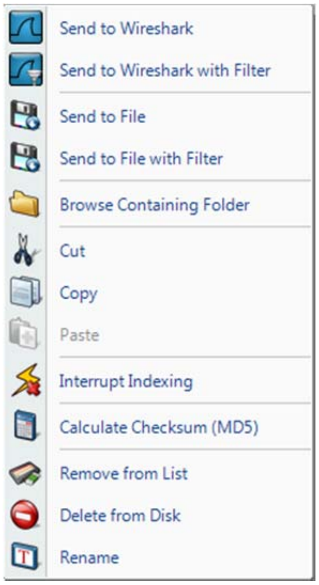


Figure 132: Add Trace Index context menu

Figure 133: Interrupt Indexing

Remove Trend Index

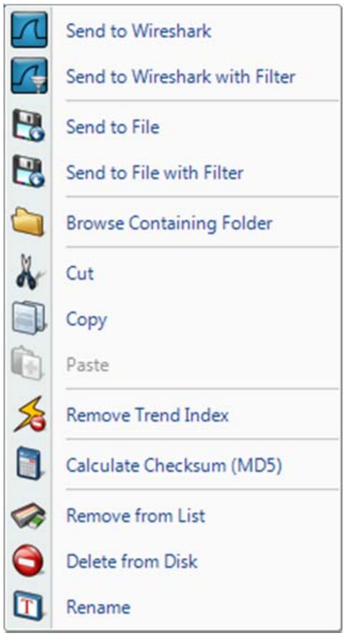


Figure 134: Remove an Index context menu

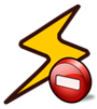


Figure 135:Remove Trend Index

The context menu for a Trace File with an index applied on it shows:

Remove Trend Index

The *Remove Trend Index* menu option removes the current Index from the selected file.

Index Icons on Trace Files

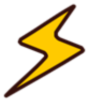


Figure 136: Index Applied

Index Applied means that the index has been applied successfully and thus many views will be accelerated.

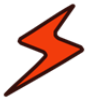
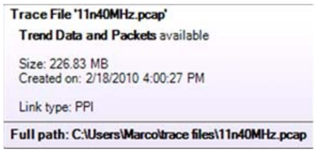


Figure 137: Index Broken

Index Broken means that either the file does not support indexing (e.g. a Wi-Fi file) or the index was interrupted before completion. To show the cause of the broken index, text in gray appears on the right of the trace file containing either:

- *Indices not supported on wireless sources*
- *Index not complete*

Tooltips



Trace File '11n40MHz.pcap'
Trend Data and Packets available

Size: 226.83 MB
Created on: 2/18/2010 4:00:27 PM

Link type: PPI

Full path: C:\Users\Marco\trace files\11n40MHz.pcap

Tooltip 1 Indexed File Tooltip

The *Indexed File* tooltip shows the full path of trace file that the mouse is hovering over along with the three metrics:

Trend Data and Packets available

Indicates that the index has been applied and both accelerated trend data and detailed packet data are available for this trace file.

Trace File

The name of the file.

Created On

The date the trace file was created.

Size

The size of the trace file in kilobytes.

Link Type

The link type of the trace file. This is important because not all views can be applied on all files. In particular, if the Link type is PPI, then the index cannot be created.

Drag and Drop Cursors for Indexed Trace Files

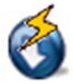
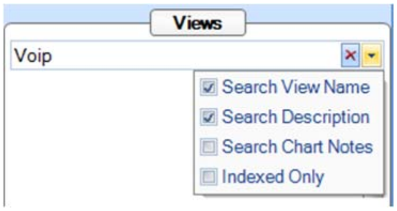


Figure 138: Drag and Drop cursor for Indexed Files

The *Drag and Drop cursor* for indexed Trace Files includes a yellow lightning bolt to indicate that the index will be used.

Search Text Box

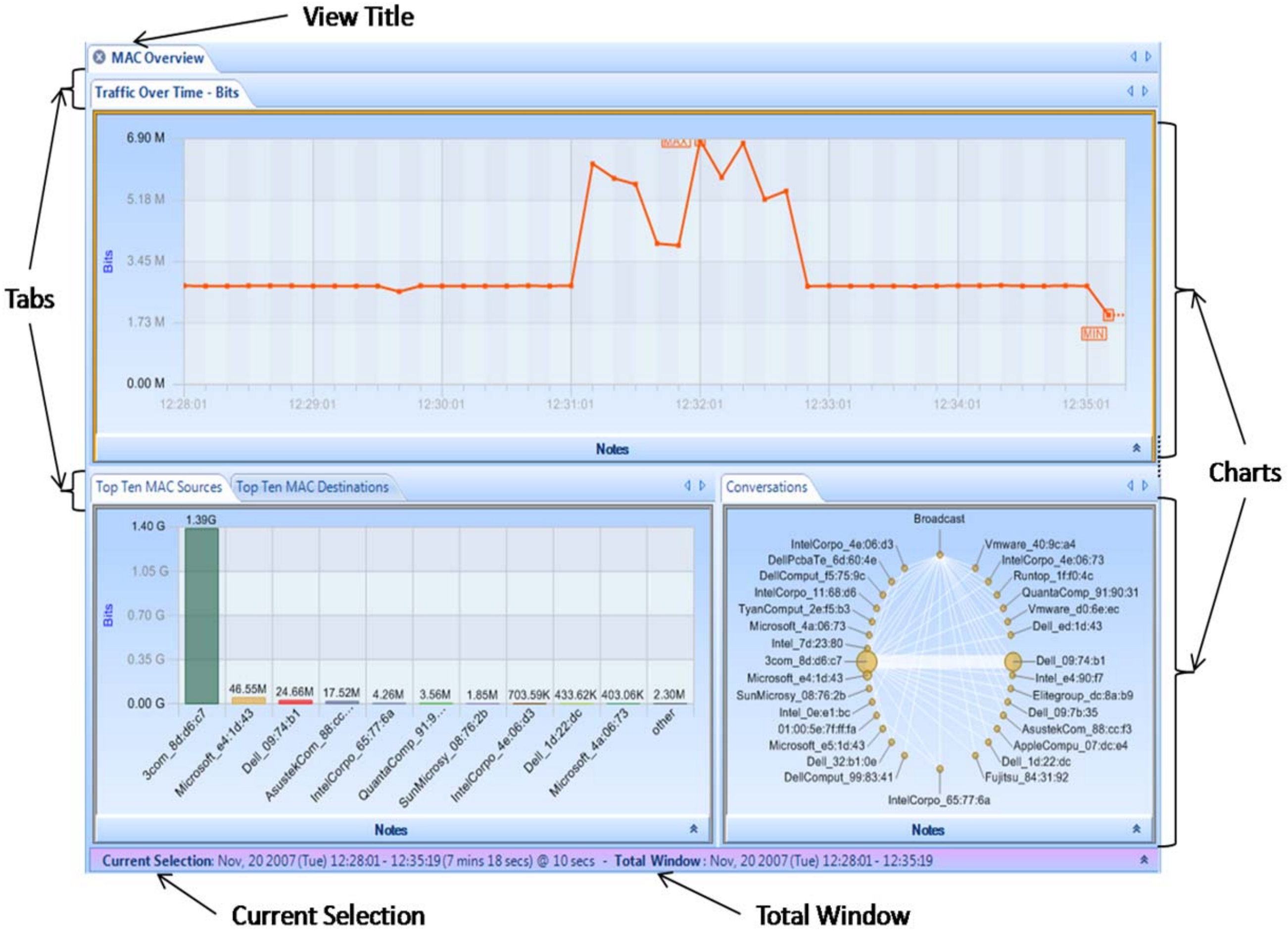


Context Menu 24 View Panel Search

The Search box has an Indexed Only option to include only Views that support indexing.

Main Workspace

The *Main Workspace* uses tabbed windows that are usually be referred to as “views” or the more general term “tabs.” A View consists of a number of Charts – for example, the View depicted below consists of a strip chart, a bar chart, and a conversation ring. In general, the specific analyses supported by a View are displayed in the Charts that make up the View.



Current Selection: Nov, 20 2007 (Tue) 12:28:01 - 12:35:19 (7 mins 18 secs) @ 10 secs - Total Window: Nov, 20 2007 (Tue) 12:28:01 - 12:35:19

Figure 139: A View in the Main Workspace

Each View has a main tab that contains the *View Title*. Each of the Charts that make up a View has its own tab.

The Time Control window along the bottom edge of the View displays two time intervals: the *Current Selection* interval and the *Total Window* interval.

- *Current Selection*: The Charts that comprise the View display metrics are computed over the *Current Selection* interval. The duration following the “@” sign has two different potential meanings. For a live View, the interval indicates the time interval between updates to the View metrics. Alternatively, if one to the Charts in the View is a strip chart, then the value is the subsampling interval for the points in the strip chart. For all other Chart types, this value is not used.

- *Total Window*: For a live source, the *Total Window* is the time duration from when the View was first applied until the current time. For a trace file, the Total Window is the interval of time over which the trace file was captured.

Context Menus

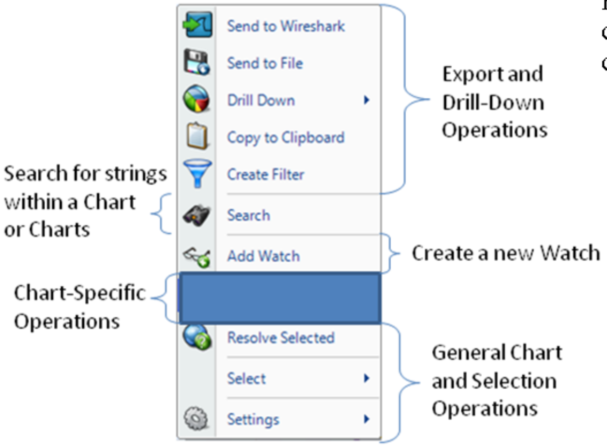

Send to Wireshark
Send to File
Drill Down
Copy to Clipboard
Create Filter
Search
Add Watch
Resolve Selected
Select
Settings
Export and Drill-Down Operations
Search for strings within a Chart or Charts
Create a new Watch
Chart-Specific Operations
General Chart and Selection Operations

Figure 140: Chart Context Menu Overview

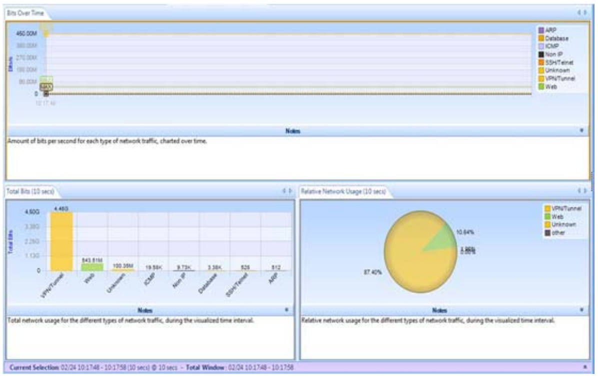
Each chart has a context menu that is specific to that chart. However, with few exceptions, all charts share certain options in their context menus:

- Export and Drill Down Operations
- Search over Charts
- Add Watch (only for Strip Charts and Bar Charts)
- Chart-Specific Operations
- General Chart and Selection Operations

Tooltips

Since some of the methods of data display afford solely qualitative comparison, tooltips are available on some charts to give a quantitative representation of what is graphically displayed.

Notes



Amount of bits per second for each type of network traffic, charted over time.

Total network usage for the different types of network traffic, during the visualized time interval.

Relative network usage for the different types of network traffic, during the visualized time interval.

Current Selection: 02/24 10:17:48 - 10:17:58 (10 secs) @ 10 secs - **Total Window**: 02/24 10:17:48 - 10:17:58

Figure 141 View With Collapsed Notes

Every chart has a section that can be used to place notes that are included in a generated report and if applicable, saved in a custom view.

For example, in the view on the left, all the note areas are expanded.

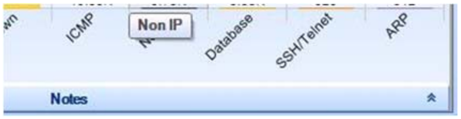
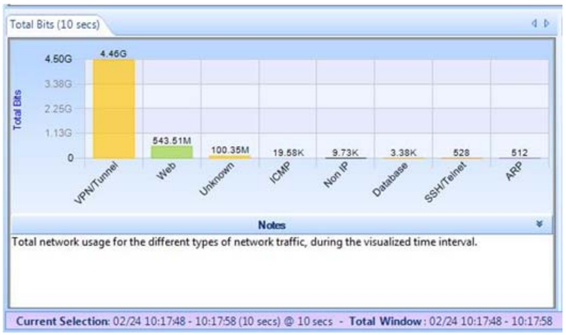


Figure 142: View Notes Toggle Button

Each chart has a long horizontal bar with a small arrow on the right bottom border.



Total network usage for the different types of network traffic, during the visualized time interval.

Current Selection: 02/24 10:17:48 - 10:17:58 (10 secs) @ 10 secs - **Total Window**: 02/24 10:17:48 - 10:17:58

Figure 143 View With Expanded Notes

When clicked, a text area will appear under the associated graph for text. There is a default description for each graph provided. The text in the notes section is included in generated reports and the notes are saved in a custom view.

Selection

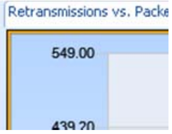


Chart Figure 1 Chart Selected

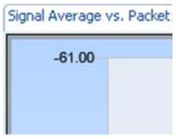


Chart Figure 2 Chart Not Selected

A chart can be selected by clicking on it, and the currently selected chart can be identified when there is an orange border around it, as depicted to the left. In any view, there is at most one chart selected at any given time.

Mini

Every Chart has a large view with legends and controls, and a mini view with just the graphic itself. The miniature shows up when there is not enough space to display the standard view. In a mini view, none of the elements can be selected and there is no contextual menu.

Conversation Ring

In the *Conversation Ring*, “conversation” endpoints are placed around an ellipse. The Conversation Ring is used for situations in which “stations,” represented by the endpoints, communicate (i.e. have a conversation) with each other. The endpoints are depicted as circles, and a line connecting a pair of endpoints signifying that two endpoints are communicating with each other. The size of the endpoint and the size of the line are proportional to the amount of traffic sent to/from the endpoints over the selected time period.

Default

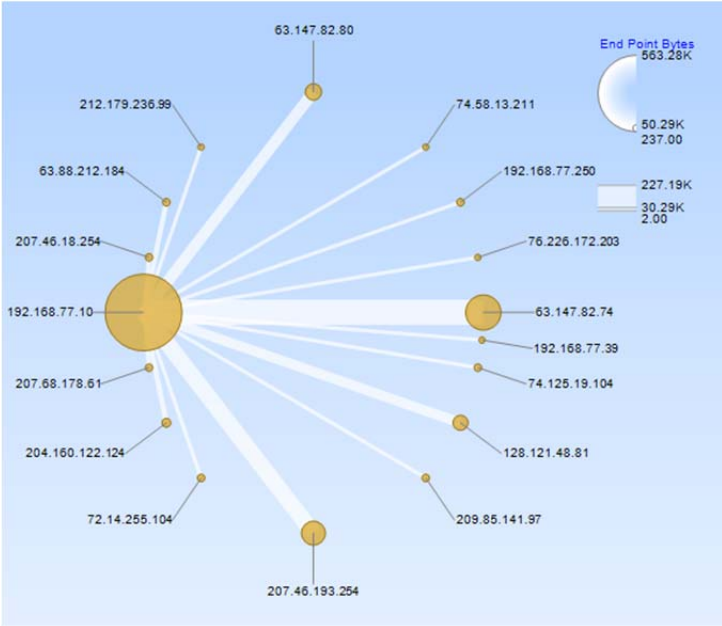


Chart Figure 3 Conversation Ring

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Conversation Ring is customizable in the following ways:

- Magnification with the scroll wheel
- Endpoint color
- Name resolution
- Bytes or packets to signify endpoint and connection size

There are three distinct mouse based operations for the conversation ring:

- Scroll Wheel
- Hover
- Selection

Size Legends

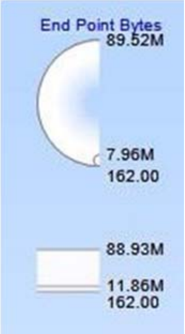


Chart Figure 4 Size Legends in a Conversation Ring

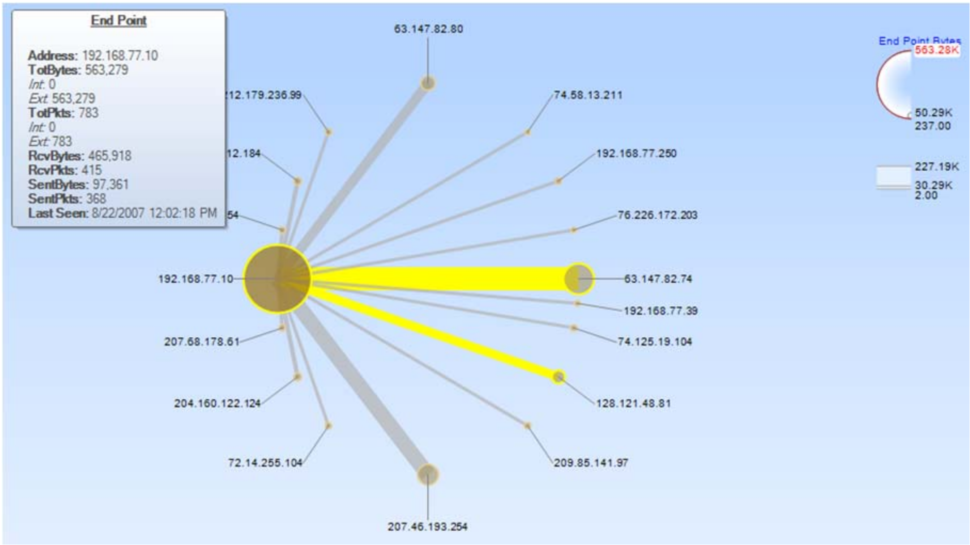
In the upper right corner of the view are two size legends that depict the maximum, average and the minimum traffic in all displayed endnotes and conversations. An example is shown in the Figure.

Scroll Wheel

The mouse *scroll wheel* is used to change the magnification level of the conversation ring. This is useful when the endpoints are densely packed and can't be individually identified.

Hover with Tooltip

A hover highlights all the connections associated with an endpoint or all the endpoints associated with a connection. The hover operation causes a tooltip to pop up (described later) giving quantitative information describing the connection or endpoint, and causes the Size Legend to display the values for the endpoint or conversation in red.



End Point

Address: 192.168.77.10
TotBytes: 563,279
Int: 0
Ext: 563,279
TotPkts: 783
Int: 0
Ext: 783
RcvBytes: 465,918
RcvPkts: 415
SentBytes: 97,361
SentPkts: 368
Last Seen: 8/22/2007 12:02:18 PM

Chart Figure 5 Conversation Ring Hover

Selected

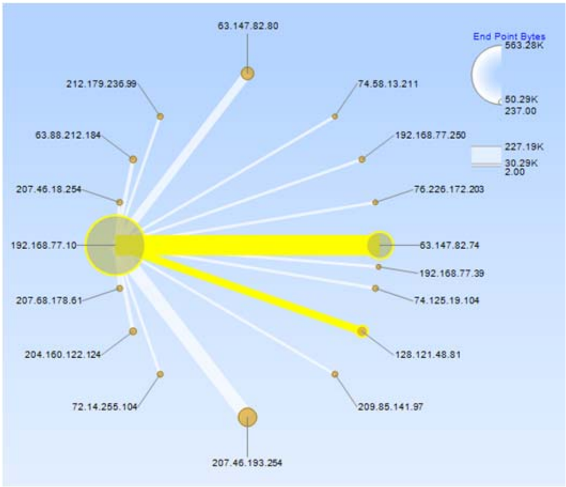
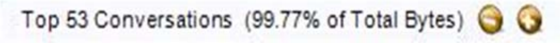


Chart Figure 6 Conversation Ring Selection

Clicking on a connection selects the connection and the associated endpoints. Clicking on an endpoint selects all the connections that include the endpoint as well as all the associated endpoints that are on the other side of the connections.

Clicking with Control key pressed is supported for multiple endpoint or connection based selections (which can be mixed).

Top Conversations



Top 53 Conversations (99.77% of Total Bytes)

Chart Figure 7 Conversation Ring Top Conversations

When there is not enough space to display all of the conversations clearly in a single ring, Pilot automatically includes data by relevance. A small label displaying the number of conversations and the percentage of the underlying data that are visible appears at the bottom of the view. The number of endpoints in the view can be increased or decreased using the two small yellow + and - buttons.

Mini

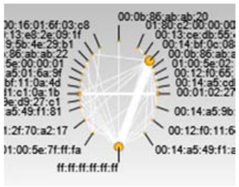
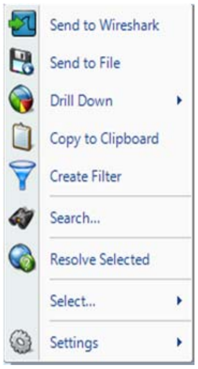


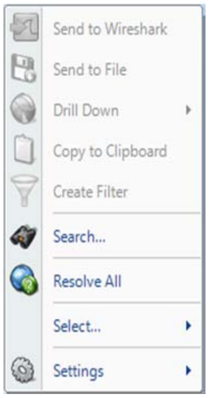
Chart Figure 8 Conversation Ring Mini

This is the miniature view of the Conversation Ring. The miniature shows up when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Context Menu



Context Menu 25 Conversation Ring (Selection)



Context Menu 26 Conversation Ring (No Selection)

Context Sub Menu 4 Select

The context menu for the Conversation Ring is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected endpoint(s) and connection(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected endpoint(s) or connection(s) to a user-specified trace file which will appear, after completion, in the Files panel.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected endpoint(s) or connection(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies a table of data values corresponding to the current selection to the clipboard. These are copied in the order that the hosts were discovered in the conversation ring. The only exception to this rule is that the “Last Seen” value is not included in what is copied to the clipboard.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts. The search context consists of the labels of the items in a chart which can be selected. For instance, an IP address, MAC address, or hostname can all be searched. The Search Dialog is described in its own section later on.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option tries to identify the unresolved IP addresses, ports, or MAC addresses from the selected endpoints and/or conversations.

Select

The *Select* menu option has two submenu options to either select all the connection(s) and endpoint(s) in the Conversation Ring, or to invert the current selection of the endpoint(s) and connection(s).

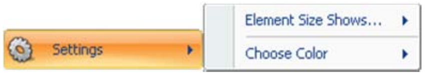
Settings

The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

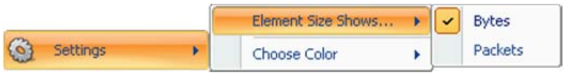
Context Sub-Menus

The Conversation Ring has the following contextual submenus:

- Settings



Context Sub Menu 5 Conversation Ring Settings



Context Sub Menu 6 Conversation Ring Settings (Detail)

The Conversation ring has the following settings:

- Element Size Shows
- Choose Color

Element Size Shows

As mentioned previously, the endpoint(s) and connection(s) are sized proportional to either the number of bytes or the number of packets received in the given time period. This submenu enables changing which metric is used.

Choose Color

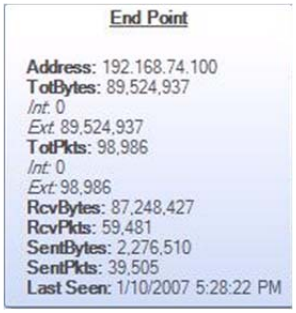
The *Choose Color* contextual submenu is used to change the color of the endpoints.

Tooltips

The conversation ring has two kinds of tooltips:

- Connection Based
- Endpoint Based

Endpoint



<u>End Point</u>

Address: 192.168.74.100
TotBytes: 89,524,937
Int: 0
Ext: 89,524,937
TotPkts: 98,986
Int: 0
Ext: 98,986
RcvBytes: 87,248,427
RcvPkts: 59,481
SentBytes: 2,276,510
SentPkts: 39,505
Last Seen: 1/10/2007 5:28:22 PM

Tooltip 2 Conversation Ring Endpoint

When hovering over an endpoint, a tooltip pops up with the following fields:

Address

The *Address* refers to the associated MAC or IP address (as applicable) of the endpoint.

ResAddr

The *ResAddr* refers to the Resolved name of the endpoint.

TotBytes

The *TotBytes* refers to the total number of bytes that have been either sent from or received at that endpoint, i.e. the sum of RcvBytes and SentBytes.
Int refers to bytes that are sent from the host to itself (i.e. the IP source is the same as the destination). *Ext* refers to bytes that are sent to or received from other hosts.

TotPkts

The *TotPkts* refers to the total number of packets that have been either sent from or received at that endpoint, i.e. the sum of RcvPkts and SentPkts. *Int* refers to packets that are sent from the host to and *Ext* refers to packets that are sent to or received from other hosts.

RcvBytes

The *RcvBytes* refers to the total number of bytes received at that endpoint over a given sample period, i.e. the sum of the packet size of all packets where the endpoint was the destination field in the packet.

RcvPkts

The *RcvPkts* refers to the total number of packets received at that endpoint over a given sample period, i.e. the count of all packets where the endpoint was the destination field in the packet.

SentBytes

The *SentBytes* refers to the total number of bytes sent from that endpoint over a given sample period, i.e. the sum of the packet size of all packets where the endpoint was the source field in the packet.

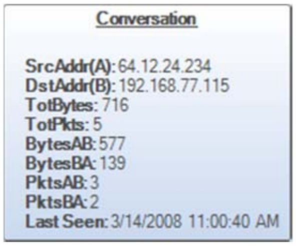
SentPkts

The *SentPkts* refers to the total number of packets sent at that endpoint over a given sample period, i.e. the count of all packets where the endpoint was the source field in the packet.

Last Seen

The *Last Seen* refers to the last time a packet with either the source or the destination field of the endpoint was seen.

Conversation



Conversation

SrcAddr(A): 64.12.24.234
DstAddr(B): 192.168.77.115
TotBytes: 716
TotPkts: 5
BytesAB: 577
BytesBA: 139
PktsAB: 3
PktsBA: 2
Last Seen: 3/14/2008 11:00:40 AM

Tooltip 3 Conversation Ring Conversation

When hovering over a connection, a tooltip pops up with the following fields:

SrcAddress(A)

The *SrcAddress(A)* refers to the source address in the first packet for that connection.

DstAddress(B)

The *DstAddress(B)* refers to the destination address in the first packet for that connection.

TotBytes

The *TotBytes* refers to the total number of bytes sent between the SrcAddress and DstAddress over the given sample period and is the sum of BytesAB and BytesBA.

TotPkts

The *TotPks* refers to the total number of packets sent between the SrcAddress and DstAddress over the given sample period and is the sum of PktsAB and PktsBA.

BytesAB

The *BytesAB* refers to the total number of bytes sent from the SrcAddress and DstAddress over the view’s sample period.

BytesBA

The *BytesBA* refers to the total number of bytes sent from the DstAddress to the SrcAddress over the view’s sample period.

PktsAB

The *PktsAB* refers to the total number of packets sent from the SrcAddress to the DstAddress over the view’s sample period.

PktsBA

The *PktsBA* refers to the total number of packets sent from the DstAddress to the SrcAddress over the view’s sample period.

Last Seen

The *Last Seen* refers to the last time a packet was seen with the source and destination field being the endpoints of the connection.

Sequence Diagram

The sequence diagram presents a sequential analysis of transactions and messages between hosts. The chart represents hosts as vertical lines arranged over the X axis, and messages as arrows between the hosts. The vertical axis represents time proceeding downward, which can be either relative (default) or absolute.

Layers

The chart can display data in one of two layers. The *Transport* layer displays each packet in the trace as a separate message in the sequence diagram. The *Application* layer decodes the packets for supported protocols and displays the protocol-specific messages. The user can toggle between these layers to gain different understandings of the underlying network transaction(s).

For example, the figures below show both the transport layer view and the application layer view for an HTTP download transaction. In the transport layer, separate message arrows show the three way TCP handshake to establish the connection, and then each data and acknowledgement packet in the exchange. In the application layer, on the other hand, only three messages are shown – one to establish the TCP connection, one to represent the HTTP GET request, and one to represent the HTTP response.

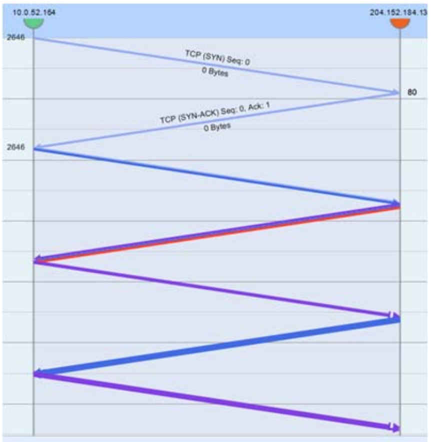


Chart Figure 9 Transport Layer View

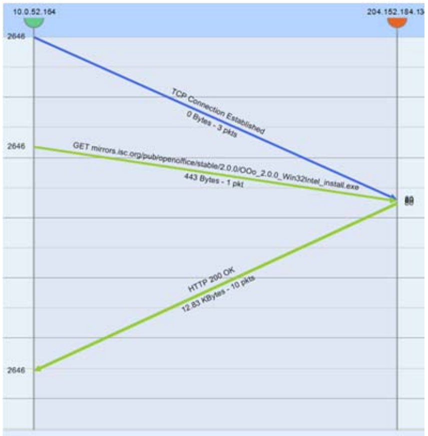

10.0.52.164
204.152.184.13
2646
TCP Connection Established
0 Bytes - 3 pkts
2646
GET mirrors.isc.org/pub/openoffice/stable/2.0.0/OOo_2.0.0_Win32Intel_install.exe
443 Bytes - 1 pkt
80
HTTP 200 OK
12.83 KBytes - 10 pkts
2646

Chart Figure 10 Application Layer View

Node

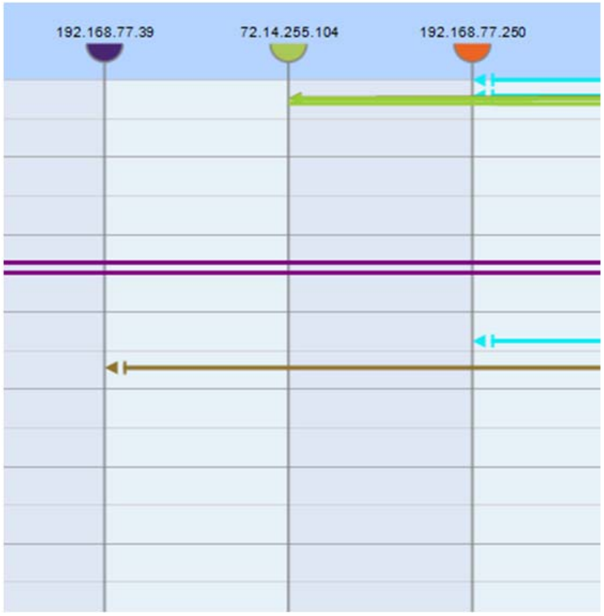


Chart Figure 11 Sequence Diagram nodes

Nodes are visualized over the X axis and separated by columns of different shades of grey to emphasize the space among them.

A node is represented by three graphic objects:

Head
: Half circles with a color for each host. Using the node head, it is possible to select, highlight and drag the node itself;

Body
: Gray vertical line where messages arrive and leave; the body also allows selecting and highlighting the node itself;

Label
: Node name, which is typically the IP address of the host or its resolved DNS name.

The node depiction varies based on selection and highlighting:

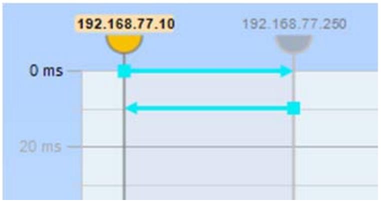


Chart Figure 12 Selected node

If a node or message is selected (i.e. clicked), then the label is bolded and is given a background color. The label, head and body of all other nodes are grayed out.

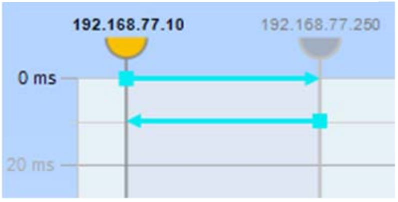


Chart Figure 13 Highlighted node

If a node is highlighted (i.e. by hovering the mouse on it), its label is bolded, and all other nodes are grayed out.

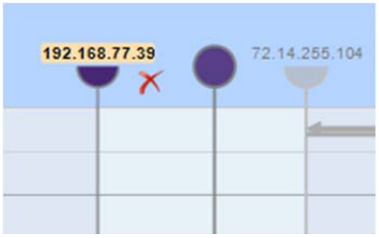


Chart Figure 14 Dragged node

When dragging a node, it is represented as a transparent full circle head with no label. The node also stays in its original place until the drag is complete.

Node Layout

The Sequence Diagram has a minimum column width which constrains the total number of nodes that can be shown to ensure they can be displayed properly. When a view is applied, the graph selects a default initial column width, and using the horizontal scroll bar, the user can scroll and zoom to change the set of displayed nodes.

By default, the chart arranges the nodes from left to right based on the timestamp of the first message sent or received by the node. Users can override this ordering by dragging nodes and/or hiding nodes to reduce the number in the display.

Selection

When selecting a node, the selection includes all messages sent or received by the specific host. If multiple nodes are selected (by pressing Control key), the selection includes only messages between the set of selected nodes.

When holding the Shift key and selecting a node, the selection toggles among:

- All messages sent or received by the specific host;
- All messages sent by the selected host;
- All messages received by in the selected host.

Highlight

When highlighting (hovering over) a single node, the chart highlights all messages sent or received by the highlighted host. If multiple selection is enabled (by pressing the Control key) and at least one other node has been selected, the chart highlights only messages between the selected host(s) and the highlighted one.

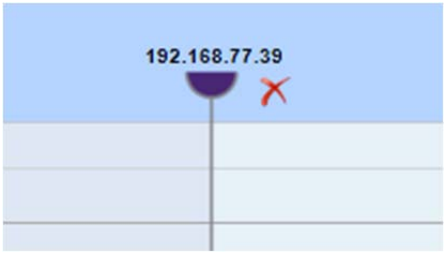


Chart Figure 15 Hide button

Also, when highlighting a host, the “Hide” button is shown to allow the user to hide the node itself, only if the column width is large enough to display it without overlapping the adjacent nodes.

Drag

As mentioned previously, users can manually arrange the order of the nodes by dragging hosts in different positions.

Additionally, the user can use the selection to define a filter by dragging the selected node(s) over the Filter panel or the Filter Bar. This action creates a Pilot filter for the selected host(s) and can then be used for additional views.

Node Context Menu

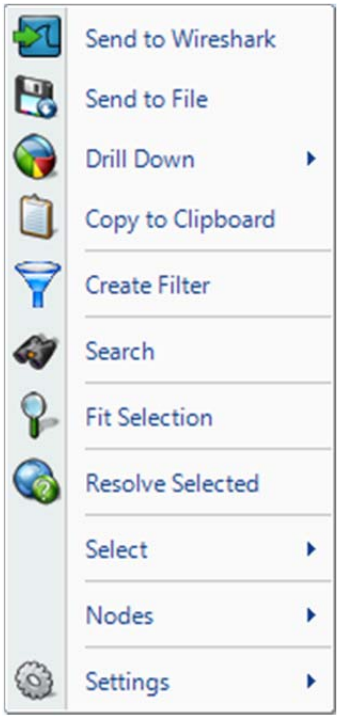


Chart Figure 16 Node Context menu

With one or more nodes selected, the context menu provides the following options:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected host(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected host(s) to a user-specified trace file that will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected host(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies a tabular form of the selected data to the system clipboard.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Fit Selection

The *Fit Selection* menu option arranges the horizontal range to fit the selected nodes.

Resolve Selected

The *Resolve Selected* menu option resolves the IP addresses of the selected nodes.

Select

The *Select* menu option allows user to control which messages are selected based on the set of selected hosts. If only one host is selected, options include selecting all messages from or to the node, all messages from the node or all messages to the node.

If two nodes have been selected, options include selecting conversations between the selected nodes, all messages from the first node to the second or all messages from the second node to the first.

If more than two nodes are selected, the only option is to select all messages between the selected nodes.

Nodes

The *Node* menu provides options to control which nodes are hidden or shown.

Show All:

Shows all hidden nodes.

Show Selected Only:

Hides all nodes but the selected one(s).

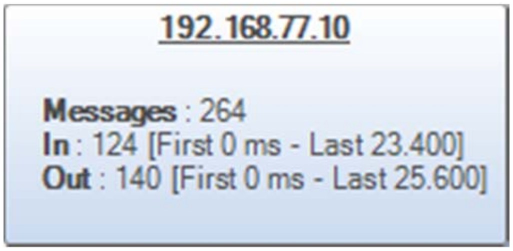
Show All But Selected:

Hide the selected nodes and show all others. Note that at least two nodes must be visible at all times.

Inverse:

Inverts the hidden node set, by showing all hidden nodes and hiding all visible ones.

Tooltip



192.168.77.10

Messages : 264
In : 124 [First 0 ms - Last 23.400]
Out : 140 [First 0 ms - Last 25.600]

Chart Figure 17 Node tooltip

The node tooltip shows data about the node itself.

Node label

IP address of the highlighted node.

Messages

Statistics about the number of messages to and from the highlighted node, as well as timing information about the messages.

Message

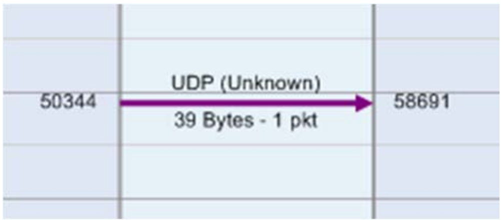


Chart Figure 18 Sequence message

A message is displayed as an arrow from the source host line to the destination host line.

The arrow itself is graphically composed by:

Shaft

Represents the body of the message as a line between source and destination nodes.

Head

Represents the arrival of the message as a triangle pointing at the destination node.

Nock

Represents the source of the message as a square at the source node (only in “Ruler Mode”).

Labels

Shows text information about the message, including the protocol, packet and byte count, etc.

Compression

The diagram applies a compression algorithm over the set of messages to maximize performance and clarify the display. The algorithm can both reduce the number of displayed messages and change the message layout.

First, message labels are not displayed if there is not enough room to show them. Second, overlapping messages are combined into a group messsage. A group message uses a special nock and head to inform the user that it represents more than one message. A highlighted or selected group message does not show Top, Bottom and Main labels.

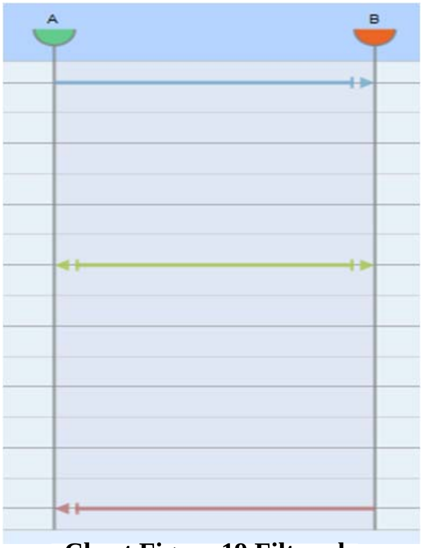
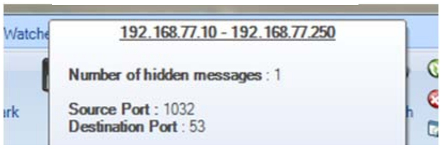


Chart Figure 19 Filtered messages

If all messages in the group have the same orientation, then the arrow is shown in one direction. Otherwise it is shown with nock and head in both directions.

When all messages in a group have the same source and destination ports, then they are shown. Otherwise, they are not. The group message tooltip shows the number of hidden messages.



192.168.77.10 - 192.168.77.250

Number of hidden messages : 1

Source Port : 1032
Destination Port : 53

Chart Figure 20 Group message tooltip

Message and node status

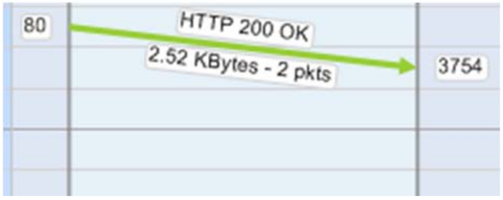


Chart Figure 21 Highlighted message

If a message is selected or highlighted, it is brought to the foreground, increasing the likelihood that the label will be displayed.

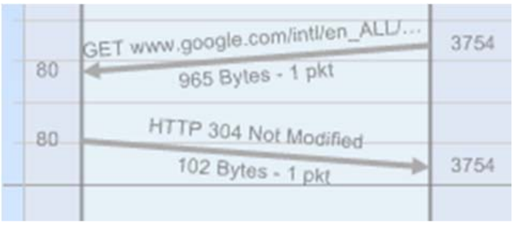


Chart Figure 22 Not focused message

Messages that are not selected or highlighted are greyed out to emphasize the selected ones.

Selection

Selecting one or more messages also selects the nodes that are the source or destination for one or more of the messages.

Highlight

Highlighting a single message causes the chart to highlight the source and destination nodes.

Double click

Double clicking on a message toggles between the layers and zooms the display to fit the message in the time range.

Context Menu

By selecting one or more messages, the following actions can be performed through the context menu.

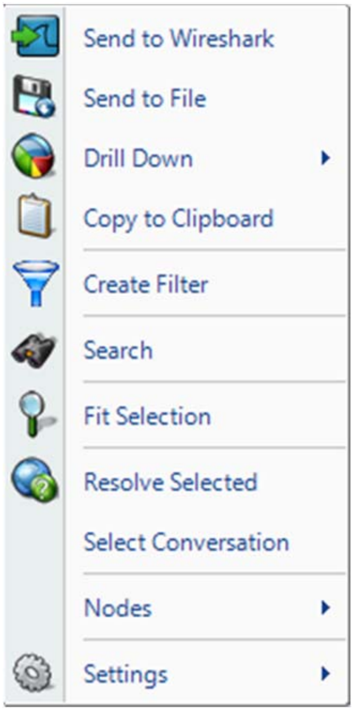


Chart Figure 23 Message context menu

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected message(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected message(s) to a user-specified trace file that will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected message(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies a tabular form of the selected data to the system clipboard.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the Sequence Diagram and adds the filter to the Filter List. The filter comprises the core message attributes: source and destination address, source and destination port numbers, start and end time.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Fit Selection

The *Fit Selection* menu option sets the horizontal range to fit the source and destination nodes and the vertical range to fit the start and end times of the selected message. If more than one message is selected then the minimum start time and maximum end time are used.

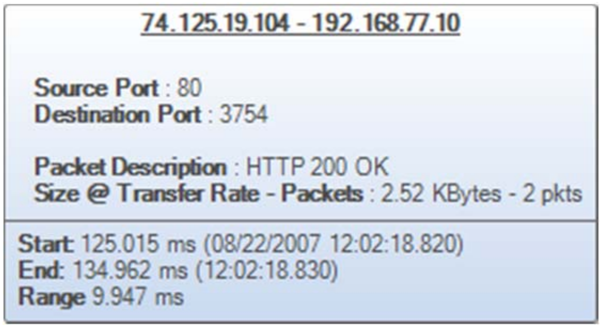
Resolve Selected

The *Resolve Selected* menu option resolves the IP addresses of the selected source and destination nodes.

Select Conversation

The *Select Conversation* selects all messages with the same source and destination IP addresses and source and destination ports as the selected message.

Tooltip



74.125.19.104 - 192.168.77.10

Source Port : 80
Destination Port : 3754

Packet Description : HTTP 200 OK
Size @ Transfer Rate - Packets : 2.52 KBytes - 2 pkts

Start: 125.015 ms (08/22/2007 12:02:18.820)
End: 134.962 ms (12:02:18.830)
Range 9.947 ms

Chart Figure 24 Message tooltip

The message tooltip shows information about the message itself

Tooltip header

Comprises the source and destination IP addresses.

Tooltip body

Displays the port numbers, a description of the message, and its sizing information.

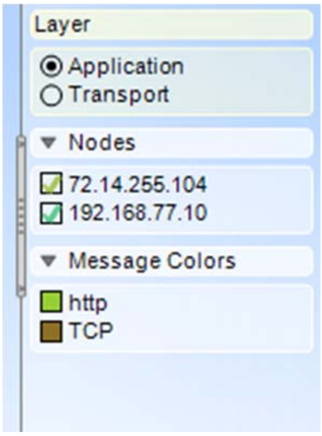
Tooltip footer

Shows statistics about the start and end time in both absolute and relative terms.

Legend area

The Legend area always occupies the right side of the chart. It contains a set of legends that show information about the displayed diagram and enable interaction with the chart. The legend can be resized by dragging the handle, or collapsed and expanded by double clicking the handle.

The legend area contains the following legends:



Layer
● Application
○ Transport

▾ Nodes
☑ 72.14.255.104
☑ 192.168.77.10

▾ Message Colors
🟩 http
🟫 TCP

Chart Figure 25 Sequence legend area

Layer

Shows the currently selected layer and enables switching between layers.

Nodes

Checkbox list of nodes in the current sequence diagram. Enables selecting one or more hosts, highlighting a single host and hiding or showing a host by clicking the label icon.

Message Colors

List of colors used by messages in the current sequence layers and their meaning. Clicking on a color highlights all messages having the highlighted color.

Both the Message Colors and the Nodes legends can be expanded or collapsed by clicking the header.

Scroll bar

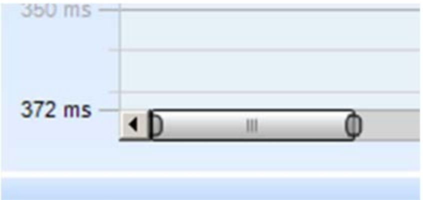


Chart Figure 26 Scroll bar

Scroll bars enable interaction with both the X and Y axis. In addition to panning left and right and up and down by dragging the scroll thumb, the user can expand or contract the view by dragging the ends of the thumb.

Time Filter

By selecting a vertical region, the user selects a time range. All messages starting within the time range are displayed as selected. In the time selection area is possible to perform the following actions:

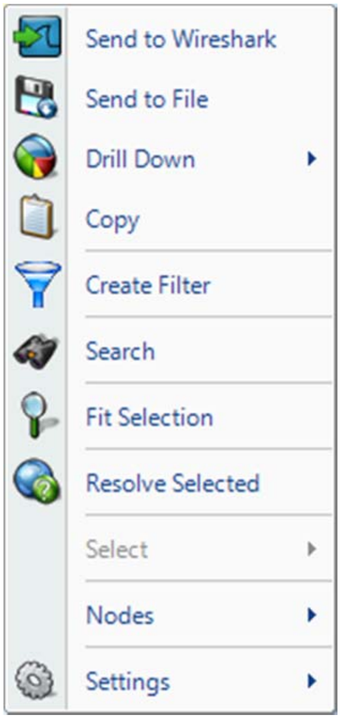


Chart Figure 27 Time Filter Context Menu

Context Menu

Send to Wireshark

The *Send to Wireshark* menu option sends all the traffic within the selected time range to Wireshark.

Send to File

The *Send to File* menu option sends all the traffic within the selected time range to a user-specified trace file that will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected time range and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies a tabular form of the data within the selected time range to the system clipboard.

Create Filter

The *Create Filter* menu option creates a time filter based on the current time selection.

Double Click

Double click expands the current time range to reflect the time filter range.

Dragging

The time selection can be used to create a time filter by dragging it on the Filter panel or the Filter Bar. Also, dragging the time selection onto a different Sequence Diagram or Strip Chart highlights the messages in the other chart that fall within the selected time range.

A time selection can be removed by clicking on the area outside and hosts grid or, after a double-click, by clicking over the area itself.

Ruler Mode

Ruler mode displays detailed timing information about one or more messages. It is activated by clicking the mode icon.

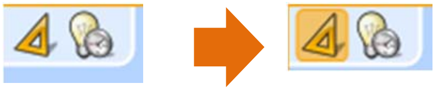


Chart Figure 28 Ruler Mode Icon

The system shows timing information in two modes:

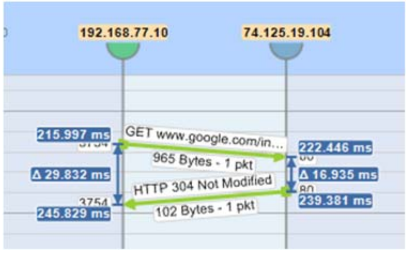


Chart Figure 29 Node ruler mode

Node Mode

When a message is selected or a time range is created, the diagram shows the start time, end time and delta value between the first and the last message in the range.

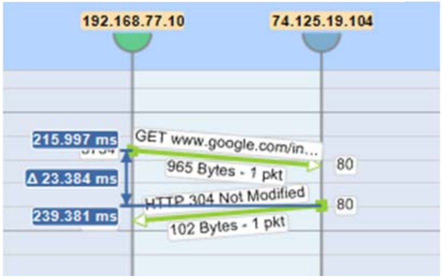


Chart Figure 30 Global ruler mode

Message Mode

When a first message terminator (nock or head) is clicked, followed a second terminator, the system shows the timing of the two messages as well as the interval between them.

If a third terminator is selected, the initial selection is retained, and the system updates to show the timing information between the first message terminator and the newly clicked one. Selecting another message or clicking in the background will clear the original selection.

Time Hints

Time hints enable the sequence diagram to visually represent the network delay between nodes. The feature is activated or deactivated using the icon in the upper-left corner of the chart.

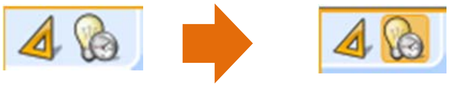


Chart Figure 31 Time Hints Icon

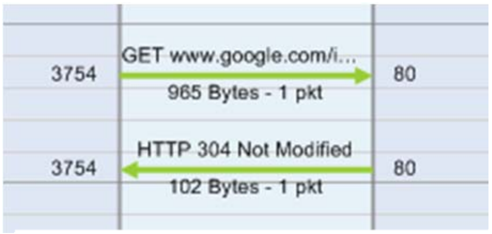


Chart Figure 32 Time without hints

When time hints are disabled, all messages are shown as horizontal lines, where the Y axis value represents the message timestamp as recorded in the trace file.

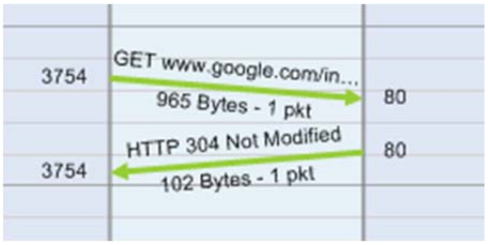


Chart Figure 33 Time with hints

When time hints are enabled, the network delay is inferred from the TCP calculations, and the message lines are drawn with a slope that illustrates the network delay.

Strip Chart

The Strip Chart displays quantitative data with respect to time.

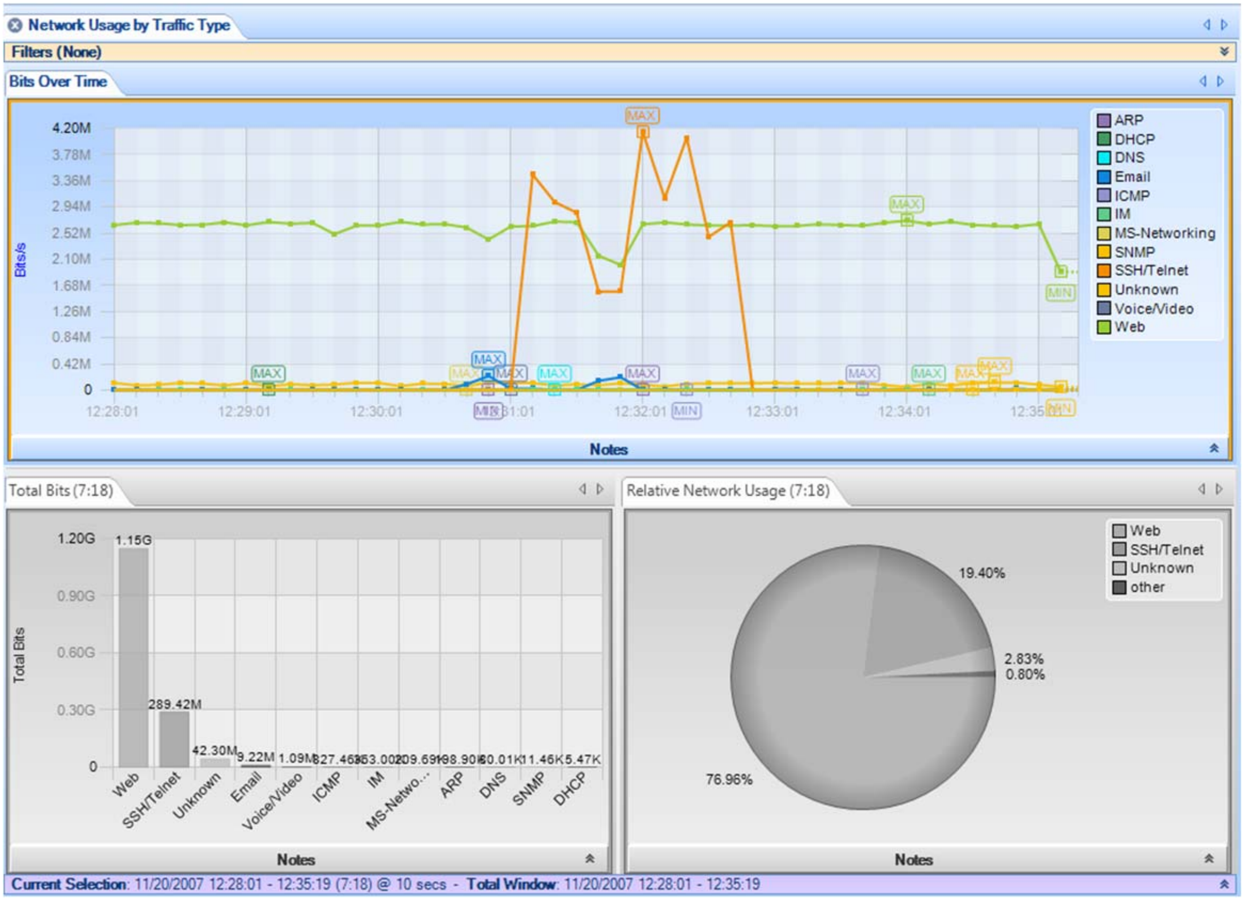
Diagram

The Strip Chart diagram has the following elements:

- Time Control Area
- Legend
- Data area
- Min/Max

Current Selection Interval

This is an Example of a View containing a Strip Chart:



Current Selection: 11/20/2007 12:28:01 - 12:35:19 (7:18) @ 10 secs - **Total Window**: 11/20/2007 12:28:01 - 12:35:19

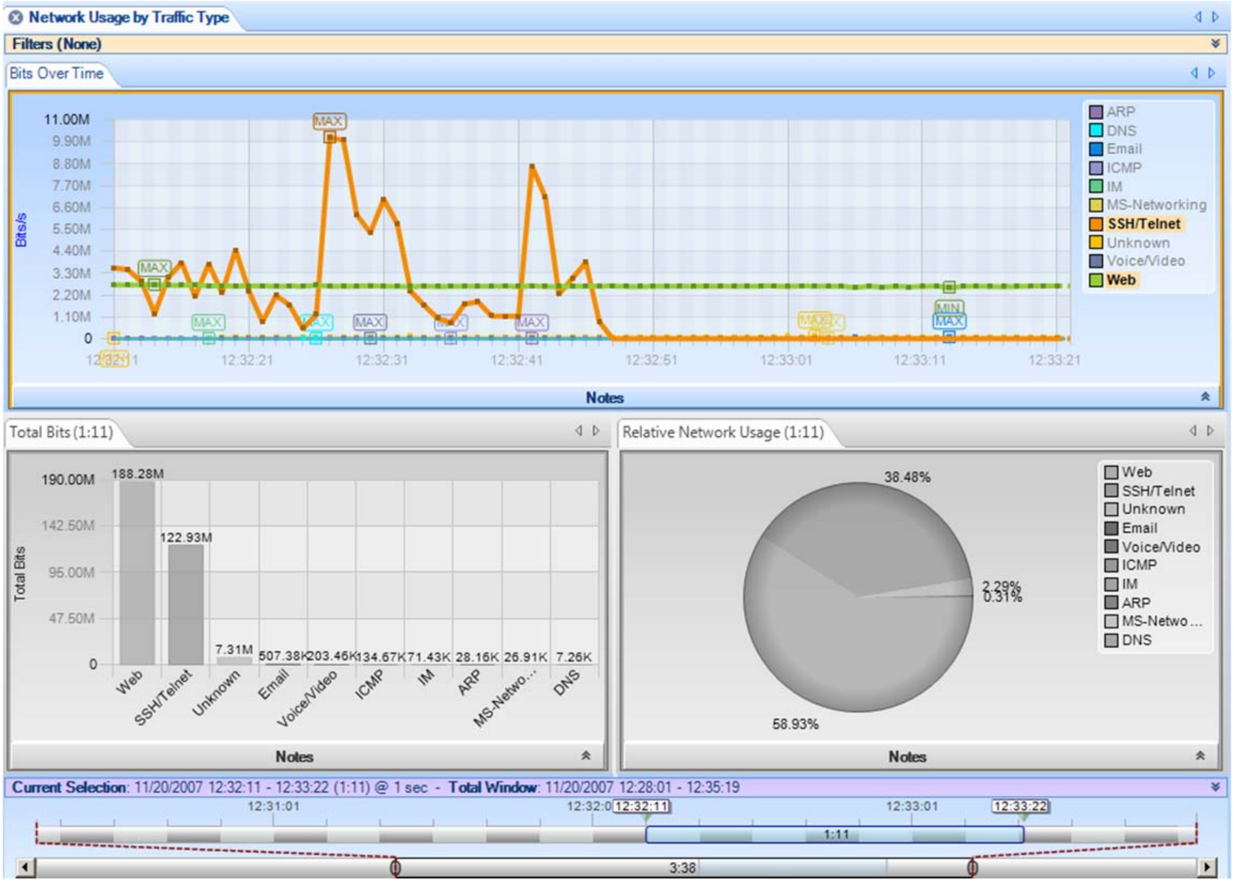
Figure 144: Strip Chart

Note: ***The Current Selection bar (at the bottom of the View) simultaneously applies to all of the Charts contained in a View.***

The View depicted above consists of 3 charts, namely, a strip chart, a bar chart, and a pie chart. This section discusses the strip chart (the top-most chart).

Current Selection: The data points displayed in the strip chart correspond to the View metric (Bits per Second) computed over the *Current Selection* Interval.

Total Window: The *Total Window* interval shows the total duration of the source trace file or, for a live source, the total duration of the capture or the Data Retention Time, whichever is smaller.



Current Selection: 11/20/2007 12:32:11 - 12:33:22 (1:11) @ 1 sec - Total Window: 11/20/2007 12:28:01 - 12:35:19

Figure 145: Strip Chart with Horizontal Zoom

Figure 145 shows the strip chart "zoomed" horizontally using the Selection bar in the Time Window. The Time Control Ribbon can also be used to set the duration and location of the Current Selection. The minimum and maximum values in the Current Selection are displayed (unless they are obvious from the context).

Along with the "Sampling Time" and "Data Retention Time" options as previously described, the Strip Chart can be customized by:

- Toggling legend visibility
- Rescaling Y Axis

Selection

The Strip Chart supports two types of selection:

- Time based
- Line based

Time Based Selection

A *Time Based Selection* can be applied to any Strip Chart and is performed by clicking and dragging the mouse over a time period. An example result is shown below:

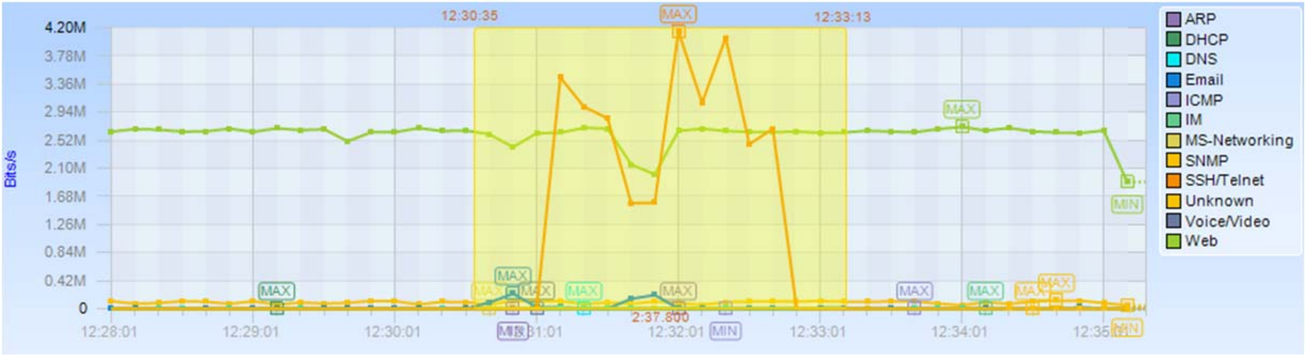


Chart Figure 34 Strip Chart Selection (Time)

Note that multiple selection cannot be performed using time-based selection.

Line Based Selection

A *Line Based Selection* can be applied to Strip Charts where more than one metric is being displayed, for example in the case of multiple protocols over time:

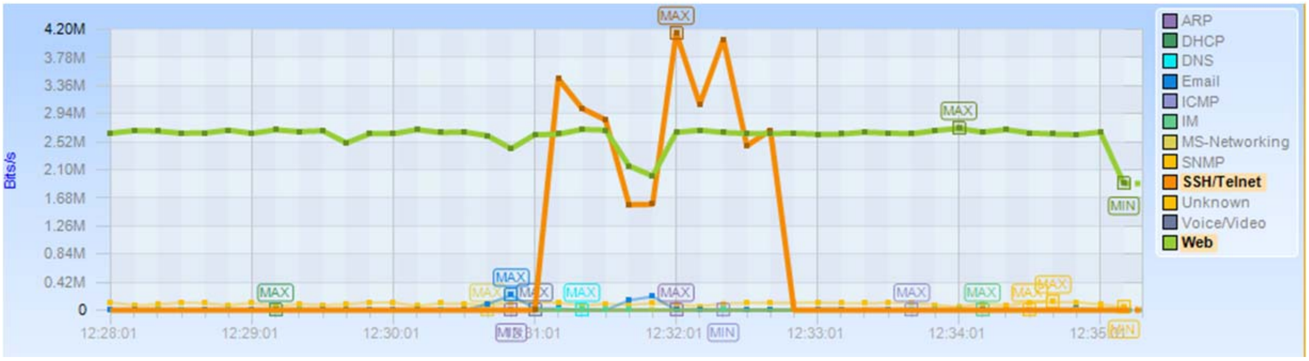


Chart Figure 35 Strip Chart Selection (Element)

Individual lines are selected by clicking either on the line itself, or its representation in the legend. Multiple lines can be selected clicking with the Control key pressed.

Mini

The miniature view of the strip chart is shown when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no context menu. The legend disappears and a gray border appears around the image.

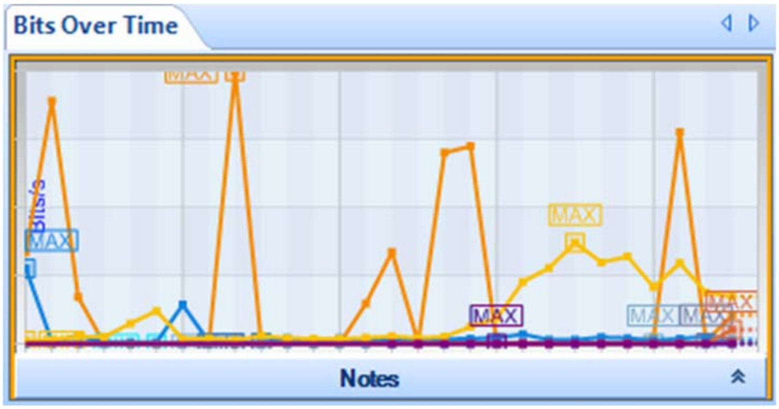
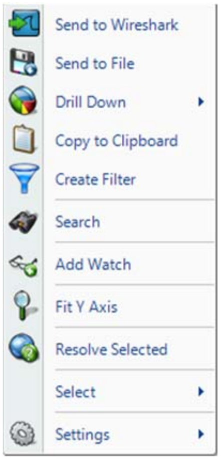


Chart Figure 36 Strip Chart Mini

Context Menu



Context Menu 27 Strip Chart (Selection)

The context menu for the Strip Chart has the following options:

Send to Wireshark

The *Send to Wireshark* menu option will send the traffic from the selected time slice or line(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option will send the traffic from the selected time slice or line(s) to a user-specified trace file that will appear, after completion, in the Files panel, for immediate analysis.

Drill Down

The *Drill Down* menu option will apply the user-specified view to the selected time slice or line(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu copies a tabular form of the selected data to the system clipboard.

Create Filter

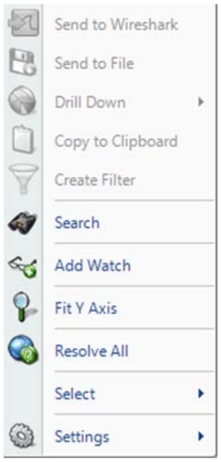
The *Create Filter* menu option creates a filter based on the current selection within the strip chart and adds the filter to the Filter List.

Search

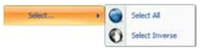
The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Add Watch

The *Add Watch* menu option opens up the Watch Editor dialog window. The Trigger Condition is based on the currently selected strip chart. The Data Filter, if any, is based on the line selection within the strip chart.



Context Menu 28 Strip Chart (No Selection)



Context Sub Menu 7 Select

Fit Y Axis

Scale the vertical height of the strip chart to fit within the chart.

Time Display Format

See below.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves the Port Name, IP Address, or Mac Address of all elements in the Strip Chart that were not automatically resolved.

Select

The *Select* menu option has two submenu options described at the beginning of this section. However, since multiple selections cannot be done with time slices, the invert option is only available after line selection.

Settings

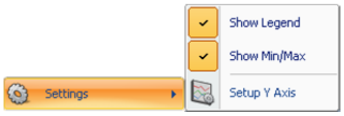
The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

Context Sub-Menu

The Strip Chart has the following contextual submenu:

- Settings

Settings



Context Sub Menu 8 Strip Chart Settings

The Settings context submenu for the Strip Chart has the following options:

Show Legend

Toggle off or on the legend for the Strip Chart.

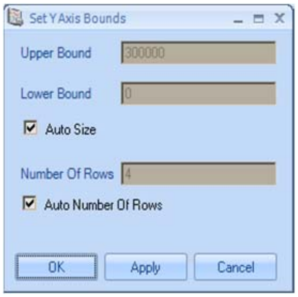
Show Min/Max

Toggle off or on the display of minimum and maximum text indications next to the minimum and maximum values for a line.

Setup Y Axis

Opens up a separate dialog box, which is described next.

Dialogs



Set Y Axis Bounds

Upper Bound: 300000

Lower Bound: 0

☑ Auto Size

Number Of Rows: 4

☑ Auto Number Of Rows

Dialog 1 Strip Chart Settings

The Set Y Axis Bounds dialog box is opened from the context menu underneath the Settings submenu. When opened, it has the following parameters:

Upper Bound

Set the upper Y axis bound for the Strip Chart.

Lower Bound

Set the lower Y axis bound for the Strip Chart.

Auto Size

Handle the upper and lower bounds of the Strip Chart automatically.

Number Of Rows

The number of division increments on the Y Axis. For instance, if the lower bound is 0 and the upper bound is 100 and the *Number Of Rows* is set to 10, then the Y axis will increment by units of 10 and there will be 10 alternating colors in the horizontal axis of the chart.

Auto Number Of Rows

Calculate the Number Of Rows of the Strip Chart automatically.

Tooltips

The tooltips for the Strip Chart show the full quantitative value of a specific sample point of the element in the data area.

Bar Chart

This chart displays quantitative metrics in a graphical bar based chart. It is used when there is a known domain for a metric and division of the domain is useful. Quantities are graphically represented and restricted to a linear scale.

There are three types of Bar Charts:

- Single Bars
- Stacked Bar Chart
- Grouped Bars

Single Bar Chart

Single Bar Charts are the most basic form of Bar Charts. Each column is a single valued bar. The colors of the bars match the labels in the legend.

Along with the “Sampling Time” and “Date Retention Time” options as previously described, the Single Bar Chart is customizable in the following ways:

- Reorder Bars
- Rescale Y-Axis
- Toggle legend visibility
- Toggle label visibility above individual bars
- Select value or percentage as label

Default

This is an example of the default view for a Single Bar Chart:

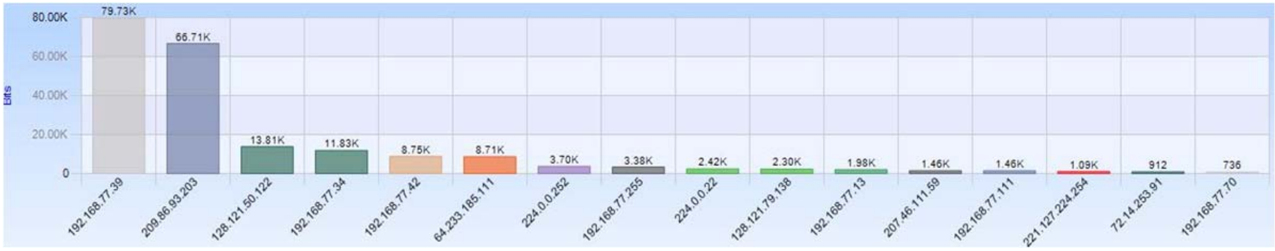


Chart Figure 37 Single Bar Chart

Selection

A bar in a Single Bar Chart is selected by clicking on the bar itself, its column, or its representation in the legend. Clicking with the Control key pressed is supported for multiple selection.

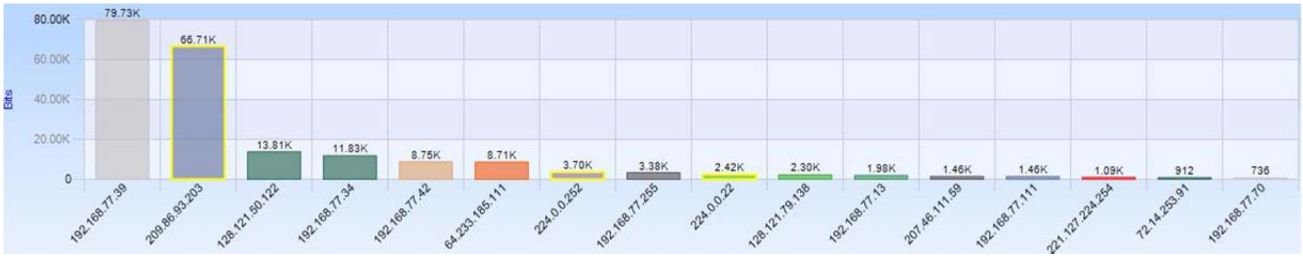


Figure 38: Bar Chart Multiple Selection

Mini

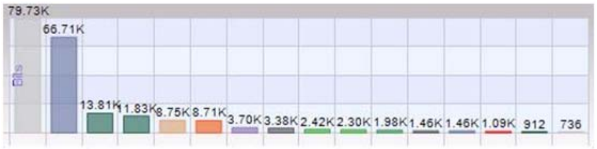


Figure 146: Single Bar Chart Mini

The miniature view is shown when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no context menu.

Stacked Bar Chart

A *Stacked Bar Chart* is similar to a Single Bar Chart except that each column is subdivided into predetermined constituents. These constituent components can be selected and analyzed individually or collectively.

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Stacked Bar Chart is customizable in the following ways:

- Sort Bars
- Rescale of Y-Axis
- Toggle of legend visibility
- Toggle of label visibility above individual bars
- Select value or percentage as label

Default

This is an example of the default view for a Stacked Bar Chart:

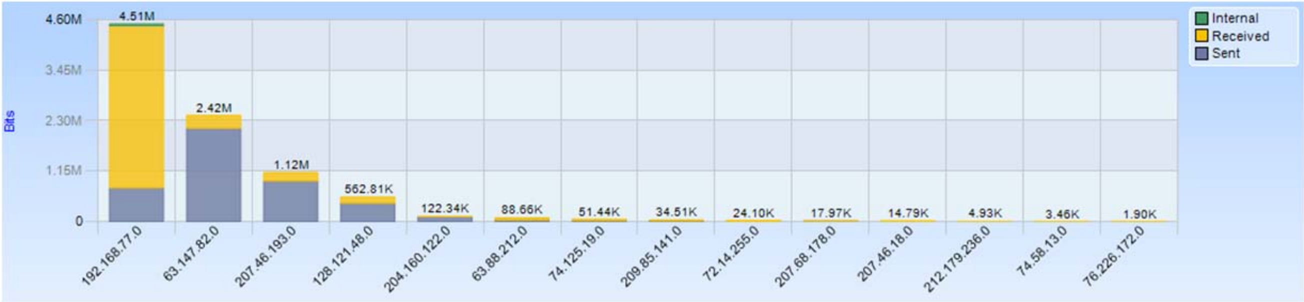


Chart Figure 39 Stacked Bar Chart

Selection

A bar in a Stacked Bar Chart is selected by clicking on the bar itself, its column, or its representation in the legend. Clicking with the Control key pressed is supported for multiple selection.

Mini

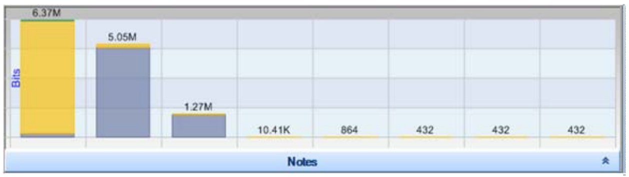


Figure 147: Stacked Bar Chart Mini

The miniature view is shown when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Grouped Bar Chart

A *Grouped Bar Chart* is similar to a Single Bar Chart except that each column is subdivided into two or more sub columns.

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Grouped Bar Chart is customizable in the following ways:

- Sort Bars
- Rescale Y-Axis
- Toggle legend visibility
- Toggle label visibility above individual bars
- Select value or percentage as label

Default

This is an example of the default view for a Grouped Bar Chart:

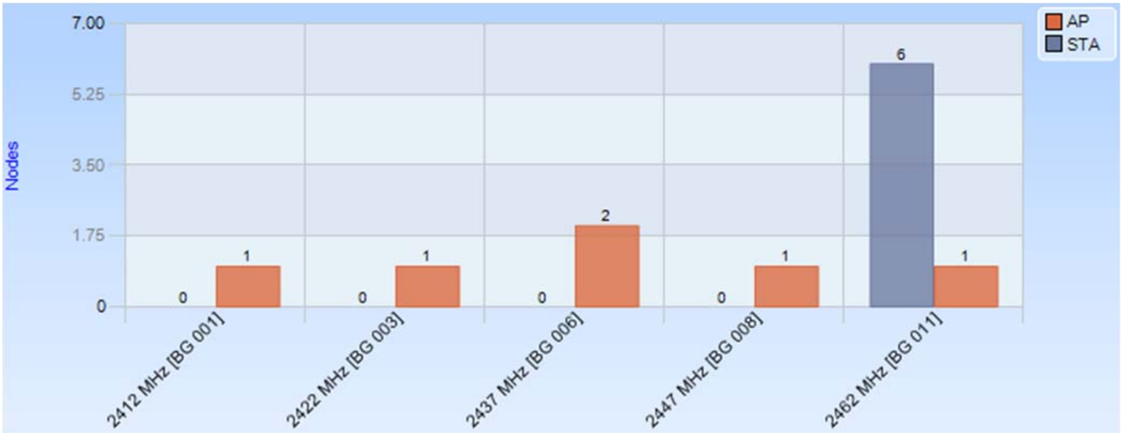


Chart Figure 40 Grouped Bar Chart

Selection

Selection of the Grouped Bar Chart can happen three ways:

- Selection of a column.
- Selection of one of the components of a column.
- Selection of all instances of a certain subcomponent across all columns.

Column

A *column based* selection selects all data corresponding to the column. This method of selection is achieved by selecting the area around the bar with respect to the desired column inside the chart, but not the bar itself.

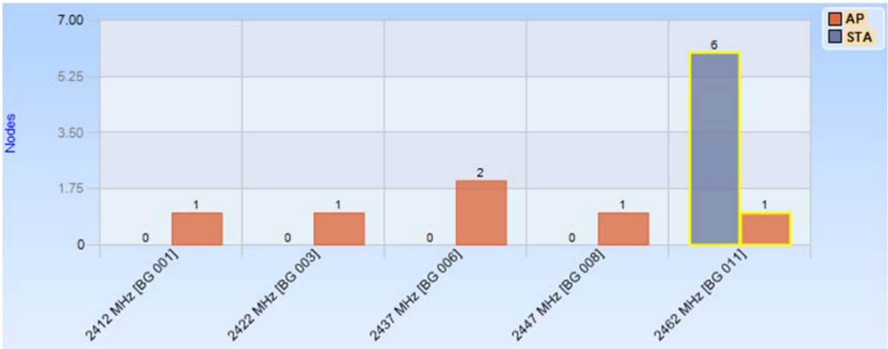


Chart Figure 41 Grouped Bar Chart Selection (Column)

Component Instance

A *component instance based* selection selects a subset of the data in a particular column. This method of selection is achieved by clicking on the component.

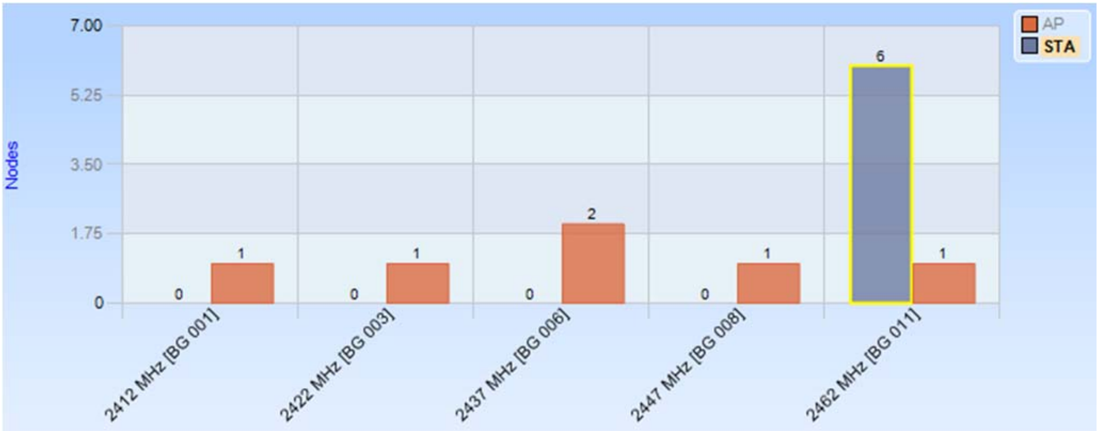


Chart Figure 42 Grouped Bar Chart Selection (Component Instance)

Component

A *component based* selection selects data in all columns for a particular component subset. This method of selection is achieved by clicking on the representation of the component in the legend.

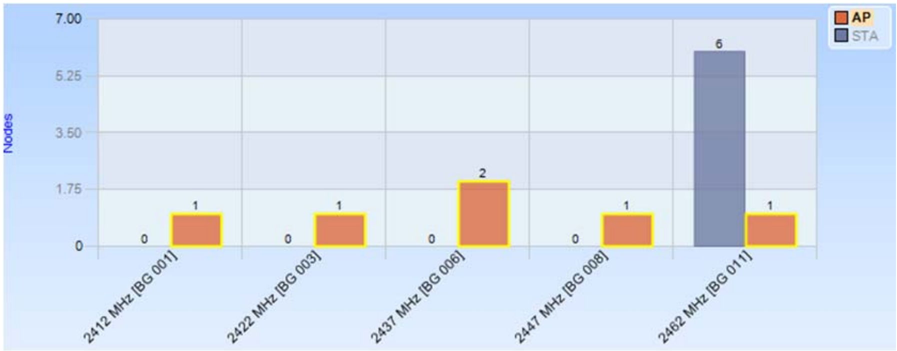


Chart Figure 43 Grouped Bar Chart Selection (Component)

Mini

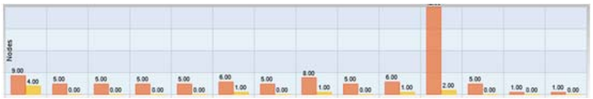


Chart Figure 44 Grouped Bar Chart Mini

The miniature view of the bar chart is shown when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Navigation Through Data

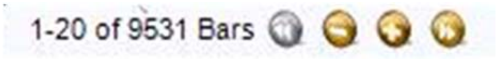


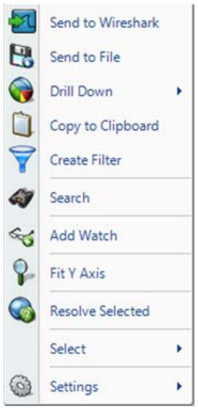
Chart Figure 45 Bar chart Top Bars

When there is not enough space to display clearly all the bars in a single chart, the system automatically ranks and displays data by relevance, based on the selected sorting option.

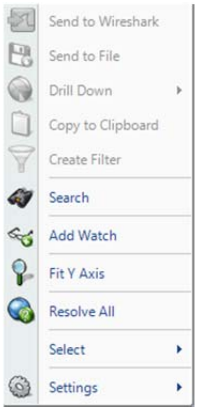
By default, the columns are sorted from high to low (usually by value). A small label displaying the total number of bars and the current interval is shown at the bottom of the view. One can navigate through data using the four buttons in the label. + and - buttons increase or decrease the length of the interval shown, while the arrows (<< and >>) shift the interval inside the data.

Context Menu

All three types of Bar Charts; Single, Stacked, and Grouped, share the same context menu (with a single exception noted below).



Context Menu 29 Bar Chart (Selection)



Context Menu 30 Bar Chart (No Selection)

Context Sub Menu 9 Select

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected bar(s) or component(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected bar(s) or component(s) to a user-specified trace file that will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected bar(s) or components(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies a tabular form of the selected data to the system clipboard.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the bar and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Add Watch

The *Add Watch* menu option opens up the Watch Editor dialog window. The Trigger Condition is based on the currently selected bar chart. The Data Filter, if any, is based on the bars selected within the bar chart (if any).

Fit Y Axis

The *Fit Y Axis* menu option resizes the Y scale of the Bar Chart so that the largest bar is equal to the height of the chart.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves the Port Name, IP Address, or Mac Address of the bar(s) in the Bar Chart but only when that to be resolved is not selected for automatic resolution in the Name Resolution submenu available in the Home Ribbon.

Select

The *Select* menu option provides the option to select the bar(s) and component(s) of the Bar Chart. Inverting the selection of bar(s) and component(s) is currently disabled for Bar Charts.

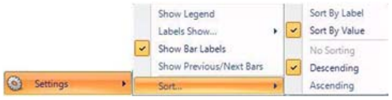
Settings

The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

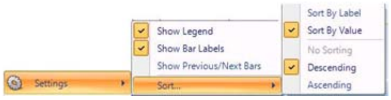
Context Sub-Menus

The Bar Charts have one contextual submenu:

- Settings



Context Sub Menu 10 Bar Chart Settings Single Bar



Context Sub Menu 11 Bar Chart Settings Staked Bars or Grouped Bars

The settings submenu for the Bar Chart context menu has several items:

Show Legend

The *Show Legend* menu option toggles off or on the Bar Chart legend.

Show Bar Labels

The *Show Bar Labels* menu option toggles off or on the Bar Chart labels.

Label Show

The *Label Show* menu option opens a submenu with two options for labels: Percentage or Value. This menu is available only in Single Bar Charts.

Sort

The *Sort* menu option opens a submenu with the following two sets of options.

The first set of mutually exclusive options:

Sort By Label

The *Sort By Label* menu option sorts the bars alphabetically by their labeled column names.

Sort By Value

The *Sort By Value* menu option sorts the bars numerically by their quantitative values.

The second set of mutually exclusive options:

No Sorting

The *No sorting* menu option disables sorting.

Descending

The *Descending* menu option sorts the bars sequentially from left to right, either by name or value, as specified by the first group.

Ascending

The *Ascending* menu option sorts the bars sequentially from right to left, either by name or value, as specified in the first group.

Tooltips

The tooltips for the Bar Chart display the label of the bar over which the mouse is hovering.

Scatter Plot

The *Scatter Plot* is a versatile and flexible chart that can display complex relationships between values using three dimensions:

- Y Axis
- X Axis
- Size of the circles, referred to as points

Each of these dimensions can be assigned to one of a predefined set of metrics. For instance, the user may specify that the Y-Axis represents either 802.11 Channel usage or average frame size.

Scatter Plots are most useful when there is expected to be a correlation between metrics, such as the total number of packets and the total bytes sent out by a host. For example, if the Y Axis is "Packet Count" and the X Axis is "Byte Count," then there is typically a diagonal line of points from the origin to the top right. An anomaly would then be visually evident if this relationship did not hold for certain situations.

Default

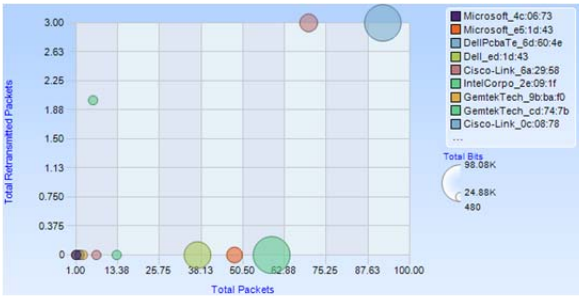


Chart Figure 46 Scatter Plot

Along with the "Sampling Time" and "Data Retention Time" options previously described, the scatter plot is customizable in the following ways:

- Assignment of the dot size relation
- Assignment of X-Axis
- Assignment of Y-Axis

Selection

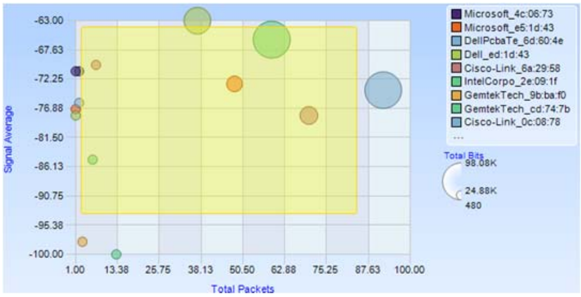


Chart Figure 47 Scatter Plot Draw Box

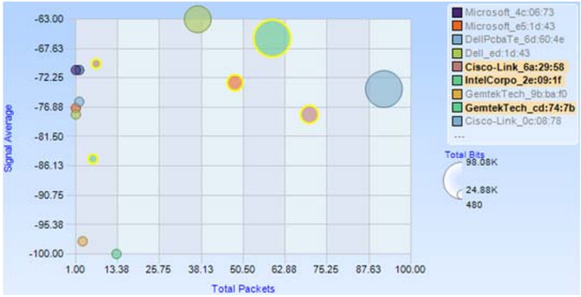


Chart Figure 48 Scatter Plot Multiple Selection

Selection in a Scatter Plot is done by one of four ways:

- Search operation
- Selection from the legend
- Drawing a box around the points
- Clicking on the Points to be selected

Clicking with the Control key pressed for multiple selection is supported for point based and legend based selection.

Mini

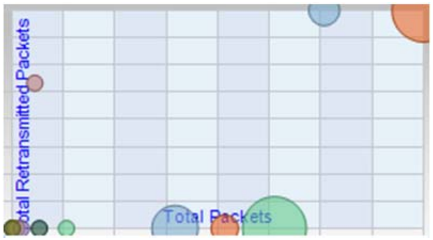
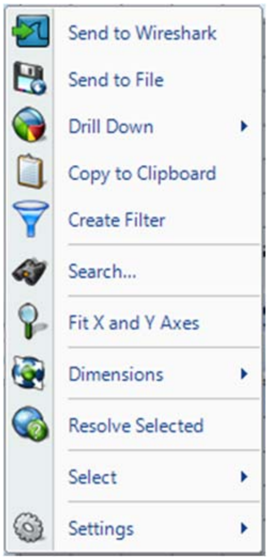


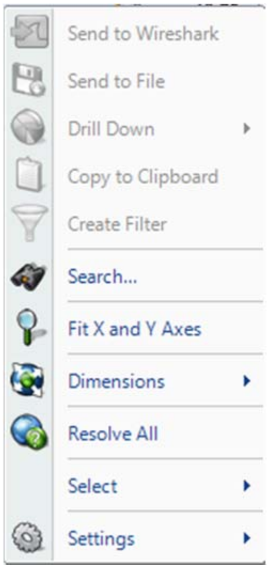
Chart Figure 49 Scatter Plot Mini

The miniature view is shown when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Context Menu



Context Menu 31 Scatter Plot (Selection)



Context Menu 32 Scatter Plot (No Selection)

Context Sub Menu 12 Scatter Plot Select

The context menu for the Scatter Plot is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected point(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected point(s) to a user-specified trace file that will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected point(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies a tabular form of the selected data to the system clipboard.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the scatter plot and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Fit X and Y Axes

The *Fit X and Y Axes* menu option resizes the X and Y scales of the Scatter Chart so that all values fit within the chart.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves the Port Name, IP Address, or MAC Address of the point(s) in the Scatter Plot. This option is available only when the fields are not automatically resolved (see the Name Resolution submenu available in the Home Ribbon).

Select

The *Select* menu option has two submenu options described at the beginning of this section with an option to either select the point(s) in the Scatter Plot, or inverts the selection of point(s).

Settings

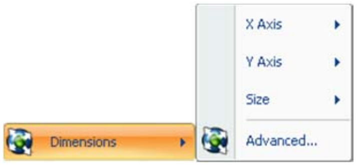
The *Settings* menu option opens up a sub-menu with specific settings for the chart. It is described below.

Context Sub-Menus

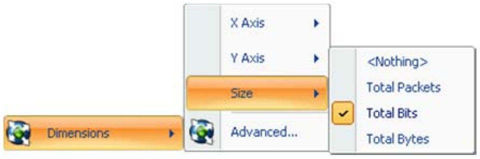
The Scatter Plot has three contextual submenus:

- Dimensions
- Select (shown above)
- Settings

Dimensions



Context Sub Menu 13 Scatter Plot Dimensions



Context Sub Menu 14 Scatter Plot Dimensions (Detail)

The Dimensions submenu for the Scatter Plot context menu has four items:

X Axis

The *X Axis* menu option presents all possible choices for the metric of the X-Axis. Some charts may only have one option, while others may have multiple; for instance, “Bits/s” versus “Bytes/s” or “Packets/s.”

Y Axis

The *Y Axis* menu option presents all possible choices for the metric of the Y-Axis. Some charts may only have one option, while others may have multiple; for instance, “Bits/s” versus “Bytes/s” or “Packets/s.”

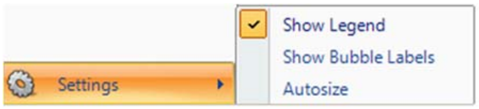
Size

The *Size* menu option has a submenu where the dot size of the points can be enabled and associated with a metric or disabled by selecting “Nothing.”

Advanced

The *Advanced* menu option opens up a separate dialog box.

Settings



Context Sub Menu 15 Scatter Plot Settings

The settings submenu for the Scatter Plot context menu has five items:

Show Legend

The *Show Legend* check box menu option toggles off or on the Scatter Plot legend.

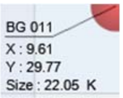
Show Bubble Labels

The *Show Bubble Labels* menu option toggles off and on the point labels, which can otherwise be viewed via a tooltip.

Autosize

The *Autosize* menu option toggles off and on whether the area will automatically resize based on maximum values.

Tooltips



BG 011
X : 9.61
Y : 29.77
Size : 22.05 K

Tooltip 4 Scatter Plot

A tooltip is shown when hovering over a point. It has the following values:

Name

The *Name* of the point being charted, such as an IP address or an 802.11 wireless channel.

X

The *X* value refers to the position the point currently occupies on the X axis and the significance of this with respect to the units for the X axis.

Y

The *Y* value refers to the position the point currently occupies on the Y axis and the significance of this with respect to the units for the Y axis.

Size

The *Size* value refers to the dot size of the point and the significance of this with respect to the units for the dot size.

Pie Chart

The *Pie Chart* shows quantitative values as a percentage of a whole. Pie Charts are useful for instance, when looking at local versus non-local traffic, or finding out what percentage of total traffic is constituted by a particular host. The elements of a Pie Chart are referred to as slices.

Default

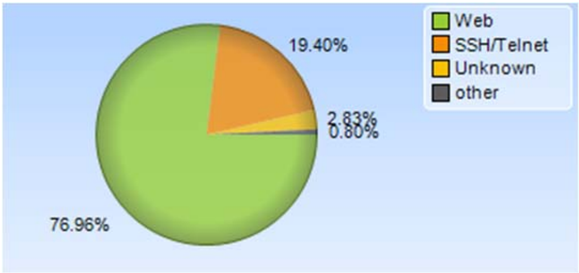


Chart Figure 50 Pie Chart

Along with the “Sampling Time” and “Data Retention Time” options previously described, the Pie Chart is customizable in the following ways:

- Toggle of percentage or quantitative value to be displayed for the time slices.
- Toggle of legend visibility.

The Pie Chart can be zoomed in and out using the scroll wheel on the mouse.

Selection

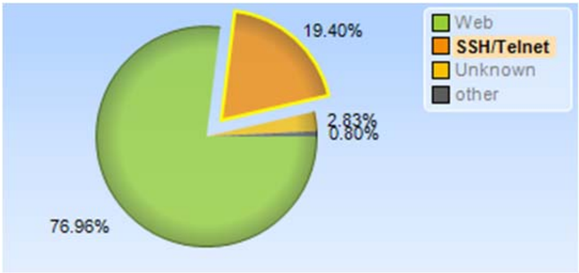


Chart Figure 51 Pie Chart Selection

Selection in a Pie Chart is done either by clicking on a slice in the Pie Chart or on its representation in the legend. Clicking with the Control key pressed for multiple selections is supported.

Mini

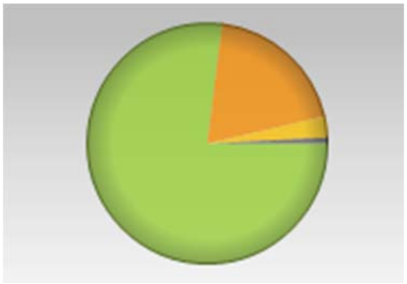
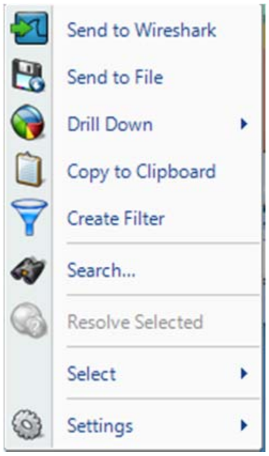


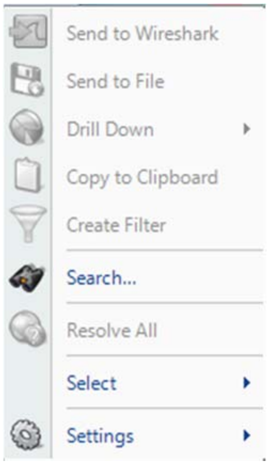
Chart Figure 52 Pie Chart Mini

The miniature view is shown when there is not enough space to display the standard view. In a mini-view none of the elements can be selected and there is no contextual menu.

Context Menu



Context Menu 33 Pie Chart (Selection)



Context Menu 34 Pie Chart (No Selection)

Context Sub Menu 16 Pie Chart Select

The context menu for the Pie Chart is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected slice(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected slice(s) to a user-specified trace file that will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected slice(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies a tabular form of the data to the system clipboard.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the Pie Chart and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Resolve Selected/Resolve All

The *Resolve Selected/Resolve All* menu option resolves, when applicable, the Port Name, IP Address, or MAC Address of the slice(s) in the Pie Chart.

Select

The *Select* menu option has two submenu options described at the beginning of this section with an option to either select the slice(s) in the Pie Chart, or invert the selection of slice(s).

Settings

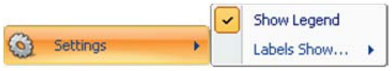
The *Settings* menu option opens up a sub-menu with specific settings for the chart. It is described below.

Context Sub-Menus

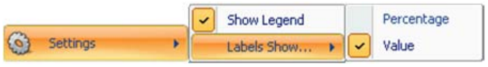
The Pie Chart has one contextual submenu:

- Settings

Settings



Context Sub Menu 17 Pie Chart Settings



Context Sub Menu 18 Pie Chart Settings (Detail)

The settings submenu for the Pie Chart context menu has two items:

Show Legend

The *Show Legend* check box menu option toggles off or on the Pie Chart legend.

Labels Show…

The *Labels Show…* menu option has a submenu with two mutually exclusive toggles:

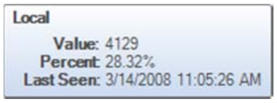
Percentage

The *Percentage* toggle labels the slice value(s) as a percentage of the whole pie.

Value

The *Value* toggle labels the slice value(s) with their quantitative equivalents.

Tooltips



Local

Value: 4129
Percent: 28.32%
Last Seen: 3/14/2008 11:05:26 AM

Tooltip 5 Pie Chart

A tooltip comes up when hovering over a slice. It has the following values:

Value

The *Value* refers to the quantitative value associated with that slice.

Percent

The *Percent* refers to the percentage that the slice constitutes of the whole.

Last Seen

The *Last Seen* refers to the last time that element of the slice was seen in traffic. This can give an idea as to what percentage in the time domain the slice refers to.

Data Grid

The *Data Grid* chart shows quantitative information pertaining to a number of metrics in a hierarchically arranged grid. The grid has rows and columns.

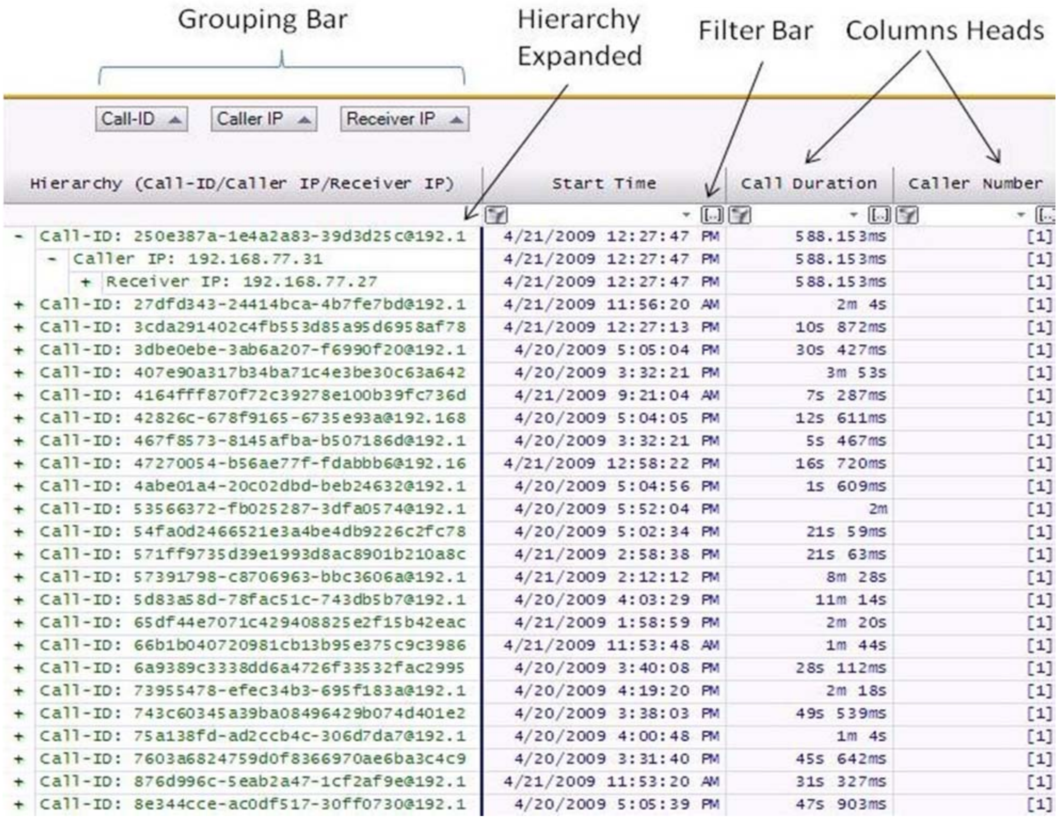
The columns can be:

- Rearranged in any order
- Resized
- Hidden and shown

The rows can be:

- Hierarchically arranged
- Collapsed and expanded
- Filtered and hidden by a variety of different means
- Sorted by any column or multiple columns simultaneously

For illustration, the figure below shows an example grid with a number of features enabled and some conventions modified for clarity.



Hierarchy (Call-ID/Caller IP/Receiver IP)	Start Time	Call Duration	Caller Number
- Call-ID: 250e387a-1e4a2a83-39d3d25c@192.1	4/21/2009 12:27:47 PM	588.153ms	[1]
- Caller IP: 192.168.77.31	4/21/2009 12:27:47 PM	588.153ms	[1]
+ Receiver IP: 192.168.77.27	4/21/2009 12:27:47 PM	588.153ms	[1]
+ Call-ID: 27dfd343-24414bca-4b7fe7bd@192.1	4/21/2009 11:56:20 AM	2m 4s	[1]
+ Call-ID: 3cda291402c4fb553d85a95d6958af78	4/21/2009 12:27:13 PM	10s 872ms	[1]
+ Call-ID: 3dbe0ebe-3ab6a207-f6990f20@192.1	4/20/2009 5:05:04 PM	30s 427ms	[1]
+ Call-ID: 407e90a317b34ba71c4e3be30c63a642	4/20/2009 3:32:21 PM	3m 53s	[1]
+ Call-ID: 4164fff870f72c39278e100b39fc736d	4/21/2009 9:21:04 AM	7s 287ms	[1]
+ Call-ID: 42826c-678f9165-6735e93a@192.168	4/20/2009 5:04:05 PM	12s 611ms	[1]
+ Call-ID: 467f8573-8145afba-b507186d@192.1	4/20/2009 3:32:21 PM	5s 467ms	[1]
+ Call-ID: 47270054-b56ae77f-fdabbb6@192.16	4/21/2009 12:58:22 PM	16s 720ms	[1]
+ Call-ID: 4abe01a4-20c02dbd-beb24632@192.1	4/20/2009 5:04:56 PM	1s 609ms	[1]
+ Call-ID: 53566372-fb025287-3dfa0574@192.1	4/20/2009 5:52:04 PM	2m	[1]
+ Call-ID: 54fa0d2466521e3a4be4db9226c2fc78	4/20/2009 5:02:34 PM	21s 59ms	[1]
+ Call-ID: 571ff9735d39e1993d8ac8901b210a8c	4/21/2009 2:58:38 PM	21s 63ms	[1]
+ Call-ID: 57391798-c8706963-bbc3606a@192.1	4/21/2009 2:12:12 PM	8m 28s	[1]
+ Call-ID: 5d83a58d-78fac51c-743db5b7@192.1	4/20/2009 4:03:29 PM	11m 14s	[1]
+ Call-ID: 65df44e7071c429408825e2f15b42eac	4/21/2009 1:58:59 PM	2m 20s	[1]
+ Call-ID: 66b1b040720981cb13b95e375c9c3986	4/21/2009 11:53:48 AM	1m 44s	[1]
+ Call-ID: 6a9389c3338dd6a4726f33532fac2995	4/20/2009 3:40:08 PM	28s 112ms	[1]
+ Call-ID: 73955478-efec34b3-695f183a@192.1	4/20/2009 4:19:20 PM	2m 18s	[1]
+ Call-ID: 743c60345a39ba08496429b074d401e2	4/20/2009 3:38:03 PM	49s 539ms	[1]
+ Call-ID: 75a138fd-ad2ccb4c-306d7da7@192.1	4/20/2009 4:00:48 PM	1m 4s	[1]
+ Call-ID: 7603a6824759d0f8366970ae6ba3c4c9	4/20/2009 3:31:40 PM	45s 642ms	[1]
+ Call-ID: 876d996c-5eab2a47-1cf2af9e@192.1	4/21/2009 11:53:20 AM	31s 327ms	[1]
+ Call-ID: 8e344cce-ac0df517-30ff0730@192.1	4/20/2009 5:05:39 PM	47s 903ms	[1]

Chart Figure 53 Grid

Grouping Bar

The elements of the *Grouping Bar*, called groups, determine the row hierarchy. In the above example, the root level contains the VOIP call ID. Each call can be expanded to show the caller IP, which can in turn be expanded to show the receiver IP.

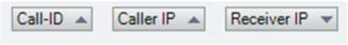


Figure 148 Grid Grouping Bar

Each element of the Grouping Bar also has an arrow after the name that specifies the sorting order of that level of the hierarchy. The order can be toggled by clicking on the group itself.

Additionally, groups can be rearranged by dragging the elements in a different order, and elements can be removed from the hierarchy by dragging them out of the sequence.

Column Headers

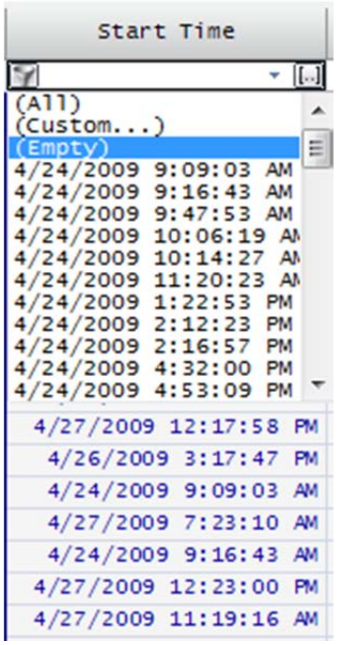
The *Column Headers* refers to columns which can be turned on and off thru the context menu. Rows can be sorted via one or more columns. The first, left-most column header contains the hierarchy specified in the Grouping Bar.

Filter Bar

The Data Grid *Filter Bar* enables filtering the data rows by column. Two types of filtering are supported:

- Selection Based
- Advanced

Selection Based

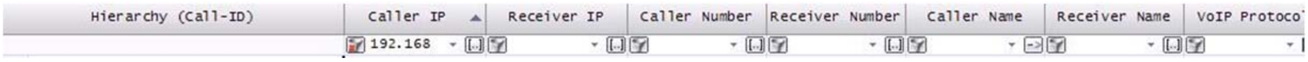


4/27/2009 12:17:58 PM
4/26/2009 3:17:47 PM
4/24/2009 9:09:03 AM
4/27/2009 7:23:10 AM
4/24/2009 9:16:43 AM
4/27/2009 12:23:00 PM
4/27/2009 11:19:16 AM

Figure 149 Selection Based Grid Filtering Drop Down

Selection Based filtering is activated by clicking the down arrow to the right of a column’s filters. A drop down list opens that lists the unique entries of the associated column. After an entry is selected, the rows not satisfying the selected filter are hidden.

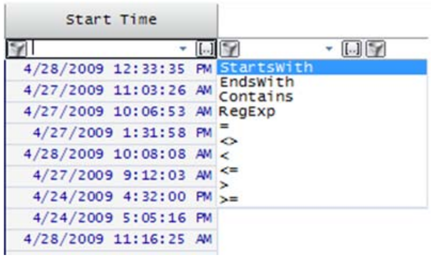
Additionally the icon on the left hand side of the filter box changes, as can be seen in Figure 150. Clicking on the icon removes the filter and shows the hidden rows.



Caller IP: 192.168

Figure 150 Selection Based Grid Filtering Enabled

Advanced



4/28/2009 12:33:35 PM
4/27/2009 11:03:26 AM
4/27/2009 10:06:53 AM
4/27/2009 1:31:58 PM
4/28/2009 10:08:08 AM
4/27/2009 9:12:03 AM
4/24/2009 4:32:00 PM
4/24/2009 5:05:16 PM
4/28/2009 11:16:25 AM

Figure 151 Advanced Grid Filtering

Advanced filtering is available by clicking on the ellipses (…) on the right of one of the column’s filters, which opens a drop down menu that lists a number of string and value manipulations and comparisons.

After an expression is entered, the rows that do not satisfy the expression are hidden.

As with the selection based filtering, the icon on the left hand side of the filter box changes, as can be seen in Figure 150. Clicking on the icon removes the filter and shows the hidden rows.

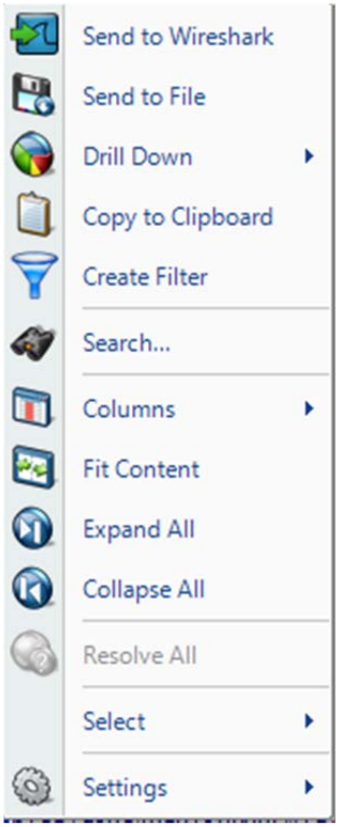
Hierarchy

The data grid rows can be organized in a multi-tiered tree via the grouping bar. They can be fully expanded and collapsed through the context menu.

Selection

Multiple-selection in the Data Grid can only be done at the same hierarchical level. For instance, a child and a parent cannot be simultaneously selected. However, a child and its siblings can.

Context Menu



Context Menu 35 Grid (Selection)

The context menu for the Data Grid is as follows:

Send to Wireshark

The *Send to Wireshark* menu option sends the traffic from the selected row(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected row(s) to a user-specified trace file that will appear, after completion, in the Files panel for immediate analysis.

Drill Down

The *Drill Down* menu option applies the user-specified view to the selected row(s) and opens a new view tab in the main workspace.

Copy to Clipboard

The *Copy to Clipboard* menu option copies a tabular form of the selected data to the system clipboard.

Create Filter

The *Create Filter* menu option creates a filter based on the current selection within the Grid and adds the filter to the Filter List.

Search

The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Columns

The *Columns* menu option expands to a submenu that is used to show and hide columns in the grid. The submenu is described below.

Fit Content

The *Fit Content* menu option resizes the columns making all of the column data visible.

Expand All

The *Expand All* menu option expands the ordered hierarchy of the rows.

Collapse All

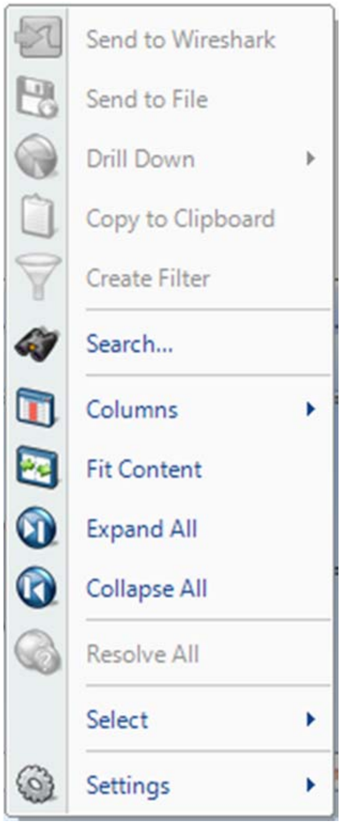
The *Collapse All* menu option collapses the ordered hierarchy of the rows.

Resolve All

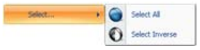
The *Resolve All* menu option is always disabled for the grid and is included in the context menu in order to be consistent with the other charts.

Select

The *Select* menu option provides the option to select all row(s) at a



Context Menu 36 Grid (No Selection)



Context Sub Menu 19 Select

certain level in the hierarchy. Inverting the selection of row(s) is currently disabled for Data Grid.

Settings

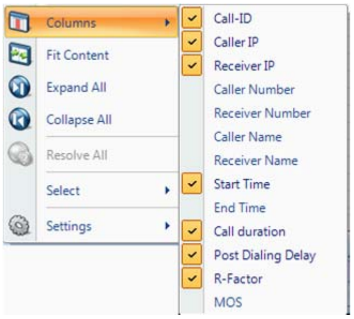
The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

Context Sub-Menus

The Data Grid has two contextual submenus:

- Columns
- Settings

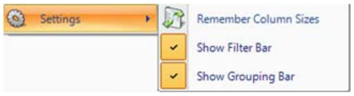
Columns



Context Sub Menu 20 Grid Columns

The *Columns* submenu of the Data Grid context menu shows a variable number of check boxes, depending on the specific data in the grid. Toggling the various options will either show or hide the corresponding columns.

Settings



Context Sub Menu 21 Grid Settings

The *Settings* submenu of the Data Grid context menu has the following options:

Remember Column Sizes

The *Remember Column Sizes* menu option saves the current size of the columns for a custom view. This is the only way to save the size of the columns as they are not automatically saved when a custom view is created or modified.

Show Filter Bar

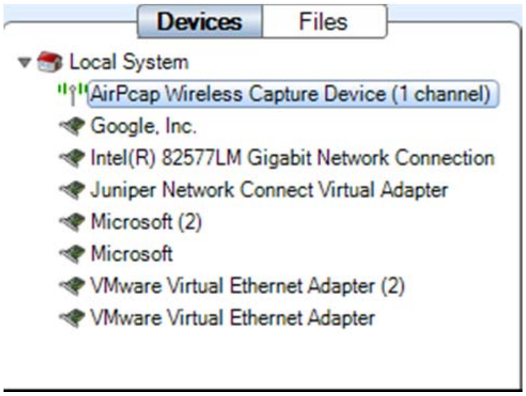
The *Show Filter Bar* menu option shows or hides the filter bar on the Data Grid Chart.

Show Grouping Bar

The *Show Grouping Bar* menu option shows or hides the Grouping Bar on the Data Grid Chart.

Channels Button

A Cascade Pilot provides 802.11 wireless analysis on live traffic using the Riverbed Technology AirPcap adapters for wireless interfaces.



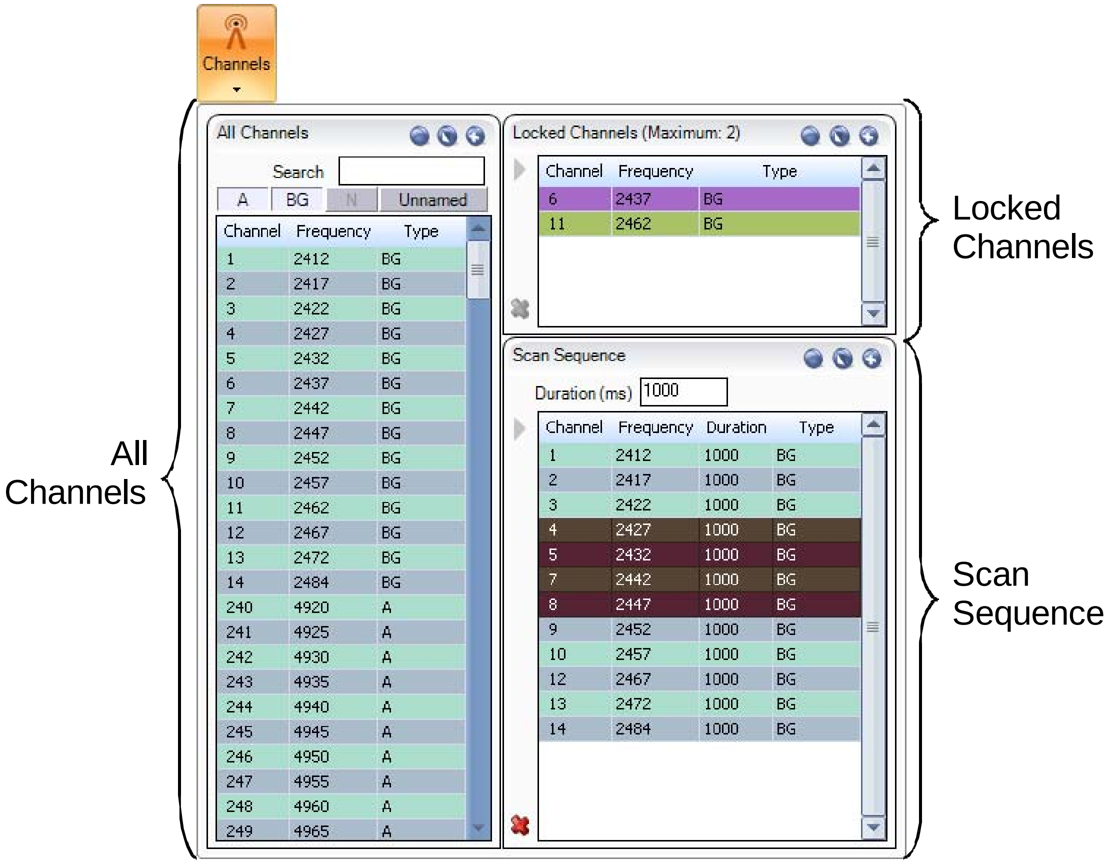
- Local System
  - AirPcap Wireless Capture Device (1 channel)
  - Google, Inc.
  - Intel(R) 82577LM Gigabit Network Connection
  - Juniper Network Connect Virtual Adapter
  - Microsoft (2)
  - Microsoft
  - VMware Virtual Ethernet Adapter (2)
  - VMware Virtual Ethernet Adapter

Figure 152 Wireless Interface in Sources Panel

Regardless of the number of AirPcap devices connected to the system, they are shown as a single aggregated capture device, where the number of channels, in parentheses, corresponds to the actual number of AirPcap capture devices (see Figure 152). The AirPcap adapters are aggregated into a single capture device for convenience in dealing with hopping or scan sequences, where the adapters are sequenced through multiple channels using the Channel Management Panel.

Note: ***Although it is possible to use different types of AirPcap adapters at the same time, in some cases there may be conflicts in the capabilities available on different adapters.***

The Channels button in the Home Ribbon brings up the Channel Management Panel. The Channel Management Panel selects which channels to capture for a particular time interval. The Channel Management Panel is available in the Home Ribbon and is shown below.



All Channels

Search

Channel	Frequency	Type
1	2412	BG
2	2417	BG
3	2422	BG
4	2427	BG
5	2432	BG
6	2437	BG
7	2442	BG
8	2447	BG
9	2452	BG
10	2457	BG
11	2462	BG
12	2467	BG
13	2472	BG
14	2484	BG
240	4920	A
241	4925	A
242	4930	A
243	4935	A
244	4940	A
245	4945	A
246	4950	A
247	4955	A
248	4960	A
249	4965	A

Locked Channels (Maximum: 2)

Channel	Frequency	Type
6	2437	BG
11	2462	BG

Scan Sequence

Duration (ms) 1000

Channel	Frequency	Duration	Type
1	2412	1000	BG
2	2417	1000	BG
3	2422	1000	BG
4	2427	1000	BG
5	2432	1000	BG
7	2442	1000	BG
8	2447	1000	BG
9	2452	1000	BG
10	2457	1000	BG
12	2467	1000	BG
13	2472	1000	BG
14	2484	1000	BG

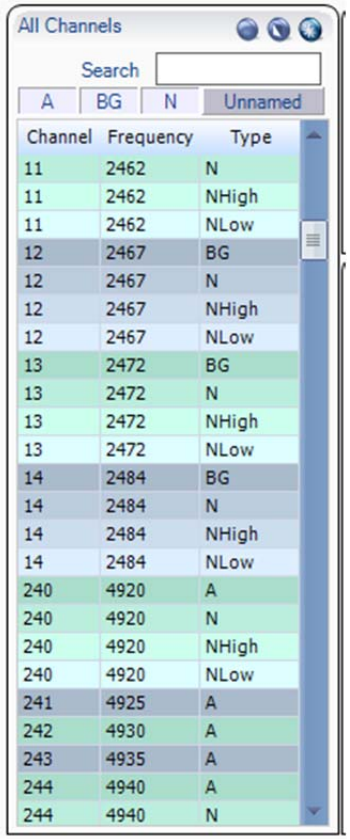
Figure 153 Channel Management Panel

Note: ***To close the Channel Management Panel, click the Channels button again or click somewhere outside of the submenu. All changes take place immediately hence there is no need for confirmation buttons.***

There are three main sections of the Channel Management Panel as shown in the above image:

- All Channels
- Locked Channels
- Scan Sequence

All Channels



Channel	Frequency	Type
11	2462	N
11	2462	NHigh
11	2462	NLow
12	2467	BG
12	2467	N
12	2467	NHigh
12	2467	NLow
13	2472	BG
13	2472	N
13	2472	NHigh
13	2472	NLow
14	2484	BG
14	2484	N
14	2484	NHigh
14	2484	NLow
240	4920	A
240	4920	N
240	4920	NHigh
240	4920	NLow
241	4925	A
242	4930	A
243	4935	A
244	4940	A
244	4940	N

Figure 154 All Channels

For the purpose of this document, a *channel* corresponds to a center frequency, bandwidth, and type of 802.11 frames that can be received. The types of frames are:

BG – 802.11b or 802.11g

A – 802.11a

N – 802.11n without an extension channel

NHigh – 802.11n with an extension channel above the center frequency

Nlow – 802.11n with an extension channel below the center frequency

The available channels depend on the specific AirPcap devices attached to the system.

2.4GHz Center Frequencies:

AirPcap Classic/Tx – 20 MHz bandwidth, 802.11b,g (BG)

AirPcap Ex – 20 MHz bandwidth, and 802.11b,g (BG)

AirPcap Nx – 20 MHz bandwidth, and 802.11b,g,n (BG or N)

AirPcap Nx – 40 MHz bandwidth, and 802.11b,g,n (BG or N or NHigh or Nlow)

5GHz Center Frequencies:

AirPcap Ex – 20 MHz bandwidth, and 802.11a (A)

AirPcap Nx – 20 MHz bandwidth, and 802.11a,n (A or N)

AirPcap Nx – 40 MHz bandwidth, and 802.11a,n (A or N or NHigh or NLow)

For example, the AirPcap Ex adapter at 2.437 GHz center frequency will capture BG frames. At 5.260 GHz, the AirPcap Ex adapter will capture A frames.

The AirPcap Nx adapter at 2.437 GHz center frequency and 20 MHz bandwidth will capture BG, A, and N frames. At 5.260 GHz center frequency and 40 MHz bandwidth (NHigh), the AirPcap Nx adapter will capture A, N, and NHigh frames.

Channel Names

Channels are generally identified with a by a number and a frequency band. For example, channel 13 in the 2.4 GHz band corresponds to center frequency 2.472 GHz. Not every available channel will have an assigned number. This is indicated by N/A for the channel name.

All Channels Panel

The *All Channels* panel includes the following:

- A list of all of the available channels. This list depends on the available AirPcap adapters. The list columns include the channel name, the center frequency, and the type of frame that can be received.
- A search bar that automatically matches any field in the channel list.
- Four filter buttons to quickly hide or show the A, BG, N, and Unnamed channels.
- Alternating color rows so that different ways to interpret a channel at the same frequency are visually broken up.
- Selection control buttons.

This view enables a traditional flat list of channels that can be quickly navigated and selected without concern for the complexities of the standards.

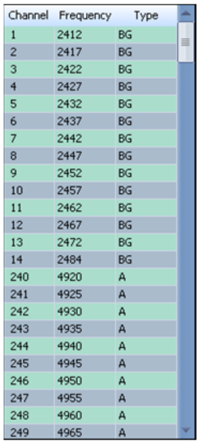
However, there are some very important restrictions that must be taken into consideration when using multiple classes of AirPcap adapters at once:

N and BG channels are mutually exclusive. If there is one N adapter and one BG adapter, then only the N adapter can scan the 2.4 GHz BGN range.

For the purpose of documentation, the control has been broken into the following components:

- Channel List
- Search and Filter Bar
- Selection Controls

Channel List



Channel	Frequency	Type
1	2412	BG
2	2417	BG
3	2422	BG
4	2427	BG
5	2432	BG
6	2437	BG
7	2442	BG
8	2447	BG
9	2452	BG
10	2457	BG
11	2462	BG
12	2467	BG
13	2472	BG
14	2484	BG
240	4920	A
241	4925	A
242	4930	A
243	4935	A
244	4940	A
245	4945	A
246	4950	A
247	4955	A
248	4960	A
249	4965	A

Figure 155
Channel List

The Channel List is a scrollable list of all channels supported by all connected AirPcap Adapters. This list automatically changes when the number of adapters changes (which is updated by clicking the *Update Sources* button, described in the Home Panel section).

The colors in the list are to provide contrast for easy navigation. The only rule they follow is that they are alternated based on frequency.

The Channel List has three columns:

Channel

The canonical name for a channel. This is how the channel is usually referred to, such as Channel 6. Not all available frequencies have a canonical name.

Frequency

The actual center frequency of the row in MHz.

Type

The type of Channel; one of the following: BG, A, N, NHigh, NLow.

Selection Controls

Icon 58 Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.

Icon 59 Invert Selection

The *Select Inverse* button inverts the channel list selection(s).

Icon 60 Select All Channels

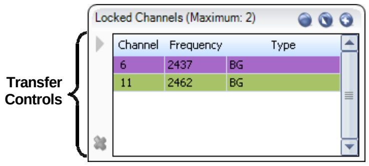
The *Select All* button selects all of the channel(s) in the channel list.

Search and Filter Bar

The search text box can be edited at any given time and gives the results in real time.

The filter bar contains four buttons, each corresponding to a set of channel types. Since there may be times when not all classes of AirPcap Adapters are plugged in, some of the filter buttons will be disabled. For instance, in the example, since there is no 802.11n wireless adapter plugged in, the N button is grayed out.

Locked Channels



Locked Channels (Maximum: 2)

Channel	Frequency	Type
6	2437	BG
11	2462	BG

Figure 156 Locked Channels

The *Locked Channels* is a list of channels that are used to assign a wireless adapter dedicated to a channel. It contains four elements:

- Title
- Selection controls
- Transfer controls
- Channel list

The following is saved in the global configuration file:

- Locked channels

Title

The *Title* specifies how many channels can be locked. This number is equal to the number of AirPcap adapters recognized by Cascade Pilot. If you plug more AirPcap Adapters in, or take some out, then you must click the *Update Sources* button in the Home Ribbon in order for your changes to be reflected in the maximum channel tally.

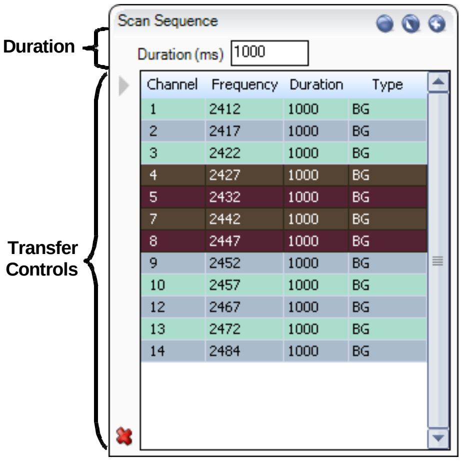
Selection Controls

 Icon 61 Select No Channels	The *Select None* button deselects all channel(s) in the channel list, if applicable.
 Icon 62 Invert Selection	The *Select Inverse* button inverts the channel list selection(s).
 Icon 63 Select All Channels	The *Select All* button selects all channel(s) in the channel list.

Transfer Controls

 Icon 64 Transfer Channels	The *Right Arrow* button adds the selected channel(s) to the lock list.
 Icon 65 Remove Channels	The *Remove* button removes the selected channel(s) from the lock list. The lock list can legally have zero elements.

Scan Sequence



Duration (ms) 1000

Channel	Frequency	Duration	Type
1	2412	1000	BG
2	2417	1000	BG
3	2422	1000	BG
4	2427	1000	BG
5	2432	1000	BG
7	2442	1000	BG
8	2447	1000	BG
9	2452	1000	BG
10	2457	1000	BG
12	2467	1000	BG
13	2472	1000	BG
14	2484	1000	BG

Figure 157 Scan Sequence

The *Scan Sequence* is a list of channels that the wireless adapter(s) will listen on occasionally. It contains four elements:

- Duration
- Selection controls
- Transfer controls
- Channel list

The following is saved in the global configuration file:

- Scan sequence elements
- Duration for each element

Note: ***The scan sequence is determined by the number of AirPcap adapters and their individual capabilities. For consistent results that are independent of the specific scan sequence, it is advisable to have only on type of AirPcap adapter in the system, e.g., either all AirPcap Ex adapters or all AirPcap Nx adapters. Having both AirPcap Ex and AirPcap Classic/Tx adapters works well in the 2.4 GHz band, but not in the 5 GHz band.***

Duration

Duration (ms) 1000

Figure 158 Channel Duration

The *Duration* edit box sets how long each selected channel will be locked before moving on to the next available channel in the scan sequence.

Selection Controls

Icon 66 Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.

Icon 67 Invert Selection

The *Select Inverse* button inverts the channel list selection(s).

✱ **Icon 68 Select All Channels**	The *Select All* button selects all channel(s) in the channel list.

Transfer Controls

▶ **Icon 69 Transfer Channels**	The *Right Arrow* button adds the selected channel(s) to the scan sequence with a duration of 1000 ms each. Durations of previous, deleted channel(s) are not saved if they are retransferred.
✖ **Icon 70 Remove Channels**	The *Remove* button removes the selected channel(s) from the scan list. The scan list can legally have 0 elements.

Scan Sequence

The *Scan Sequence* is a frequently updated color-coded list of scanned channels. The scan sequence is updated a few times per second to reflect which channels are currently being scanned. Additionally, the channel list in the Scan Sequence has one extra column, named “Duration,” which refers to how long that entry will be scanned before moving on to the next. Each entry can have a different duration value.

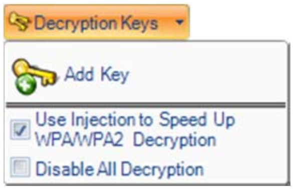
Decryption

Cascade Pilot supports three different types of Wireless decryption:

- WEP (“Wireless Encryption Protocol” or more properly, Wired Equivalent Privacy)
- WPA 1 (Wi-Fi Protected Access with CCMP as specified in IEEE 802.11i)
- WPA 2 (Wi-Fi Protected Access with TKIP as specified in IEEE 802.11i)

Decryption is done through the Wireless Decryption Keys Manager. The decryption keys are global and saved in the configuration file. Note that an exported configuration file will contain the decryption keys so care should be taken.

Wireless Decryption Keys Manager



☑ Use Injection to Speed Up WPA/WPA2 Decryption

□ Disable All Decryption

Submenu 9 Decryption Keys

The *Wireless Decryption Keys Manager* is available in the Home Ribbon.

When clicked, a submenu appears with the following options:

Add Key

The *Add Key* button, described below, is used to add a new decryption key to be used for future analysis.

Use Injection to Speed Up WPA/WPA2 Decryption

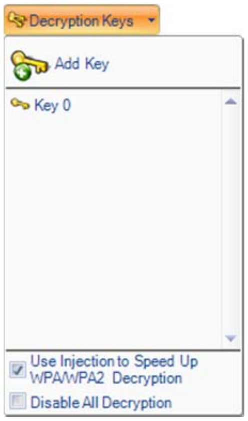
The *Use Injection to Speed Up WPA/WPA2 Decryption* check box, described below in the section entitled “WPA related packet injection” is only enabled if all plugged in AirPcap adapters are Ex. Please note that there are a number of important considerations when using this feature, as discussed below.

Disable All Decryption

The *Disable All Decryption* check box is used to completely turn off decryption. This may decrease the time required to process a packet if trying to mitigate packet loss on an extremely busy network. It can also be used to confirm that a network is encrypted.

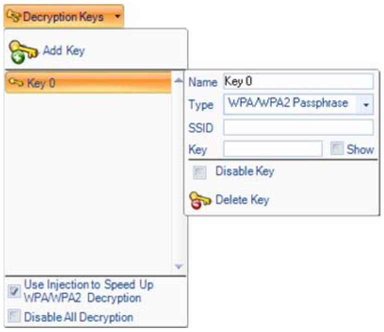
Note: ***To close the Wireless Decryption Keys Manager, click the button again or click somewhere outside of the submenu. All changes take place immediately hence there is no need for confirmation buttons.***

Adding a Key



☑ Use Injection to Speed Up WPA/WPA2 Decryption
□ Disable All Decryption

Submenu 10 Decryption Keys with Key



Name: Key 0
Type: WPA/WPA2 Passphrase
SSID:
Key: □ Show
□ Disable Key

☑ Use Injection to Speed Up WPA/WPA2 Decryption
□ Disable All Decryption

Submenu 11 Decryption Keys with Key (Detail)

To add a key, click on the *Add Key* button. The submenu will change to show a scrollable list with one decryption key, and as many decryption keys can be added as desired. Note that there is no need to associate a particular decryption key with a trace file or wireless adapter, as the appropriate decryption key will be automatically matched with its specific context.

After a decryption key has been added, its parameters need to be set by clicking on the key. A submenu opens to the right of the key title with seven controls:

Name

The *Name* field refers to the canonical name of the decryption key. This is used for management of decryption keys, as it is what will appear as the name in the key gallery, but does not affect decryption. These names need not be unique.

Type

The *Type* combo box is used to specify the type of decryption key to be added. This is a crucial option as different types will map to entirely different decryption algorithms.

SSID

The *SSID* field is required for WPA related decryption keys, but is disabled for WEP decryption keys because the SSID is not needed to decrypt WEP traffic.

Key

The *Key* field is used to specify the shared decryption key needed for a wireless network to be decrypted. Hexadecimal values can be placed here as a single string when appropriate and are not case sensitive. Additionally, 104-bit and 40-bit WEP decryption keys are detected automatically from the Key field input length. For instance, if the type is set to WEP and “A05B06c07d” was put into the Key field, it will be detected as a 40-bit WEP key.

Show

The *Show* check box shows or hides the text in the Key field. By default the Key field uses substitution characters for obfuscation. However, this can be disabled and the field can be seen in plain text by toggling on the Show check box.

Disable Key

The *Disable Key* check box disallows a decryption key from being considered when decrypting traffic. This can be useful for two reasons:

- To confirm that traffic is encrypted.
- To speed up decryption. By disabling a decryption key, fewer decryption keys will be considered as candidates for decryption and so therefore, decryption will speed up.

Delete Key

The *Delete Key* button immediately and irreversibly removes a decryption key from the Key list.

WPA Related Packet Injection

Wireless networks secured using the WPA protocol cannot be decrypted as easily as their WEP counterparts. This is because unlike with WEP, simply having a decryption key is not enough to view the traffic of other stations on a network. The access point establishes a different, temporary, ostensibly unique trusted link with each station on the network.

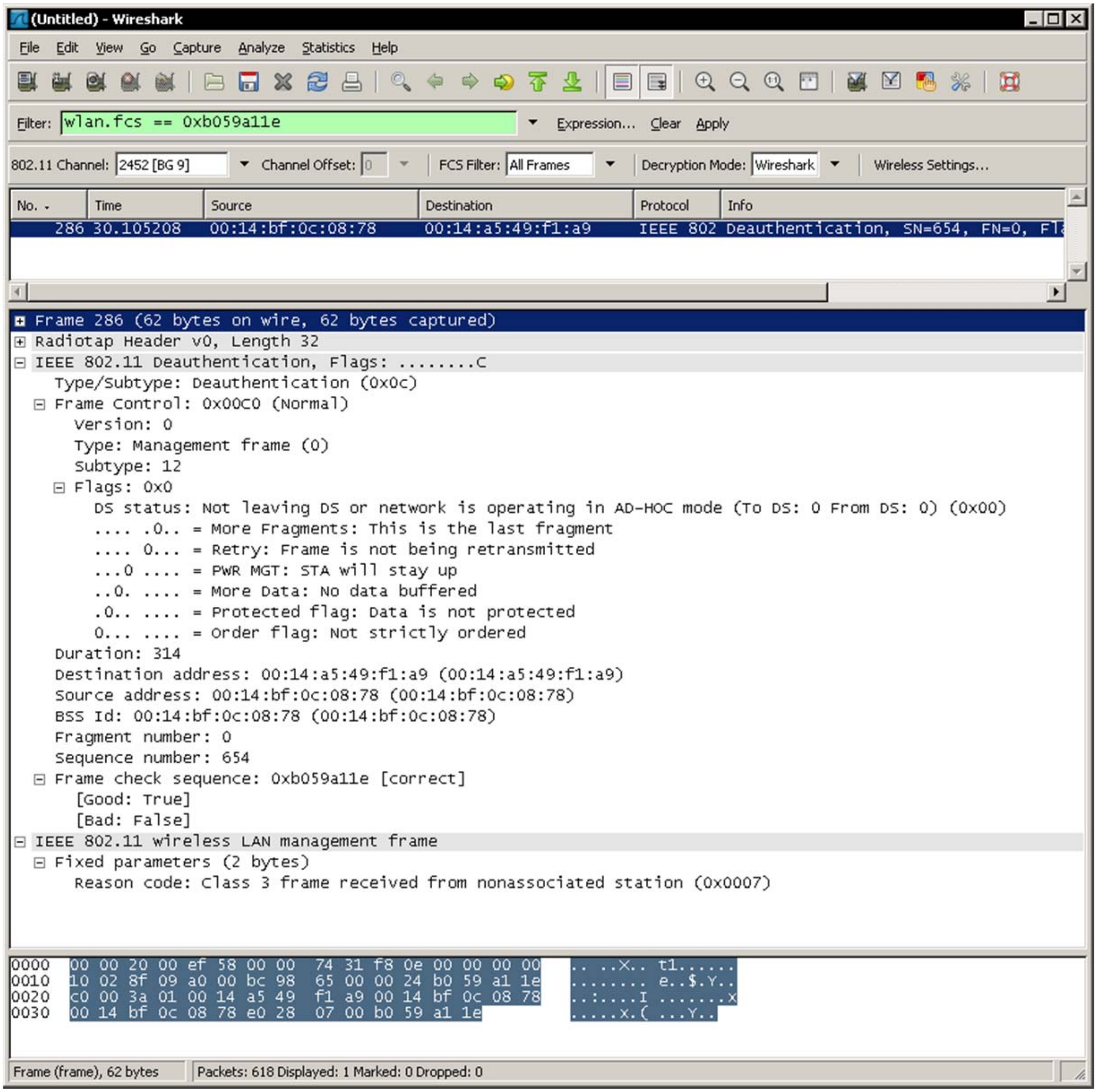
In order to successfully decrypt WPA traffic then, even with a valid decryption key, the setup of this link needs to be captured. However, because stations may not authenticate for hours or possibly longer, in order to view traffic without waiting a long time, the hosts need to re-associate with their access point.

This can be achieved by sending out a de-authentication request which asks the stations to re-associate with their access point.

Note: ***WPA packet injection only works if all the plugged in AirPcap adapters are EX class. If not all of the plugged in adapters are AirPcap EX, then the checkbox will be disabled.***

Note: ***Although it ultimately depends on the wireless adapter of the station, it is very probable that this action will temporarily drop the connection between a station and its access point.***

In Wireshark, the deauthentication frame will look similar to the figure below:


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply
Wireless Settings...

Filter: wlan.fcs == 0xb059a11e

802.11 Channel: 2452 [BG 9] Channel Offset: 0 FCS Filter: All Frames Decryption Mode: Wireshark

No.	Time	Source	Destination	Protocol	Info
286	30.105208	00:14:bf:0c:08:78	00:14:a5:49:f1:a9	IEEE 802	Deauthentication, SN=654, FN=0, Fl

```
⊞ Frame 286 (62 bytes on wire, 62 bytes captured)
⊞ Radiotap Header v0, Length 32
⊟ IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x0c)
  ⊟ Frame Control: 0x00C0 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 12
    ⊟ Flags: 0x0
        DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 314
    Destination address: 00:14:a5:49:f1:a9 (00:14:a5:49:f1:a9)
    Source address: 00:14:bf:0c:08:78 (00:14:bf:0c:08:78)
    BSS Id: 00:14:bf:0c:08:78 (00:14:bf:0c:08:78)
    Fragment number: 0
    Sequence number: 654
  ⊟ Frame check sequence: 0xb059a11e [correct]
      [Good: True]
      [Bad: False]
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (2 bytes)
      Reason code: Class 3 frame received from nonassociated station (0x0007)
```

```
0000  00 00 20 00 ef 58 00 00  74 31 f8 0e 00 00 00 00   .. ..X.. t1......
0010  10 02 8f 09 a0 00 bc 98  65 00 00 24 b0 59 a1 1e   ........ e..$.Y..
0020  c0 00 3a 01 00 14 a5 49  f1 a9 00 14 bf 0c 08 78   ..:....I .......x
0030  00 14 bf 0c 08 78 e0 28  07 00 b0 59 a1 1e         .....x.( ...Y..
```

Frame (frame), 62 bytes | Packets: 618 Displayed: 1 Marked: 0 Dropped: 0

Figure 159 Wireshark analyzing a Cascade Pilot generated Deauthentication frame

Drill Down

The *Drill Down* feature is one of the most powerful features of Cascade Pilot. Drill Down enables data to be analyzed at various levels of detail by iteratively applying views to visually selected subsets of the data.

More specifically, any information, computation, or meta information in the system can be the basis for a drill down, such as bytes over time or all traffic on TCP port 80. Views can be applied both on devices or files, or on the resulting data itself. Thus a view that is generated from the data can in turn, have another view applied on itself and so on. To do so, every chart has a means of selecting data subsets to enable execution of the drill down operation.

How to

The Drill Down functionality of Cascade Pilot is accessible in three ways:

- The Home Ribbon contains Drill Down button available in the Selection Section.
- The Context menu has a Drill Down option available on any chart.
- Dragging a view from the Views Panel over the chart (with a current selection) to be drilled down.

Example

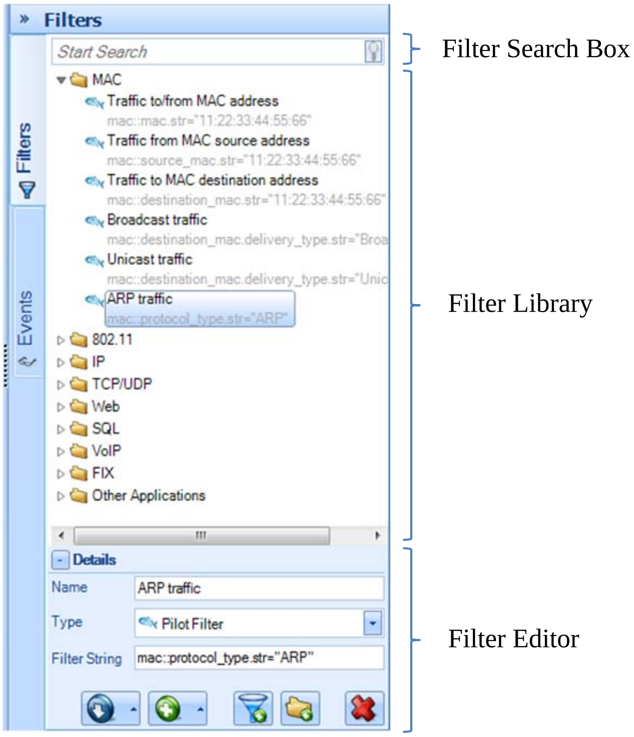
For examples of Drill Down sequences and operations, please refer to the tutorial videos.

Filtering

Cascade Pilot offers several ways to apply user-defined filters on large data sets to help focus the analysis the data of interest.

Filter panel

The Filter panel, located on the right side of the Pilot user interface in the tabbed navigation panel, displays and organizes the set of filters. The panel is composed of three elements.


Filters
Events
Start Search
MAC
Traffic to/from MAC address
mac::mac.str="11:22:33:44:55:66"
Traffic from MAC source address
mac::source_mac.str="11:22:33:44:55:66"
Traffic to MAC destination address
mac::destination_mac.str="11:22:33:44:55:66"
Broadcast traffic
mac::destination_mac.delivery_type.str="Broa
Unicast traffic
mac::destination_mac.delivery_type.str="Unic
ARP traffic
mac::protocol_type.str="ARP"
802.11
IP
TCP/UDP
Web
SQL
VoIP
FIX
Other Applications
Details

Name: ARP traffic

Type: Pilot Filter

Filter String: mac::protocol_type.str="ARP"

Filter Search Box

Filter Library

Filter Editor

Figure 160: Filter panel

Filter Search Box

The Filter Search Box is used to locate specific filters among the list. The search will match any filter that has the search string in either the filter name or the filter string.

Filter Library

The *Filter Library* displays the collection of pre-packaged and user customized filters. Filters can be selected, edited, moved, added and removed through the buttons on the bottom of the library, or through the context menu.

Filter Editor

The *Filter Editor* section has three elements:

Name

The name of the filter to be modified.

Type

The language the filter is to be written in. There are four languages available:

- Pilot Filter
- BPF[7]
- Wireshark Display Filter [8]
- Time Interval

Filter String

The code for the filter associated with the description as specified above.

Apply

The *Apply* button is used to apply selected filters to the current view. It provides the user with a list of options that can be used in applying the selected filter based on the operator. This set matches that of Wireshark's context menu for filters:

Selected	Selected filters are applied in place of applied filter of the same type.
Not Selected	
… and selected	Selected filters are applied to the currently applied filter of the same type and the new filter value depends on the chosen operator.
… and not selected	
… or selected	
… or not selected	

If more than one filter is selected, filters of the same type are aggregated using OR, while filters of different types are aggregated using AND.

Prepare

The *Prepare* button sets up the selected filters for editing in the Filter Bar (described below) without applying them. See the *Apply* button for options.

[7] BPF was published in USENIX 93 and can be seen here: http://www.tcpdump.org/papers/bpf-usenix93.pdf
[8] See http://www.wireshark.org/docs/dfref/

Edit

The *Edit* button moves focus to the Filter Editor at the bottom of the Filter panel to edit the selected filter. If no view is currently applied, the same behavior is performed by pressing the Enter key.

Delete

The *Delete* button removes the selected filters from the collection after prompting the user for confirmation. The same behavior is performed by pressing the Del key.

Duplicate

The *Duplicate* button creates a copy of the selected filter. The new copy has the same filter type and value as the original, but has a unique name, constructed by appending a counter to the original name.

Move to Top

The *Move to Top* button moves the selected filter to the top of the hierarchy level in which the filter is located, to give it more visibility.

New Filter/Folder

The *New Filter* button creates a new filter and adds it to the collection. If clicked from the context menu or in the Filter Editor when something is selected, the behavior is similar to *Duplicate* button (except for the name). Otherwise a new default BPF filter is created.

The *New Folder* button creates a new empty folder as subfolder of the selected one. If none is selected a new folder is added to the root level.

Sort

The *Sort* button sorts the collection elements based on one of the following options: Default (order defined in the Cascade Pilot configuration file), Name or Type.

Reset Filters

The *Reset Filters* button restores the factory-defined filter list. If the configuration file was imported from an older version of Pilot, there is an option to merge the filters defined by the new version into the factory list.

Drag & Drop

Filters can be easily dragged in and out of the panel to create, organize or apply filters.

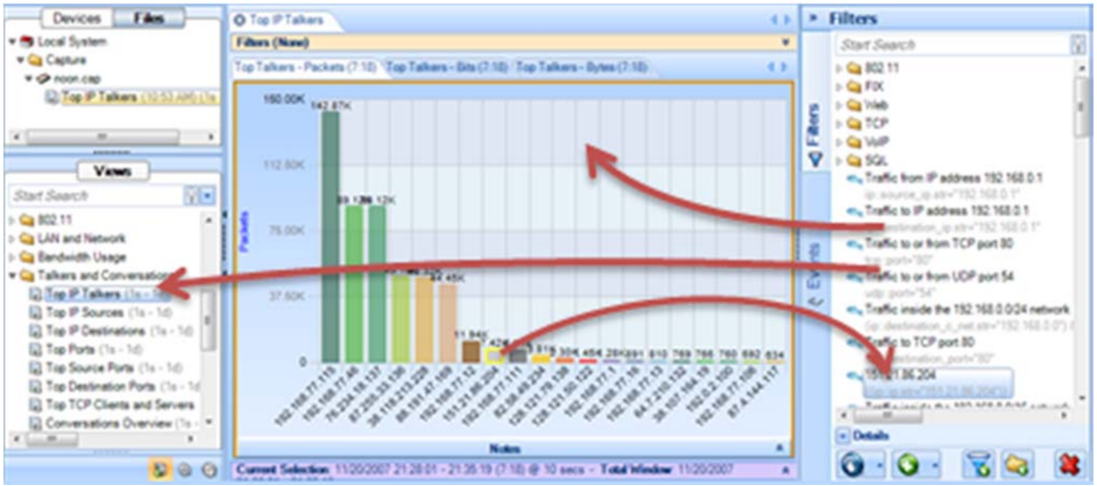

Devices
Files
Local System
Capture
noon.cap
Top IP Talkers
Views
Start Search
802.11
LAN and Network
Bandwidth Usage
Talkers and Conversations
Top IP Talkers (1s - 1d)
Top IP Sources (1s - 1d)
Top IP Destinations (1s - 1d)
Top Ports (1s - 1d)
Top Source Ports (1s - 1d)
Top Destination Ports (1s - 1d)
Top TCP Clients and Servers
Conversations Overview
Top IP Talkers
Filters (None)
Top Talkers - Packets (7:18)
Top Talkers - Bits (7:18)
Top Talkers - Bytes (7:18)
150.00K
112.50K
75.00K
37.50K
0
142.87K
Packets
Nodes
Current Selection: 11/20/2007 21:28:01 - 21:35:19 (7:18) @ 10 secs - Total Window: 11/20/2007
Filters
Start Search
802.11
FIX
Web
TCP
VoIP
SQL
Traffic from IP address 192.168.0.1
Traffic to IP address 192.168.0.1
Traffic to or from TCP port 80
Traffic to or from UDP port 54
Traffic inside the 192.168.0.0/24 network
Traffic to TCP port 80
Events
Details

Figure 161: Dragging and dropping filters

Inside Filter panel

- Within the Filter panel itself, filters can be dragged around to change their position inside their folder, or to move them from one folder to another. If the Control key is held during drag, a copy is performed instead of a move.
- Folders cannot be copied or moved. It is only possible to change their position by dragging them within the same hierarchy level.

From Filter panel

- Filters can be dragged over an unapplied standard view in the Views panel, creating a filtered view in the Custom Views folder. If a filter is dragged onto a custom view, that view is modified to add the filter.

- Filters can be dragged onto the Filter Bar or onto an applied view chart, which will apply the view to the open view. Multiple selection is supported:
    - Two or more filters of the *same type* will be applied as a single filter item in the Filter Bar in OR.
    - Two or more filters of *different type* will be set on as many filter items in the Filter Bar as the number of different filter types in the multiple selection. Filters of the same type are in OR, otherwise in AND
- When a filter is dragged onto the filter bar and a previous one of the same type is already set, the new one replaces the old one. A new filter can be applied using OR or AND with the previous one by holding, respectively, Control and Alt keys while dropping.
- A time filter can be dragged over the master controller to apply it. It can be dragged over a Strip Chart or Sequence Diagram to perform a time selection or over the Filter Bar to apply it to the view.

To Filter panel

- Any filter can be dragged from the Filter Bar onto the filter panel to create a new item in the list. Also, time filters can be created by dragging a time selection from the Strip Chart, Sequence Diagram or Master Controller onto the Filter panel.

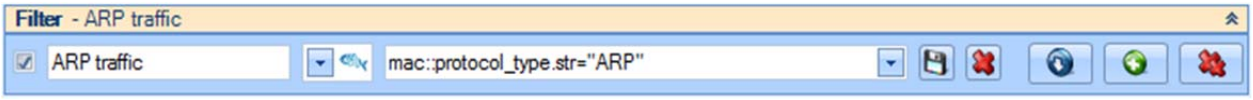
Shortcuts

Some of the operations can be performed by keyboard shortcuts:

- **Double-Click / Enter:**
    - **Folder list item:** expands the folder in the Filter panel to show its name and moves focus to it.
    - **Filter list item**
        - If no view is applied, expands the Filter panel editor showing the filter details and moves focus to the editor.
        - If a view is applied, adds the filter to the view and updates it instantly.
- **F2:** expands Filter Editor details and gives focus to it.
- **F3:** gives focus to search box.
- **Del:** removes selected item.
- Typing a filter name performs a search and first occurrence is selected.

Filter Bar

The Filter Bar is a visual component on the top of an open view that shows the currently applied filters and/or the filters being edited. It is the Pilot equivalent of Wireshark's "display filter input" and provides the user with a graphical interface to disable, edit, save, remove and apply filters. Whenever a filter is applied or modified, the view is updated to show the new filtered data.



Filter - ARP traffic

☑ ARP traffic

mac::protocol_type.str="ARP"

Figure 162: Filter bar

The bar displays the filter parameters and a check box on the left shows if a filter item is currently applied to the view. Checking or unchecking that item performs an instant view update.

Save

The *Save* button saves the filter, adding it to the root folder in the Filter panel.

Delete

The *Delete* button removes the applied filter and updates the view. If the filter isn't applied, all the fields are simply cleared.

Apply

The *Apply* button applies the filter changes and updates the view. This behavior can also be performed by pressing the Enter key.

Prepare

The *Prepare* button creates a new empty row and adds it to the filter bar so that a new filter can be edited and applied.

Delete All

The *Delete All* button removes all the filters from the Filter Bar and updates the view accordingly.

Note: ***It is NOT possible to have two or more filter rows with the same filter type because each filter item specifies one and only filter type. Different types are defined on different rows and are combined using AND.***

Drag & Drop behavior

Filters in the Filter panel can interact with the Filter Bar through Drag & Drop or by means of the context menu.

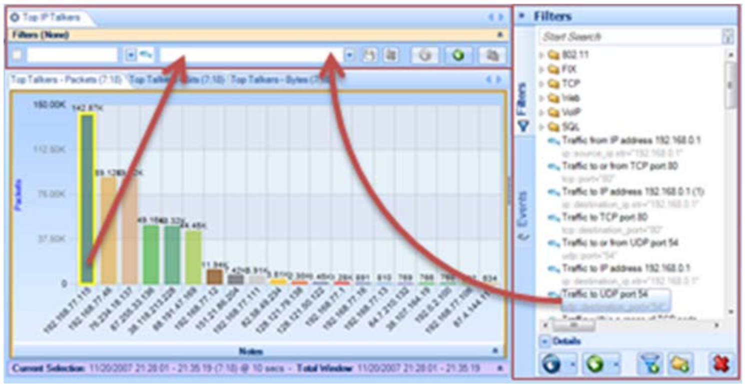

Top IP Talkers
Filters (None)
Top Talkers - Packets (7.18)
Top Talkers - Bytes
160.00K
112.50K
75.00K
37.50K
0
Packets
Notes
Current Selection: 11/20/2007 21:28:01 - 21:35:19 (7:18) @ 10 secs - Total Window: 11/20/2007 21:28:01 - 21:35:19
Filters
Start Search
802.11
FIX
TCP
Web
VoIP
SQL
Traffic from IP address 192.168.0.1
Traffic to or from TCP port 80
Traffic to IP address 192.168.0.1 (1)
Traffic to TCP port 80
Traffic to or from UDP port 54
Traffic to IP address 192.168.0.1
Traffic to UDP port 54
Filters
Events
Details

Figure 163: Filter panel - Filter bar interaction

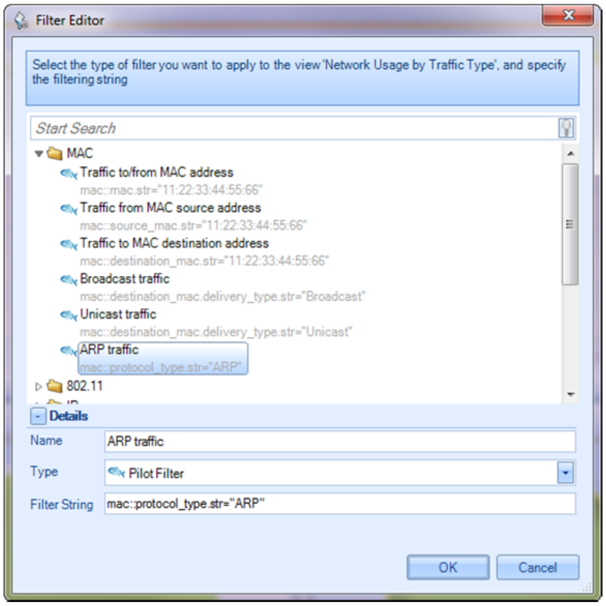
As mentioned above, any filter can be dragged over the Filter Bar to instantly apply it. See the previous section for a description of the various options for applying filters using drag & drop.

Shortcuts

Some operations can be performed using keyboard shortcuts:

- **Enter:** Apply the filter, if modified.
- **Control+Z:** Undo changes in the filter value combo box in order to show the history of the applied filters.
- **Control+Y:** Redo changes in the filter value combo box.

Filter Dialog



Select the type of filter you want to apply to the view 'Network Usage by Traffic Type', and specify the filtering string

- MAC
  - Traffic to/from MAC address
    mac::mac.str="11:22:33:44:55:66"
  - Traffic from MAC source address
    mac::source_mac.str="11:22:33:44:55:66"
  - Traffic to MAC destination address
    mac::destination_mac.str="11:22:33:44:55:66"
  - Broadcast traffic
    mac::destination_mac.delivery_type.str="Broadcast"
  - Unicast traffic
    mac::destination_mac.delivery_type.str="Unicast"
  - ARP traffic
    mac::protocol_type.str="ARP"
- 802.11

Details

Name: ARP traffic

Type: Pilot Filter

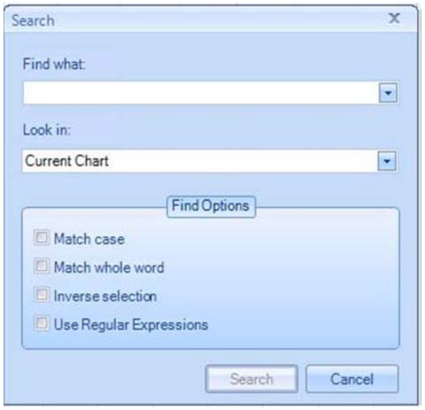
Filter String: mac::protocol_type.str="ARP"

Dialog 2 Filter Editor

The *Filter Dialog* appears every time an operation with a filter is requested; for example, after selecting any option to send traffic with a filter either to file or to Wireshark.

The Filter Dialog implements the same graphical interface shown in the Filter panel, but it is not possible to apply filters, drag them out of the control, delete or reset them.

Search Dialog



Look in: Current Chart

Dialog 3 Search Dialog

The *Search* dialog can be activated either by clicking on the binocular icon labeled Search in the Main Ribbon or by context clicking on a chart and choosing the "Search" option. There are two search features:

- Search Context
- Search Style

Search Context

Using the *Look in* drop down selection, searches can be executed over the following three scopes:

Current Chart

The *Current Chart* drop down menu option refers to the currently selected chart, identified with an orange border.

Current View

The *Current View* drop down menu option refers to the foremost tab and all associated charts.

All Open Views

The *All Open Views* drop down menu option refers to all open views with a tab in the main workspace

Search Style

Different types of searches can be executed based on what is selected in the Find Option subsection of the Search dialog. There are four checkboxes:

Match case

The *Match Case* check box toggles case sensitivity for alphabetic characters [A-Z].

Match whole word

By default, search looks for substrings. For example, if a hostname is "www.riverbed.com" and "river" is searched, then "www.riverbed.com" would still be matched. When *Match whole word* is checked, then only entering the full "www.riverbed.com" string will match.

Inverse Selection

The *Inverse Selection* check box toggles whether the results that match the search term should be selected, or their respective inverse.

Use Regular Expressions

Cascade Pilot supports POSIX regular expressions for advanced searching, which are well documented elsewhere. The basic syntax includes:

^ Match the beginning of a label.
“^i” would match “intel” but not “cisco”.

$ Match the end of a label.
“l$” would match “intel” but not “airlink”.

. Any single character.
“i.t” would match “intel” or “virtech” but not “cisco”.

? Zero or one of the previous character.

“i.?t” would match “intel” and “itech” but not the word “inert”.

***** Zero or more of the previous character.
“i.*e” would match “intel” and “virtech” but not “cisco”.

+ One or more of the previous character.
“i.*n” would match “intel” but “i.+n” would not.

| Multiplicity operator
“intel|cisco” will match either “intel” or “cisco” but not “virtech”. The parenthesis can be used to encapsulate an expression. For instance “(el|co)$”

\ The escape character.
In order to find a dot, “.” will not suffice since it will select any character. Specifying “\.” overrides the default operation of the dot.

{#,#} A certain count of the previous character.
The “{“ operator specifies a range. At least one is required.
“i.{2}e” would match “intel” since there are 2 characters between the I and e.
“{2}” or “{2,}” can be read as “only 1 character”.
“{1,4}” can be read as “between 1 and 4 characters”.

[range] A range of characters.
Ranges can be either an enumerated list of characters, such as “[abde]” or a hyphenated list such as “[A-Z]” or “[0-9]”. For instance “1[0-3]{2}” would match “103” and “121” but not “140” or “152”.
Additionally, ranges support the ^ operator for inversion. For instance, “^[^i]” would select say “airlink” and “netgear” but not “intel”.

Regular Expression Example

All local IPv4 networks

The IPv4 address ranges 10.0.0.0/8, 192.168.0.0/16, and 172.16.0.0/16 are reserved for local networks. A regular expression that matches all of them would be as follows:

```
^(192\.168|10\.|172\.16)
```

Security Disclosures

Please carefully read the following important disclosures.

- Unlike with Wireshark, once a valid decryption key is defined, all relevant subsequent traffic is automatically decrypted, and, if saved, will be stored decrypted to disk.
- Regardless of whether decryption keys are shown or hidden, they are stored on disk in plain text. Exporting a configuration file will export the plain text decryption keys that have been entered.

Appendix A Chart Types

The names for the various chart types are as follows.

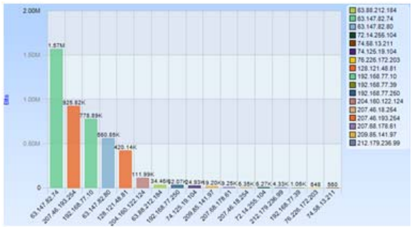


Chart Figure 54 Bar Chart

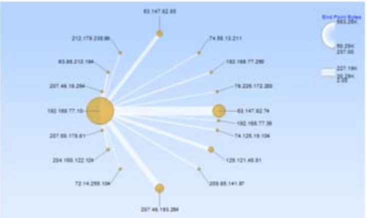
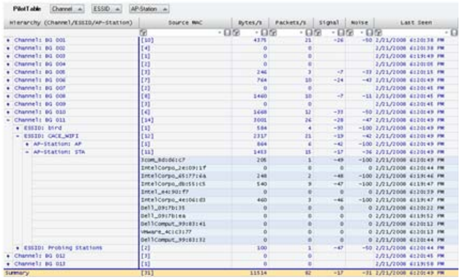


Chart Figure 55 Conversation Ring



Hierarchy (Channel/ESSID/AP-Station)	Source MAC	Bytes/s	Packets/s	Signal	Noise	Last Seen
+ Channel: BG 001	[10]	4375	21	-26	-50	2/21/2008 6:20:38 PM
+ Channel: BG 002	[4]	0	0			2/21/2008 6:20:38 PM
+ Channel: BG 003	[1]	0	0			2/21/2008 6:19:49 PM
+ Channel: BG 004	[2]	0	0			2/21/2008 6:20:06 PM
+ Channel: BG 005	[3]	246	3	-7	-33	2/21/2008 6:20:15 PM
+ Channel: BG 006	[7]	764	10	-24	-47	2/21/2008 6:20:49 PM
+ Channel: BG 007	[2]	0	0			2/21/2008 6:20:45 PM
+ Channel: BG 008	[8]	1440	10	-7	-11	2/21/2008 6:20:45 PM
+ Channel: BG 009	[3]	0	0			2/21/2008 6:20:45 PM
+ Channel: BG 010	[4]	1668	12	-33	-50	2/21/2008 6:20:49 PM
- Channel: BG 011	[14]	3001	26	-28	-47	2/21/2008 6:20:49 PM
+ ESSID: bird	[1]	584	4	-30	-100	2/21/2008 6:20:49 PM
- ESSID: CACE_WIFI	[12]	2317	21	-19	-42	2/21/2008 6:20:49 PM
+ AP-Station: AP	[1]	864	6	-42	-100	2/21/2008 6:20:49 PM
- AP-Station: STA	[11]	1453	15	-17	-36	2/21/2008 6:20:49 PM
	3com_8d:d6:c7	206	1	-49	-100	2/21/2008 6:20:49 PM
	IntelCorpo_2e:09:1f	0	0	0	0	2/21/2008 6:20:44 PM
	IntelCorpo_65:77:6a	248	2	-48	-100	2/21/2008 6:19:46 PM
	IntelCorpo_db:55:c5	540	9	-47	-100	2/21/2008 6:19:47 PM
	Intel_e4:90:f7	0	0	0	0	2/21/2008 6:20:39 PM
	IntelCorpo_4e:06:d3	460	3	-46	-100	2/21/2008 6:19:47 PM
	Dell_09:7b:35	0	0	0	0	2/21/2008 6:20:22 PM
	Dell_09:7b:ea	0	0	0	0	2/21/2008 6:19:52 PM
	DellComput_99:83:41	0	0	0	0	2/21/2008 6:20:12 PM
	Vmware_4c:c3:77	0	0	0	0	2/21/2008 6:20:13 PM
	DellComput_99:83:32	0	0	0	0	2/21/2008 6:20:44 PM
+ ESSID: Probing Stations	[2]	100	1	-47	-50	2/21/2008 6:20:44 PM
+ Channel: BG 012	[3]	0	0			2/21/2008 6:20:45 PM
+ Channel: BG 013	[1]	0	0			2/21/2008 6:19:58 PM
Summary	[31]	11514	82	-17	-31	2/21/2008 6:20:49 PM

Chart Figure 56 Data Grid

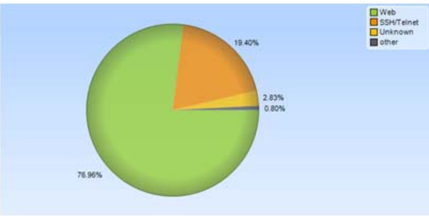


Chart Figure 57 Pie Chart

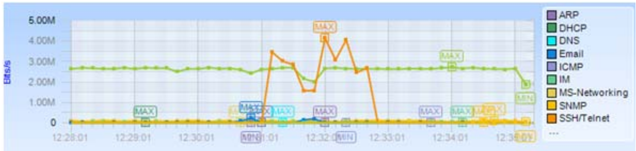


Chart Figure 58 Strip Chart

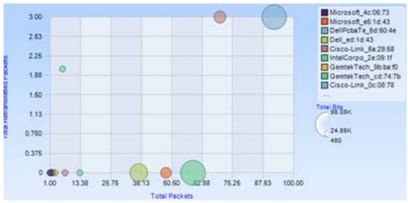


Chart Figure 59 Scatter Plot

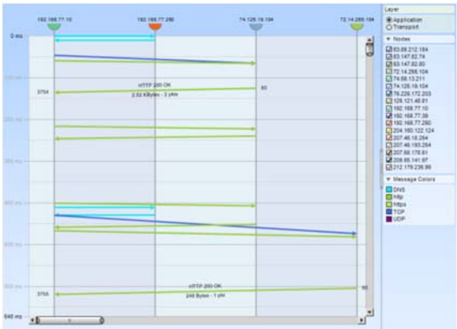
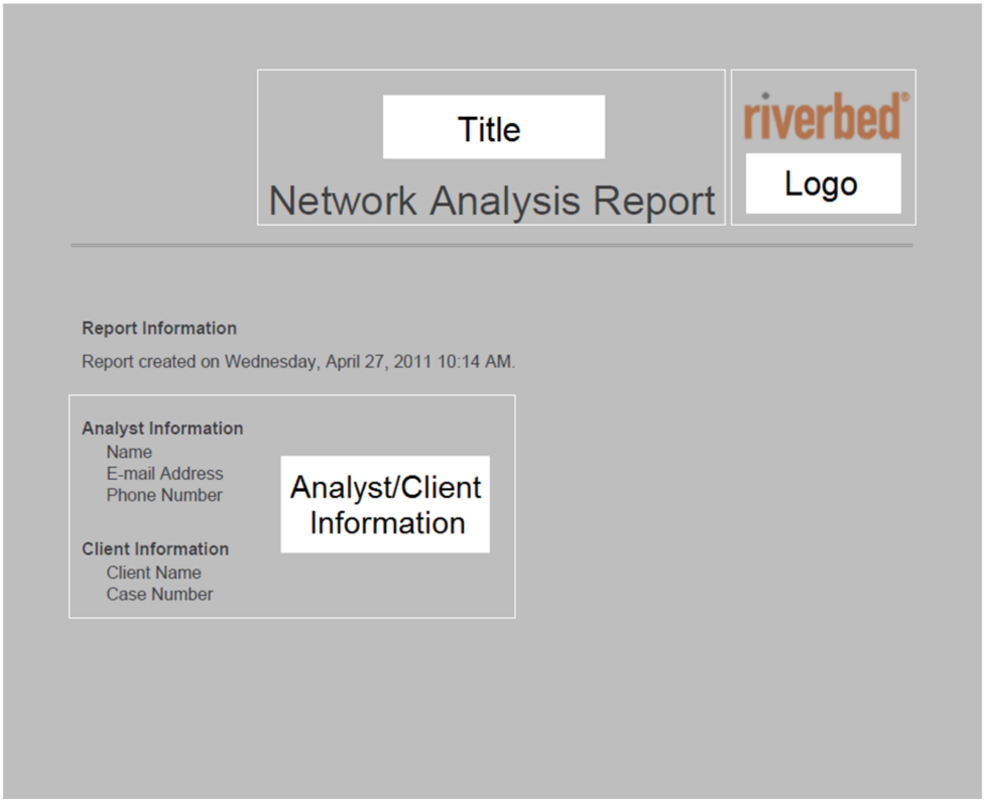


Chart Figure 60 Sequence

Appendix B Report Example Breakdown



Network Analysis Report

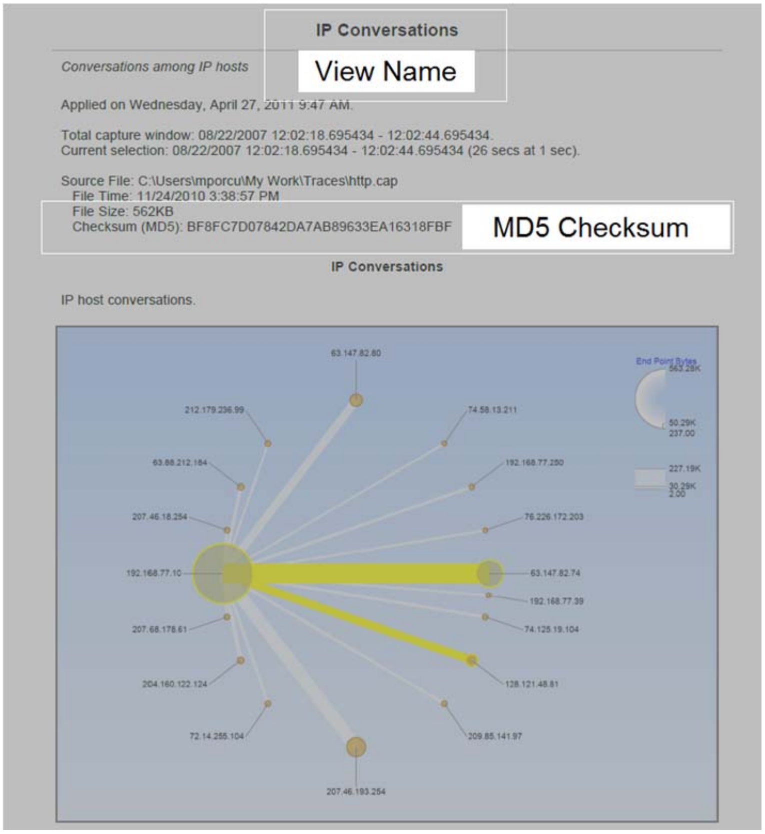
Report Information

Report created on Wednesday, April 27, 2011 10:14 AM.

Analyst Information
Name
E-mail Address
Phone Number

Client Information
Client Name
Case Number

Figure 164: Report layout



IP Conversations

Conversations among IP hosts

Applied on Wednesday, April 27, 2011 9:47 AM.

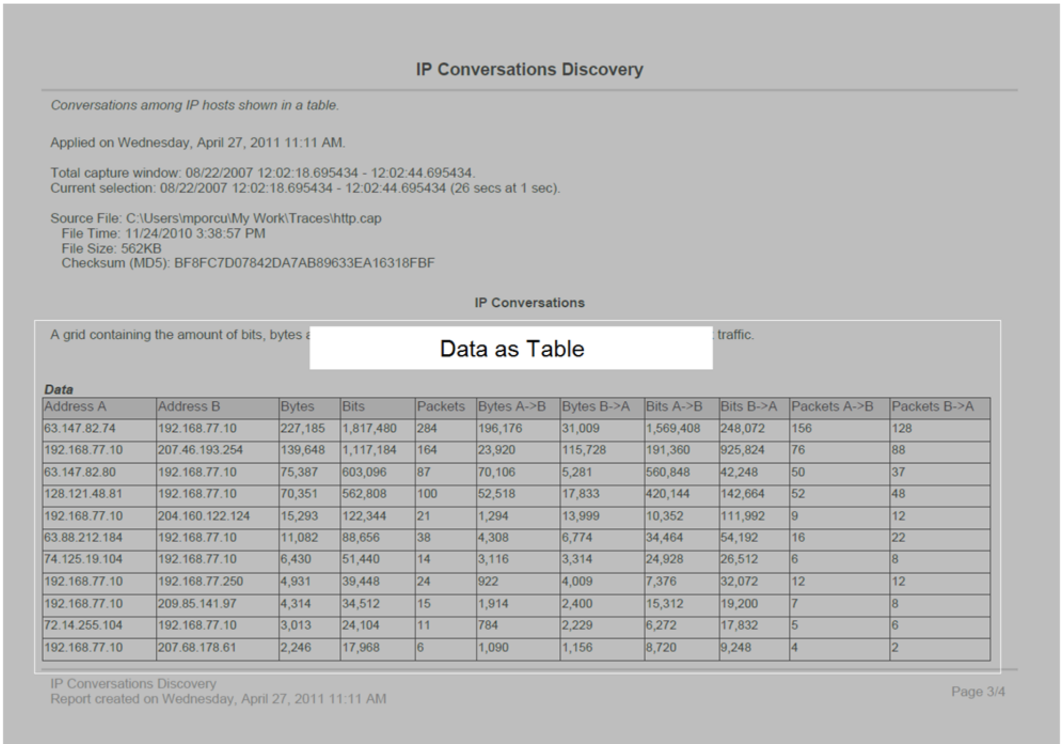
Total capture window: 08/22/2007 12:02:18.695434 - 12:02:44.695434.
Current selection: 08/22/2007 12:02:18.695434 - 12:02:44.695434 (26 secs at 1 sec).

Source File: C:\Users\mporcu\My Work\Traces\http.cap
File Time: 11/24/2010 3:38:57 PM
File Size: 562KB
Checksum (MD5): BF8FC7D07842DA7AB89633EA16318FBF

IP Conversations

IP host conversations.

Figure 165: IP Conversations layout



IP Conversations Discovery

Conversations among IP hosts shown in a table.

Applied on Wednesday, April 27, 2011 11:11 AM.

Total capture window: 08/22/2007 12:02:18.695434 - 12:02:44.695434.
Current selection: 08/22/2007 12:02:18.695434 - 12:02:44.695434 (26 secs at 1 sec).

Source File: C:\Users\mporcu\My Work\Traces\http.cap
File Time: 11/24/2010 3:38:57 PM
File Size: 562KB
Checksum (MD5): BF8FC7D07842DA7AB89633EA16318FBF

IP Conversations

A grid containing the amount of bits, bytes a traffic.

Data

Address A	Address B	Bytes	Bits	Packets	Bytes A->B	Bytes B->A	Bits A->B	Bits B->A	Packets A->B	Packets B->A
63.147.82.74	192.168.77.10	227,185	1,817,480	284	196,176	31,009	1,569,408	248,072	156	128
192.168.77.10	207.46.193.254	139,648	1,117,184	164	23,920	115,728	191,360	925,824	76	88
63.147.82.80	192.168.77.10	75,387	603,096	87	70,106	5,281	560,848	42,248	50	37
128.121.48.81	192.168.77.10	70,351	562,808	100	52,518	17,833	420,144	142,664	52	48
192.168.77.10	204.160.122.124	15,293	122,344	21	1,294	13,999	10,352	111,992	9	12
63.88.212.184	192.168.77.10	11,082	88,656	38	4,308	6,774	34,464	54,192	16	22
74.125.19.104	192.168.77.10	6,430	51,440	14	3,116	3,314	24,928	26,512	6	8
192.168.77.10	192.168.77.250	4,931	39,448	24	922	4,009	7,376	32,072	12	12
192.168.77.10	209.85.141.97	4,314	34,512	15	1,914	2,400	15,312	19,200	7	8
72.14.255.104	192.168.77.10	3,013	24,104	11	784	2,229	6,272	17,832	5	6
192.168.77.10	207.68.178.61	2,246	17,968	6	1,090	1,156	8,720	9,248	4	2

IP Conversations Discovery
Report created on Wednesday, April 27, 2011 11:11 AM

Page 3/4

Figure 166: IP Conversations Discovery layout

riverbed

Riverbed Technology
199 Fremont Street
San Francisco, CA 94105

Phone: 415.247.8800
Fax: 415.247.8801
Web: http://www.riverbed.com