SteelCentral Packet Analyzer Reference Manual

Personal Edition

Version 10.8

January 2015

riverbed®

Think fast.™

© 2015 Riverbed Technology. All rights reserved.

Riverbed®, SteelApp™, SteelCentral™, SteelFusion™, SteelHead™, SteelScript™, SteelStore™, Steelhead®, Cloud Steelhead®, Virtual Steelhead®, Granite™, Interceptor®, Stingray™, Whitewater®, WWOS™, RiOS®, Think Fast®, AirPcap®, BlockStream™, FlyScript™, SkipWare®, TrafficScript®, TurboCap®, WinPcap®, Mazu®, OPNET®, and Cascade® are all trademarks or registered trademarks of Riverbed Technology, Inc. (Riverbed) in the United States and other countries. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed or their respective owners.

F5, the F5 logo, iControl, iRules, and BIG-IP are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. Linux is a trademark of Linus Torvalds in the United States and in other countries. VMware, ESX, ESXi are trademarks or registered trademarks of VMware, Incorporated in the United States and in other countries.

Portions of SteelCentral™ products contain copyrighted information of third parties. Title thereto is retained, and all rights therein are reserved, by the respective copyright owner. PostgreSQL is (1) Copyright © 1996-2009 The PostgreSQL Development Group, and (2) Copyright © 1994-1996 the Regents of the University of California; PHP is Copyright © 1999-2009 The PHP Group; gnuplot is Copyright © 1986-1993, 1998, 2004 Thomas Williams, Colin Kelley; ChartDirector is Copyright © 2007 Advanced Software Engineering; Net-SNMP is (1) Copyright © 1989, 1991, 1992 Carnegie Mellon University, Derivative Work 1996, 1998-2000 Copyright © 1996, 1998-2000 The Regents of The University of California, (2) Copyright © 2001-2003 Network Associates Technology, Inc., (3) Copyright © 2001-2003 Cambridge Broadband Ltd., (4) Copyright © 2003 Sun Microsystems, Inc., (5) Copyright © 2003-2008 Sparta, Inc. and (6) Copyright © 2004 Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, (7) Copyright © Fabasoft R&D Software; Apache is Copyright © 1999-2005 by The Apache Software Foundation; Tom Sawyer Layout is Copyright © 1992 - 2007 Tom Sawyer Software; Click is (1) Copyright © 1999-2007 Massachusetts Institute of Technology, (2) Copyright © 2000-2007 Riverbed Technology, Inc., (3) Copyright © 2001-2007 International Computer Science Institute, and (4) Copyright © 2004-2007 Regents of the University of California; OpenSSL is (1) Copyright © 1998-2005 The OpenSSL Project and (2) Copyright © 1995-1998 Eric Young (eay@cryptsoft.com); Netdisco is (1) Copyright © 2003, 2004 Max Baker and (2) Copyright © 2002, 2003 The Regents of The University of California; SNMP::Info is (1) Copyright © 2003-2008 Max Baker and (2) Copyright © 2002, 2003 The Regents of The University of California; mm is (1) Copyright © 1999-2006 Ralf S. Engelschall and (2) Copyright © 1999-2006 The OSSP Project; ares is Copyright © 1998 Massachusetts Institute of Technology; libpq++ is (1) Copyright © 1996-2004 The PostgreSQL Global Development Group, and (2) Copyright © 1994 the Regents of the University of California; Yahoo is Copyright © 2006 Yahoo! Inc.; pd4ml is Copyright © 2004-2008 zefer.org; Rapid7 is Copyright © 2001-2008 Rapid7 LLC; CmdTool2 is Copyright © 2008 Intel Corporation; QLogic is Copyright © 2003-2006 QLogic Corporation; Tarari is Copyright © 2008 LSI Corporation; Crypt_CHAP is Copyright © 2002-2003, Michael Bretterklieber; Auth_SASL is Copyright © 2002-2003 Richard Heyes; Net_SMTP is Copyright © 1997-2003 The PHP Group; XML_RPC is (1) Copyright © 1999-2001 Edd Dumbill, (2) Copyright © 2001-2006 The PHP Group; Crypt_HMAC is Copyright © 1997-2005 The PHP Group; Net_Socket is Copyright © 1997-2003 The PHP Group; PEAR::Mail is Copyright © 1997-2003 The PHP Group; libradius is Copyright © 1998 Juniper Networks. This software is based in part on the work of the Independent JPEG Group the work of the FreeType team.

This documentation is furnished “AS IS” and is subject to change without notice and should not be construed as a commitment by Riverbed Technology. This documentation may not be copied, modified or distributed without the express authorization of Riverbed Technology and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This documentation qualifies as “commercial computer software documentation” and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed Technology assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

Individual license agreements can be viewed at the following location: https://*<appliance_name>*/license.php

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

riverbed

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com

712-00095-14

Contents

Overview 1
Packet Analyzer Personal Edition Feature Summary 1
Wireshark Integration 1
Views and Charts 1
Drill-down 1
Time Control 2
Filtering 2
Watches 2
Report Generation 2
Hardware and Software Requirements 3
Graphical User Interface 4
Graphical User Interface Components 4
Ribbon Panel 5
Sources Panel 5
Views Panel 6
Main Workspace 6
Events Panel 7
Filters panel 7
Menu Button, Quick Access Toolbar, and Status Bar 8
Menu Button 9
Quick Access Toolbar 10
Settings Menu 10
Status Bar 15
Home Ribbon 16
Trace Files 16
Add Trace File 16
Add Folder 17
Clear List 17
General 17
Search 17
Update Sources 17

Close All Tabs 17
Getting Started 18
Wireless 18
Channels 18
Decryption Keys 18
View 19
Save 19
Restore 19
Detach 19
Chart Selection 20
Send to Wireshark 20
Send to File 20
Drill Down 20
Copy 20
Copy Chart 20
Time Control 21
Time Control Fundamentals 21
Time Control Ribbon 23
Quick Navigation 23
Begin 24
Step Back 24
Step Forward 24
End 24
Selection Duration 24
Time Selection 25
Watches and Events 26
Creating Watches on Strip Charts and Bar Charts 26
Watch in Sources Panel 27
Context Menu for Watch Applied to a Live Source 27
Context Menu for Watch Applied to a Trace File 27
The Watch Editor 28
Name and Description 28
Severity 29
Enabled 29

Trigger Conditions 29
Entering Values in Watch Triggers 30
Expanded Trigger Condition 31
Multi-line Strip Charts 31
Timing Details for Bar Charts 32
Actions 33
Transition Conditions 33
Notify Me 35
Send an email with the watch event details 36
Start a packet capture 36
Send a remote syslog message over UDP 37
Log the events in the Probe's syslog 37
Log the events in a CSV file 37
Watches/Events Ribbon 38
Add Watch 38
Selected Watches 38
Edit Selected Watch 38
Remove Selected Watch 38
Enable Selected Watch 39
Disable Selected Watch 39
Filtering Events Section 39
Views Filter 41
Severities Filter 42
Severities List 42
Watches and Events Filter 42
Events Overlay 43
Predefined Watches 44
Reporting Ribbon 46
Generate Report 46
Current View 46
All Views 47
Format 48
Open Reports 48
Management 49

Recent 49
Change Folder 49
Browse Folder 49
Settings 50
Title 50
Analyst/Client Information 50
Designer 50
Report Designer Ribbon 51
Styles 51
Includes 51
Change Logo 51
Table of Contents 52
Checksums 52
Cover Page 52
Data as Table 52
Visual Settings 52
White Chart Background 52
Draft Images (Faster) 52
Page Setup 53
Size 53
Orientation 53
Display 53
Page Width 53
Full Page 53
Custom 53
Close Designer 54
Sources Panel 55
Devices 55
Wired Ethernet Adapters 56
Wireless Adapters 56
Context Menus in the Devices Panel 56
With Nothing Selected 56
With an Interface Selected 57
With a View Selected 58

Files 59
Context Menus in the Files Panel 60
With Nothing or Local System Selected 60
With a Trace Folder Selected 61
With a Trace File Selected 62
With a View Selected 63
Views Panel 64
Using Views 65
Applying a View 65
Applying a View with a Filter 66
View Library 67
Context Menus 67
Tooltips 69
Recently Used 69
Context Menus 69
Custom Views 70
Context Menus 70
Search Text Box 74
Regular Views, Fast Views, and Forbidden Views 74
Microflow Indexing 75
Indexing a Trace File 75
Apply an Index to a Trace File 75
Context Menu 75
Add Microflow Index 75
Interrupt Microflow Index 76
Remove Microflow Index 76
Index Icons on Trace Files 77
Tooltips 77
Drag and Drop Cursors for Indexed Trace Files 78
Search Text Box 78
Main Workspace 79
Context Menus 80
Tooltips 80
Notes 81

Selection 81
Undocking Views 82
Conversation Ring 89
Default 89
Size Legends 90
Scroll Wheel 90
Hover with Tooltip 90
Selected 91
Top Conversations 91
Context Menu 92
Tooltips 93
Endpoint 94
Conversation 95
Strip Chart 96
Diagram 96
Current Selection Interval 96
Display Modes 98
Data Display 100
Stacking Order 100
Custom sampling interval 101
Selection 101
Context Menu 104
Tooltips 106
Bar Chart 107
Single Bar Chart 107
Default 107
Selection 107
Stacked Bar Chart 108
Default 108
Selection 108
Grouped Bar Chart 109
Default 109
Selection 109
Navigation Through Data 111

Context Menu 111
Context Sub-Menus 113
Tooltips 114
Scatter Plot 115
Default 115
Selection 116
Context Menu 117
Context Sub-Menus 118
Tooltips 120
Pie Chart 121
Default 121
Selection 121
Context Menu 122
Context Sub-Menus 123
Tooltips 124
Data Grid 125
Grouping Bar 126
Column Headers 126
Sorting 126
Filter Bars 126
Values 127
Operators 128
Selection 128
Summaries 129
Context Menu 130
Context Sub-Menus 132
Channels Button 133
All Channels 135
2.4GHz Center Frequencies: 135
5GHz Center Frequencies: 135
Channel Names 135
All Channels Panel 136
Channel List 137
Selection Controls 137

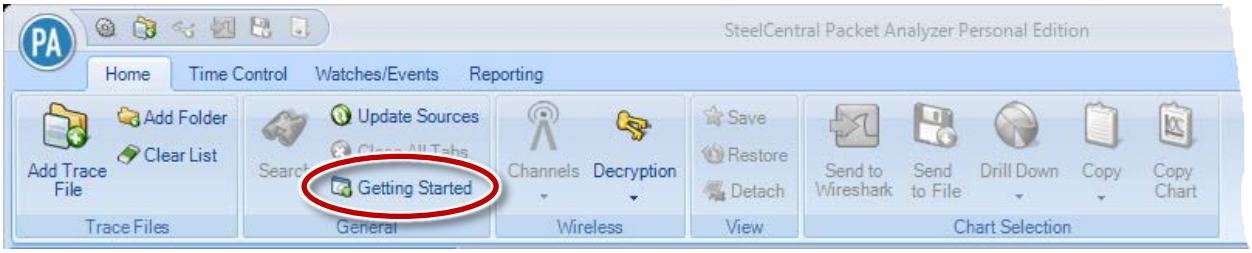
Search and Filter Bar 137
Locked Channels 138
Title 138
Selection Controls 138
Transfer Controls 138
Scan Sequence 139
Duration 139
Selection Controls 139
Transfer Controls 140
Scan Sequence 140
Decryption 141
Wireless Decryption Keys Manager 141
Adding a Key 142
WPA Related Packet Injection 143
Drill Down 145
How to 145
Examples 145
Filtering 146
Filter panel 146
Apply 147
Prepare 147
Edit 148
Delete 148
Duplicate 148
Move to Top 148
New Filter/Folder 148
Sort 149
Reset Filters 149
Filter Bar 150
Save 151
Delete 151
Apply 151
Prepare 151
Delete All 152

Filter Dialog 153
Search Dialog 154
Search Context 154
Search Style 154
Regular Expression Example 156
Security Disclosures 157
Appendix A Chart Types 158
Appendix B Report Example Breakdown 159

About this guide

The purpose of this reference manual is to document and explain each Riverbed® SteelCentral™ Packet Analyzer personal edition 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 Packet Analyzer personal edition. Video tutorials on how to perform common actions are available in the product. Upon startup, Packet Analyzer personal edition displays links to video tutorials. These can also be accessed at any time by clicking the *Getting Started* icon, located in the "General" section of the "Home" tab.



Overview

Riverbed® SteelCentral™ Packet Analyzer personal edition is a Windows-based packet analysis tool that provides network visibility through live traffic monitoring and analysis. It analyzes traffic seen on the local interfaces of the Windows platform on which it is installed, including traffic monitored by Riverbed AirPcap™ wireless LAN packet capture adapters. It also analyzes standard .pcap packet trace files. Its graphical user interface supports a wide variety of views and charts for analyzing network traffic on local interfaces or trace files.

Packet Analyzer Personal Edition Feature Summary

SteelCentral Packet Analyzer personal edition includes the following features:

- Wireshark integration
- Views and charts
- Drill-down
- Time control
- Watches
- Report generation

Wireshark Integration

Packet Analyzer personal edition is 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, Packet Analyzer personal edition can select a 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 Packet Analyzer personal edition. 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 as part of Packet Analyzer personal edition automated report generator.

Drill-down

Drill-down is one of the most powerful and unique features of Packet Analyzer personal edition. 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

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

selections to a Chart display. This simple yet powerful exercise increases your analysis capabilities many-fold. By employing this visually based drill down feature, Packet Analyzer personal edition 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 Packet Analyzer personal edition "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 NetShark, BPF, Wireshark and time filters. Users can also organize custom filters in folders in the Filter panel.

Watches

Packet Analyzer personal edition 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 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

Hardware and Software Requirements

Beginning with release 10.5, Packet Analyzer personal edition (formerly Cascade Pilot Personal Edition) no longer requires administrator privileges to install the product for use by a single user on a PC. To enable all users on a PC to run Packet Analyzer personal edition, the installer must be run by a user with administrative privileges. “Install for All users” is the default setting for the installer.

Each user requires a single-seat license to activate Packet Analyzer personal edition. License activation requires administrative privileges. Once a user’s license is activated, they can open and operate Packet Analyzer personal edition. For installation instructions, see the *SteelCentral Packet Analyzer Installation Guide*.

Although the system requirements for Packet Analyzer personal edition scale with usage, the following minimum configuration is recommended to use Packet Analyzer personal edition effectively:

Operating System	Windows XP (SP3), Windows Vista, Windows 7, Windows 8, Windows 8.1
System Software	Microsoft NET Framework 4.0 (or later)
Host Hardware	A dual-core 2.0 GHz CPU or better
Available Disk Space	*Base installation*: approximately 300MB *Plus*: additional space for generated reports or trace files
Memory	2 GB or more of system memory
Video Hardware and Settings	A graphics card with a minimum resolution of 1024 x 768
Display Settings	Text size: 100% (default) - displayed text may be truncated when a larger text size is used – see Control Panel > All Control Panel Items > Display
Internet Access	(Recommended) Used to activate a single-seat license online

Graphical User Interface

Graphical User Interface Components

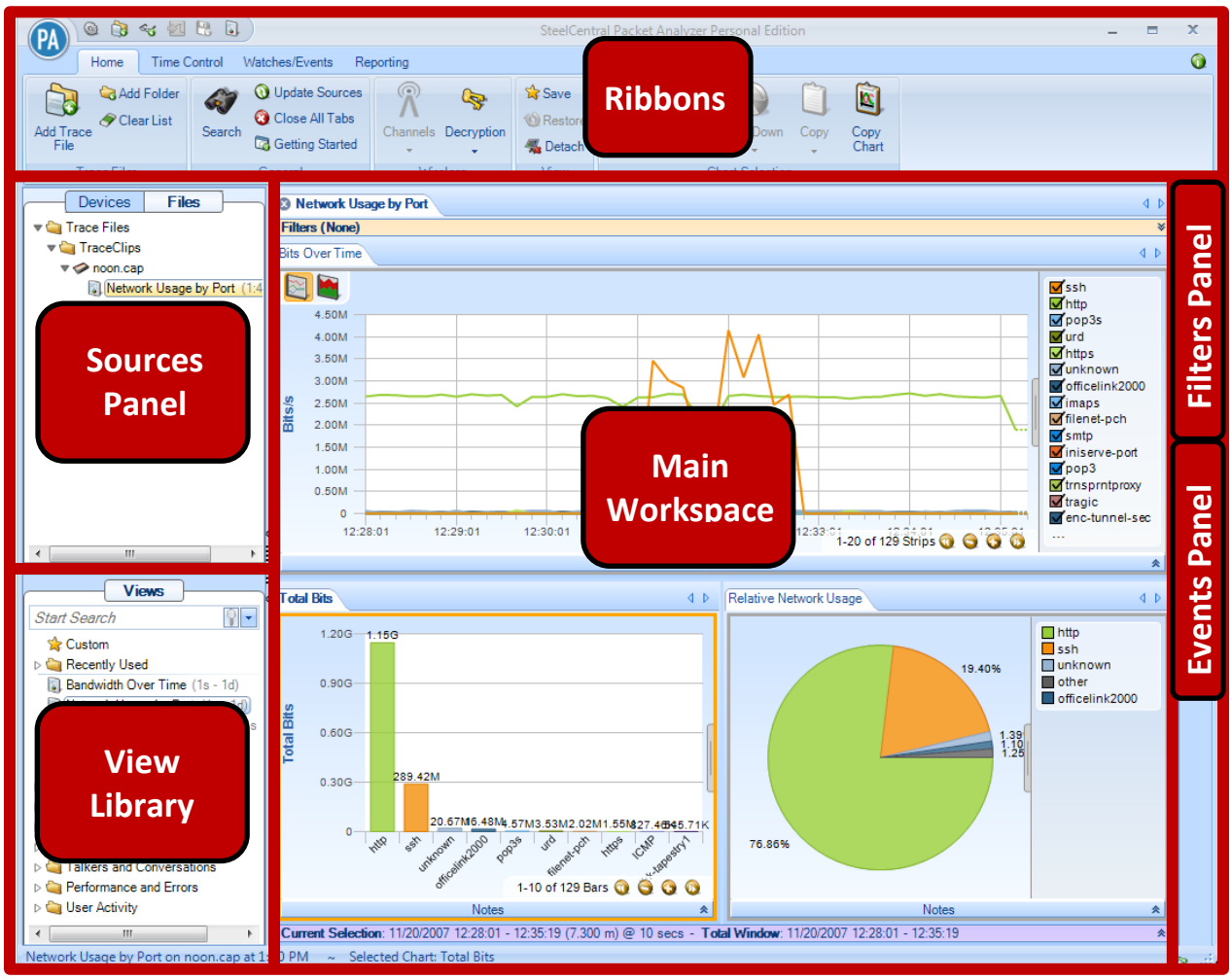


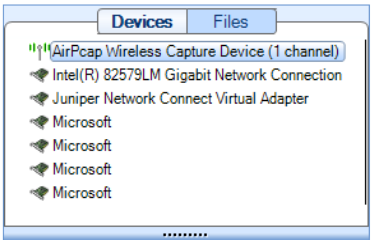
Figure 1: User Interface Breakdown (Major)

The graphical user interface of Packet Analyzer personal edition, divided into the six main sections, is shown in Figure 1. Each section represents a major topic in this manual. The descriptions below are conceptual overviews of each section.

Ribbon Panel

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

Sources Panel



The *Sources Panel* contains representations of interfaces and trace files, and is one of the most important parts of Packet Analyzer personal edition. It has two tabs, "Devices" and "Files" that can be cycled through by clicking on them.

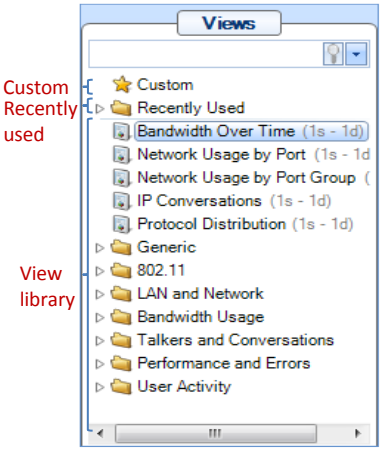
Devices

Shows local interfaces that offer live sources of network traffic.

Files

Shows folders and trace files on the local system.

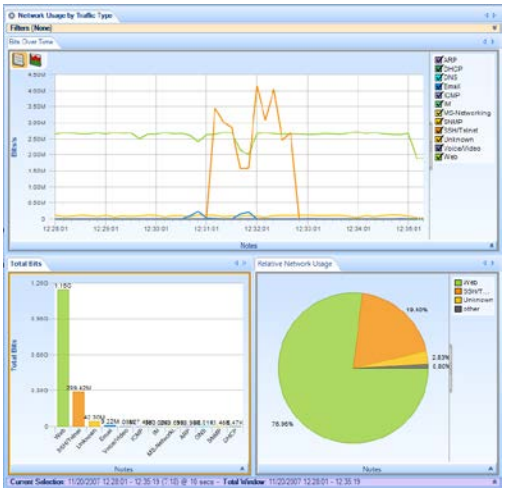
Views Panel



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.).

To find Views and Folders quickly, enter one or more keywords in the Search box at the top of the Views Panel. The scope of the search includes titles and descriptions by default; you can expand the scope using the drop-down menu (down arrow) on the right side of the search box.

Main Workspace



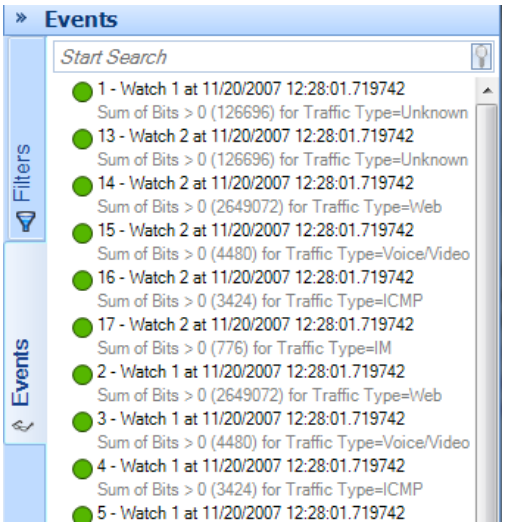
The *Main Workspace* has tabbed windows that can be one of the following:

- 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.

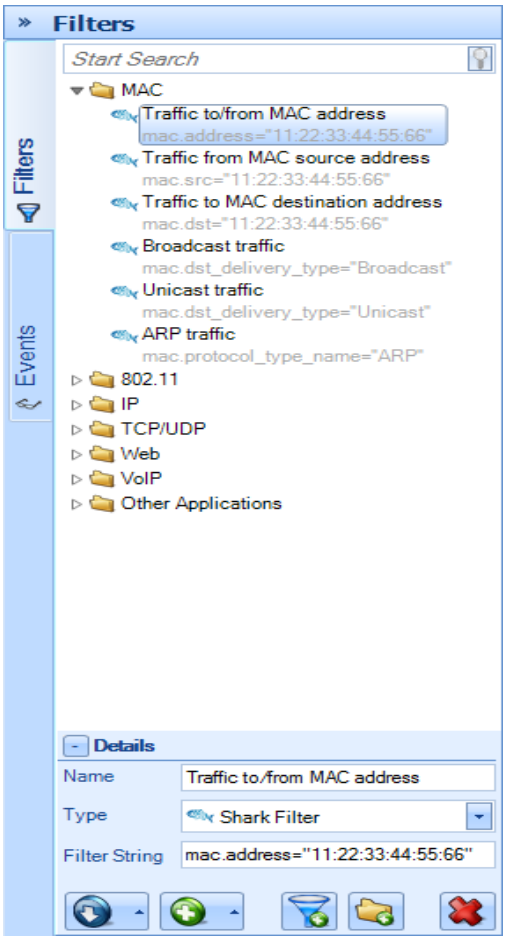
In addition, you can "undock" the main workspace to create a separate window that you can enlarge and place wherever you want, even on a second monitor.

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.

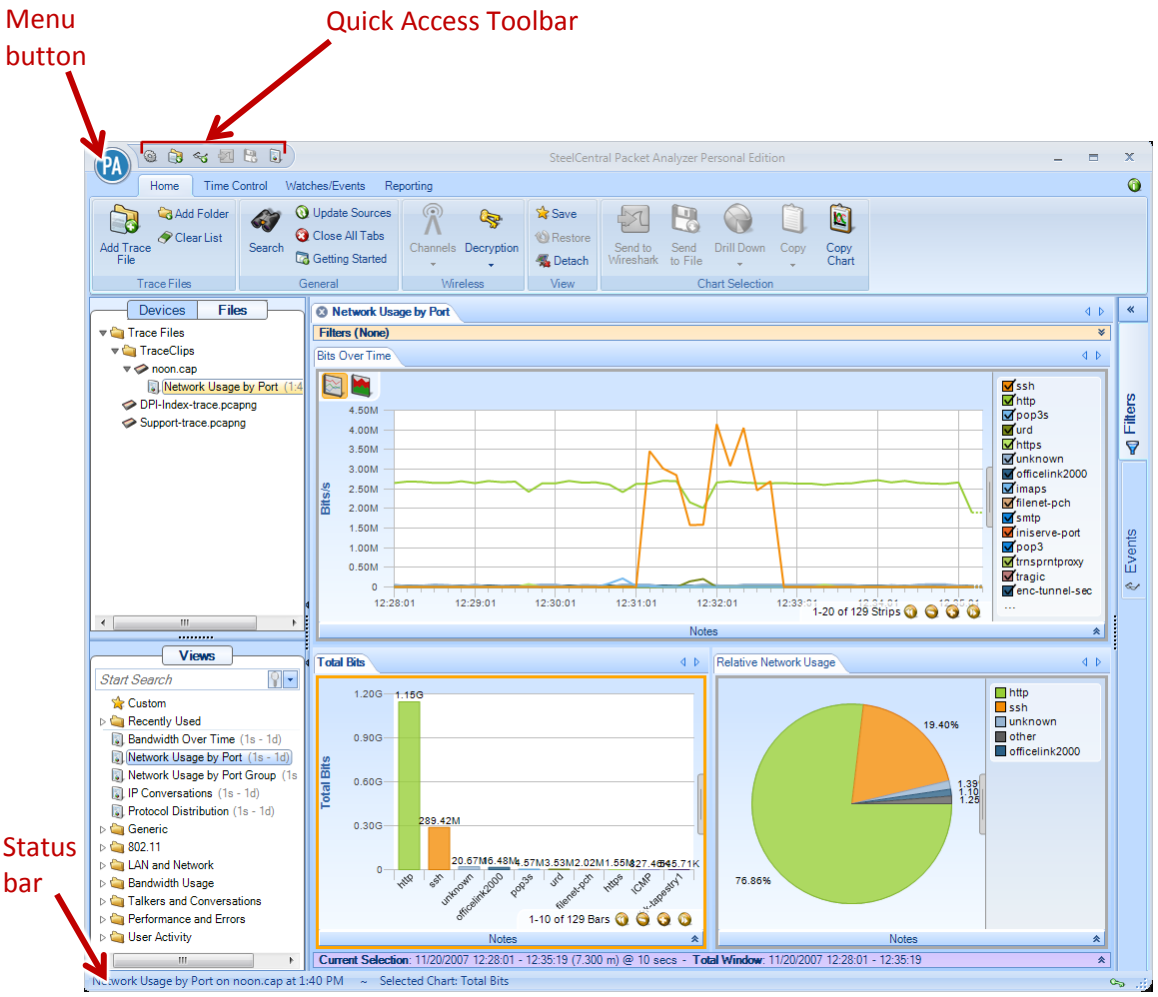
Filters panel



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.

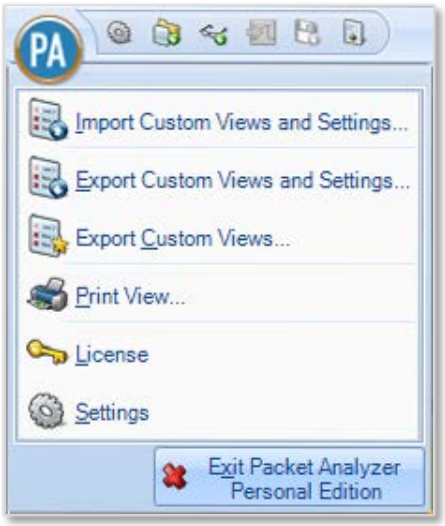
Menu Button, Quick Access Toolbar, and Status Bar

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



User Interface Breakdown (Minor)

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 Packet Analyzer personal edition. This applies to all settings in the global configuration file, which are enumerated throughout this manual. Briefly, it entails items such as

- Custom views
- Custom filters
- 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 Packet Analyzer personal edition. 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 Packet Analyzer personal edition 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.

License

Opens the Packet Analyzer personal edition License page, providing a direct way to activate, deactivate or review your license information.

Settings

Opens the Settings menu, described below.

Quick Access Toolbar

The Quick Access Toolbar has the following buttons:

Settings
Opens the Settings menu, described below.

Add a Trace File
Adds a trace to the Files panel.

Send to Wireshark
Sends traffic from the current selection to Wireshark. This button is enabled only if a selection is made in the currently selected chart in the view.

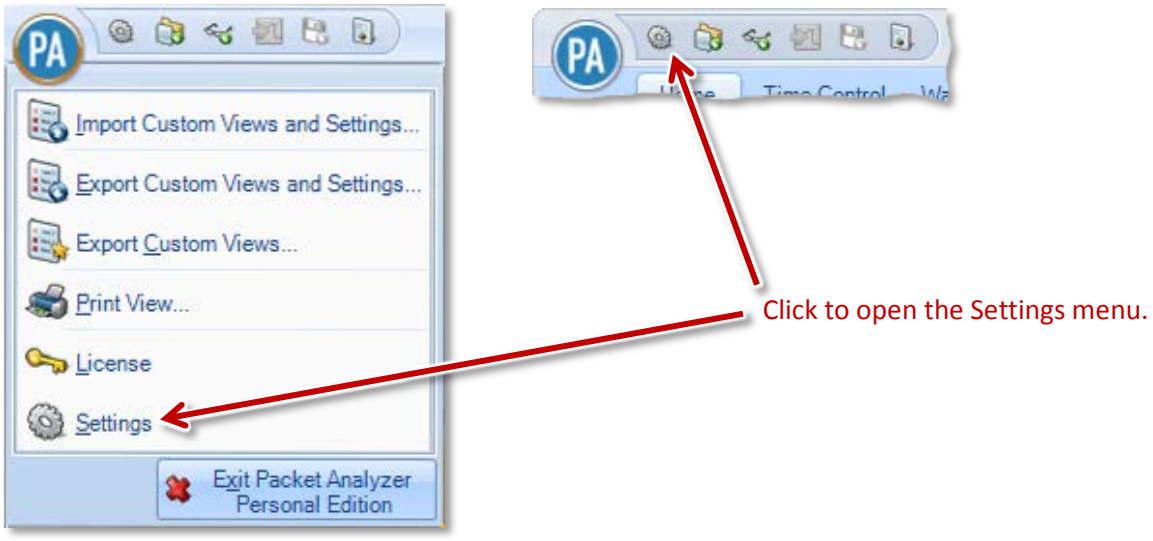
Send to File
Extracts traffic from the current selection and sends it to disk as a PCAP trace file. This button is enabled only if a selection is made in the currently selected chart in the view.

Create Report from Current View
Creates a report from the currently selected view.

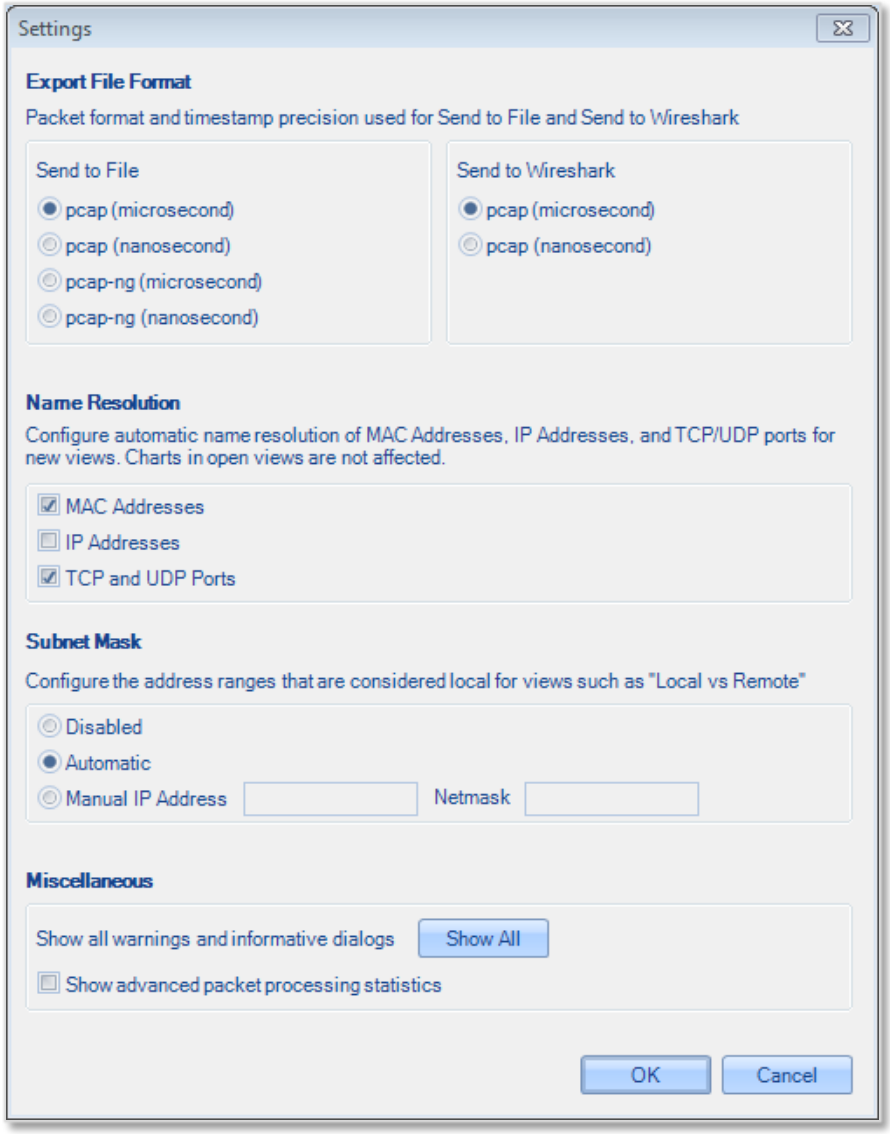
Settings Menu

The Settings menu lets you configure parameters for some of the operations available in Packet Analyzer personal edition.

Open the Settings menu by clicking the Menu button and selecting Settings from the drop-down list or by clicking the Settings icon in the Quick Access Toolbar.

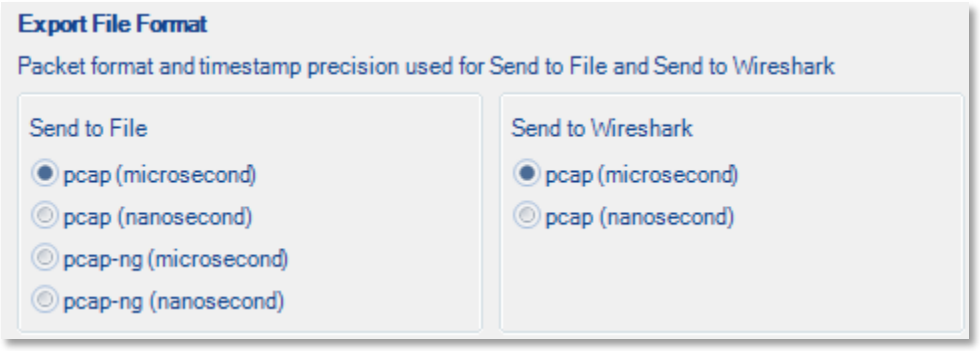


The Settings menu appears. The image below shows the default values.



Export file format

These settings determine the format and timing precision for "Send to…" operations.

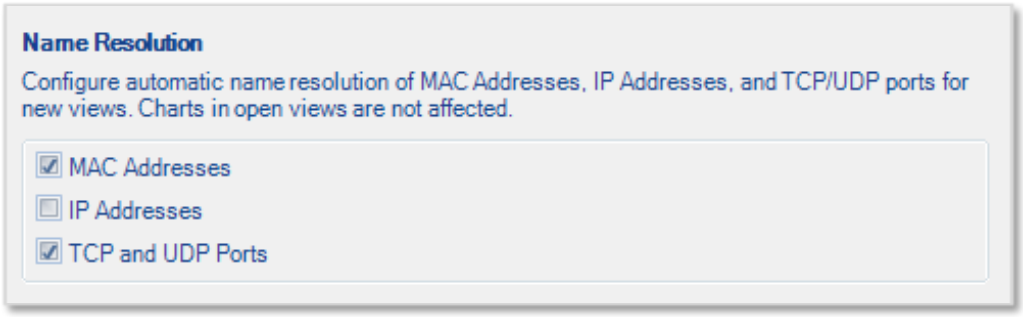


The "Send to File" option lets you configure the format that Packet Analyzer personal edition uses to create a trace file from another trace file or from a subset of one. In addition, this option is used when Packet Analyzer personal edition exports packets from a trace clip. This option is especially useful if you need to use a trace file with a tool that does not support the pcap-ng format or nanosecond timestamps.

The "Send to Wireshark" option lets you configure the format that Packet Analyzer personal edition uses to export a trace file or a subset of a trace file to Wireshark. Due to a limitation of Wireshark versions before 1.8.2, it is not possible to export packets with pcap-ng format to Wireshark.

Name Resolution

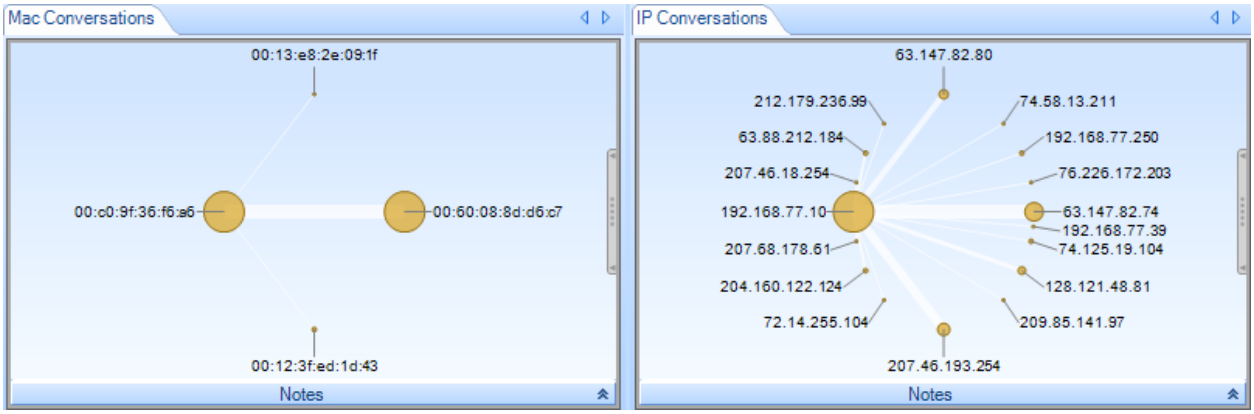
These settings let you determine whether MAC or IP addresses or TCP/UDP port numbers are presented as numbers or names (when possible). In views, name resolution can be set per chart using the Name Resolution item on a chart's submenu.



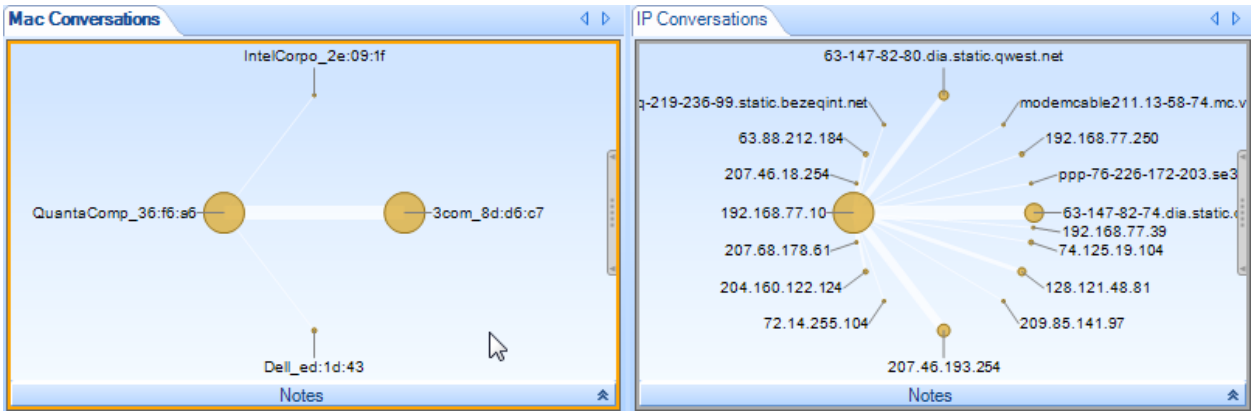
When a box is checked, Packet Analyzer searches its configuration files for names that are equivalent to MAC addresses, IP addresses, or TCP/UDP port numbers.

When you modify an option, only new views reflect the new options. There may be a brief delay while names are resolved.

For instance, here is a view with MAC and IP addresses not resolved:



And here is the same view with both MAC and IP addresses resolved:



Note that names have replaced some of the numbers in the addresses.

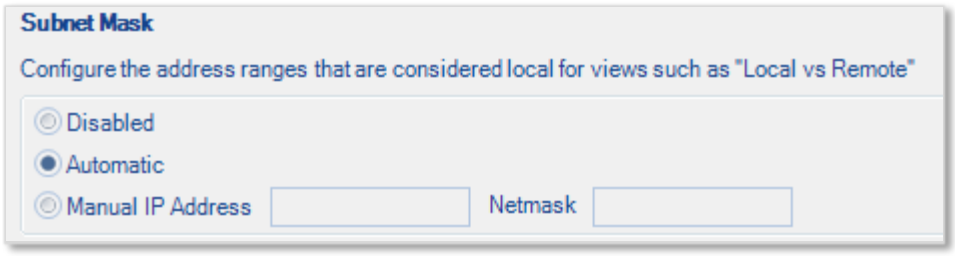
The name resolution is performed in Packet Analyzer personal edition, not in Riverbed® SteelCentral™ NetShark. MAC addresses and TCP/UDP port names are stored in these files:

- MAC addresses: [Packet Analyzer personal edition installation folder]\data\Manufacturers.xml
- TCP/UDP port names: [Packet Analyzer personal edition installation folder]\data\PortNumbers.xml

When you modify an option, all new views reflect the new options. There may be a brief delay while names are resolved.

Subnet mask

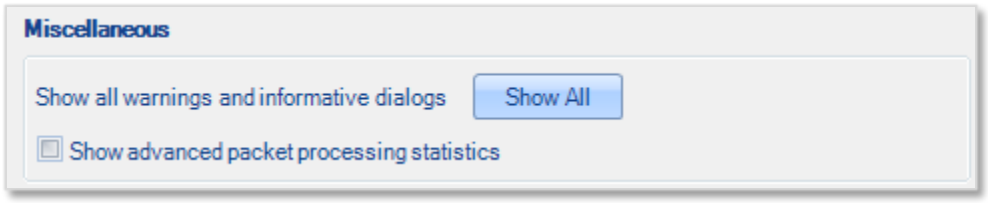
This option allows you to configure which addresses are considered to be "local" for some views.



- ***Disabled***: All IP addresses are considered local.
- ***Automatic***: Local System determines which is the best local address range (for instance, 192.168.0.0/16).
- ***Manual***: You specify the local address range by entering an IP address and a subnet mask.

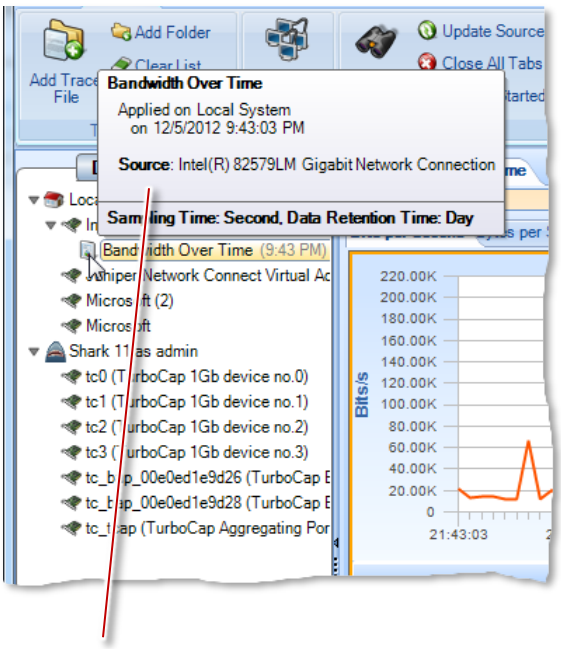
Changes are applied to the source type currently selected in the Devices/Files panel.

Miscellaneous

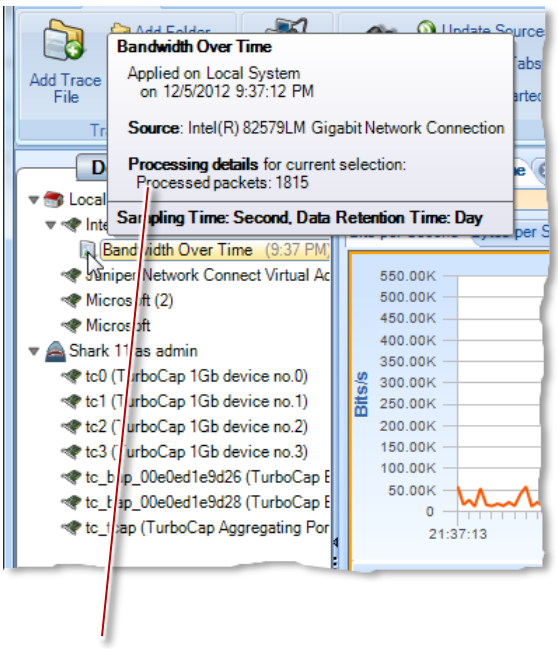


The "Show all warnings and informative dialogs" button lets you turn on the display of all warnings and dialogs. This can be useful if you have previously turned off the display of some messages (by checking a "Do not show this again" box), but want to start seeing those messages again.

The “Show advanced packet processing statistics” option defines whether Packet Analyzer personal edition exports processing statistics in tooltips or not.



Processing statistics disabled



Processing statistics enabled

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

The *Home Ribbon* serves as the primary interface to Packet Analyzer personal edition. 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** –Operations such as adding a link to a trace file in the Sources panel.
- **General** – Miscellaneous actions.
- **Wireless** – Wireless channel and decryption settings, name resolution, and subnet mask.
- **View** – Buttons for saving custom views, restoring default view settings, and detaching a view.
- **Chart 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 Packet Analyzer personal edition.***

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

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

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

General

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

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

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 Packet Analyzer personal edition recognizes a change of device. Packet Analyzer personal edition does not check for new adapters automatically. It checks only when this button is clicked.

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

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

- Access to video tutorials

Wireless

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

Channels

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 Packet Analyzer personal edition host system.***

Decryption Keys

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 Packet Analyzer personal edition and on wireless trace files located on the local system.***

View

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

Save

Save Custom View

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

Restore

Restore Default View

The *Restore* button restores default View settings.

Detach

The *Detach* button detaches the currently selected View from the source, whether the source is live or off-line. Once detached, the View is no longer visible in the Packet Analyzer personal edition main workspace. The View is still visible in the sources panel, but grayed out.

> *Note:* ***For live captures, the system 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 Packet Analyzer personal edition main workspace.

Chart 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 Chart Selection group. Each of these functions is also available through the context menu of any chart.

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.

Send to File

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.

Drill Down

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

Copy

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

Copy Chart

The Copy Chart button copies the selected chart as a metafile to the system clipboard for pasting into another application. A chart must be selected for this button to be enabled.

Time Control

The Time Control feature of Packet Analyzer personal edition 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.

Time Control Fundamentals

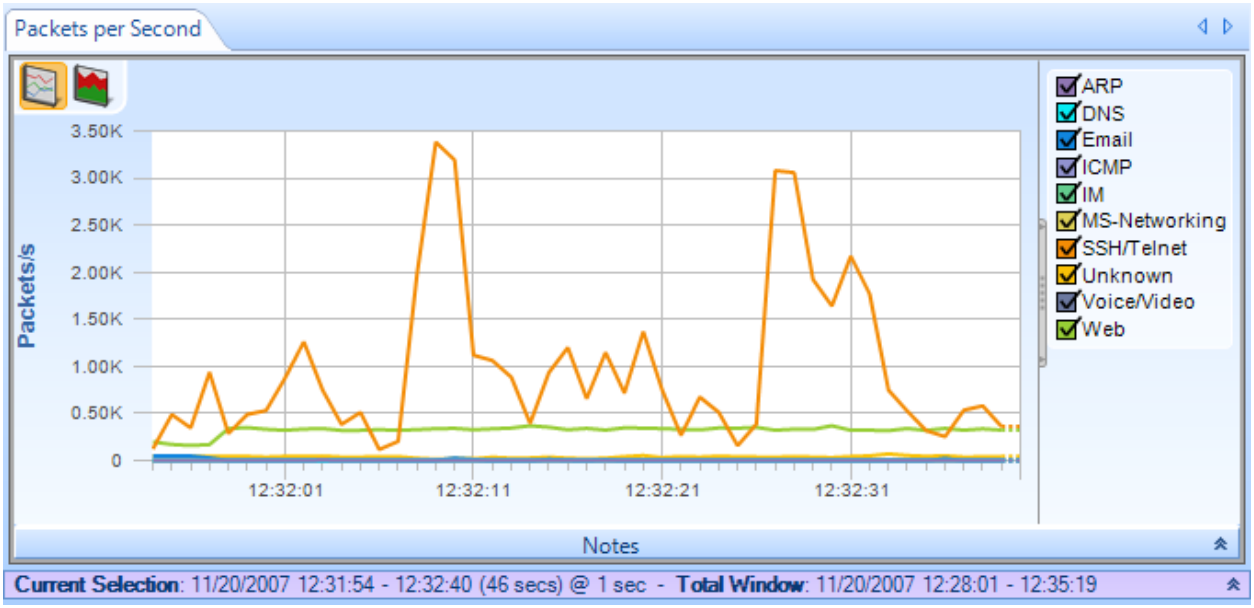


Figure 2 Port Group Over Time Showing Time Selection Windows

Figure 2 shows the Port Group 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 Packet Analyzer personal edition 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 Packet Analyzer personal edition analysis engine automatically selects the best level of subsampling based on the duration of the Current Selection.

Note: A view applied to a live source has a configurable "Data Retention Time" found on the view's context menu. The current setting is shown after Drop After: in the Time Controller.

Figure 3 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 Packet Analyzer personal edition, thereby making it very easy to move around and to zoom in and out of very long-duration trace files and live captures.

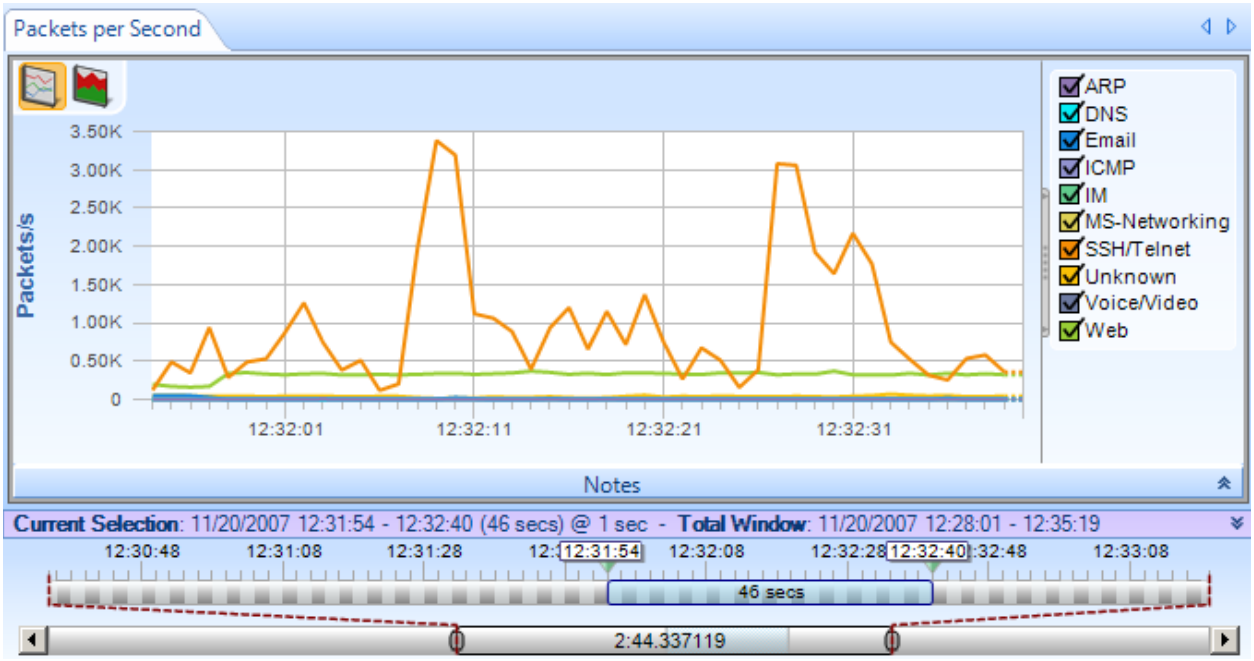


Figure 3 Port Group Over Time with Multi-Level Zoom Selection

Figure 4 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.)

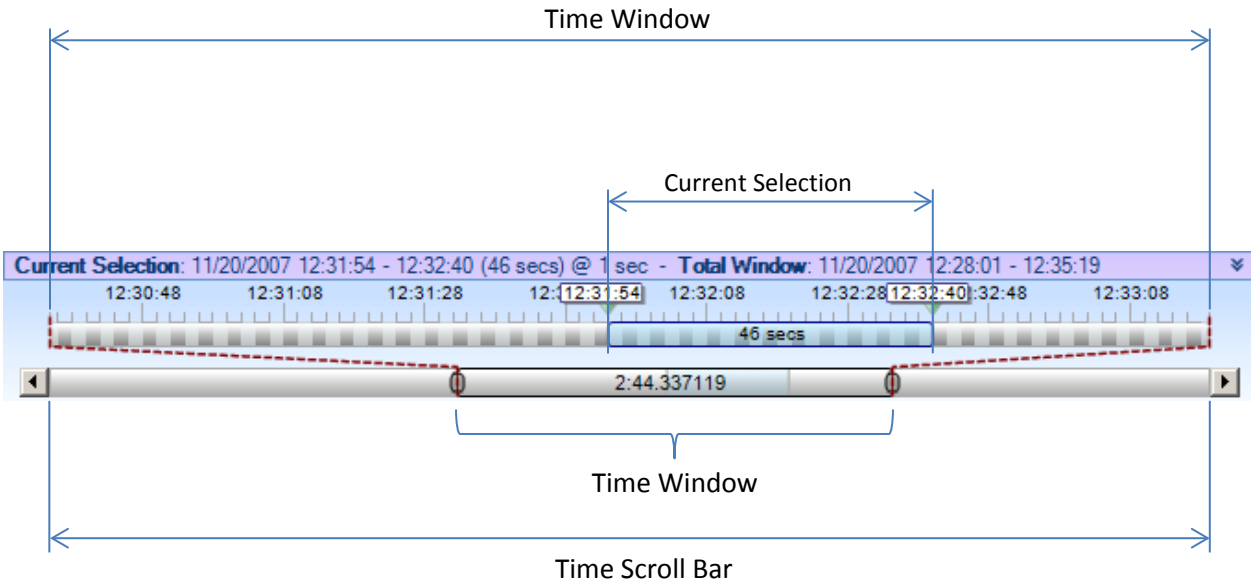
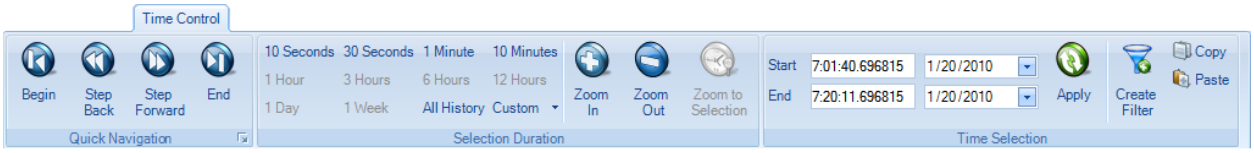


Figure 4 Time Control Bars

Time Control Ribbon



Time Control Ribbon

The Time Control feature of Packet Analyzer personal edition 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.

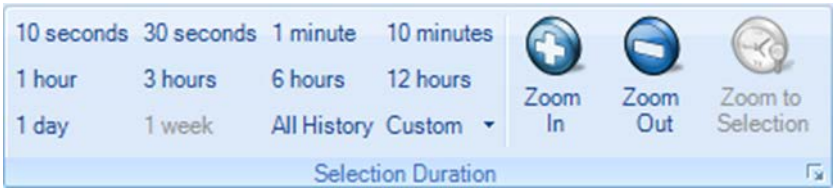
Step Forward

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



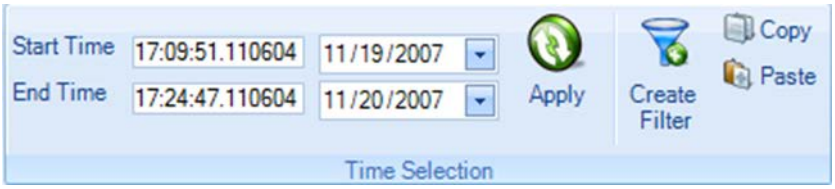
Selection Duration Section of the Time Control Ribbon

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



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

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.

> *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

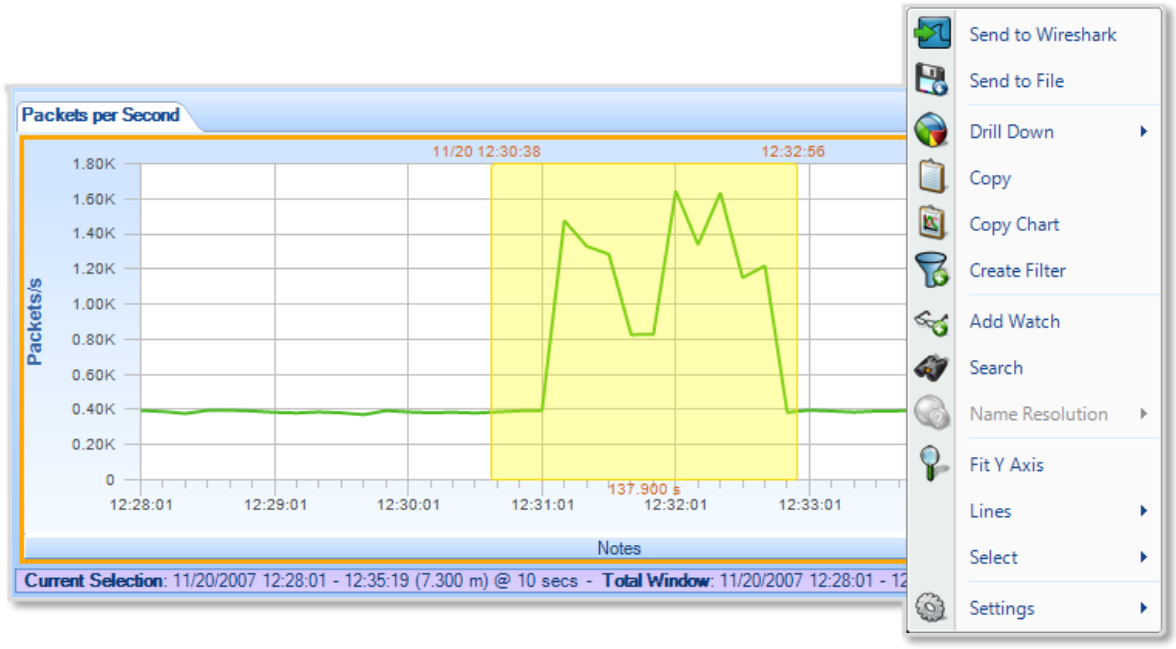


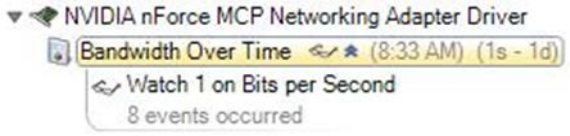
Figure 5 Strip Chart with Context Menu

Figure 5 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 6), 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 6). 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.

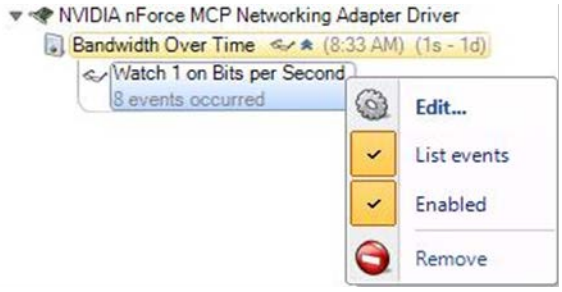
Watch in Sources Panel



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

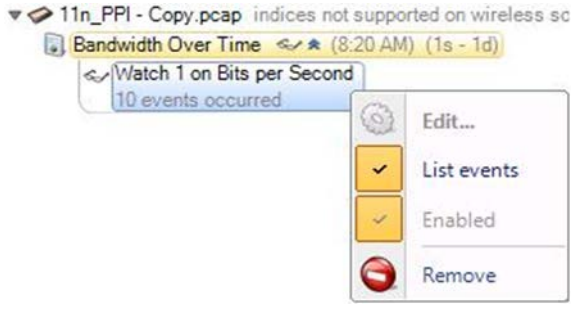


Context Menu For Watch Applied to Live Source

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



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

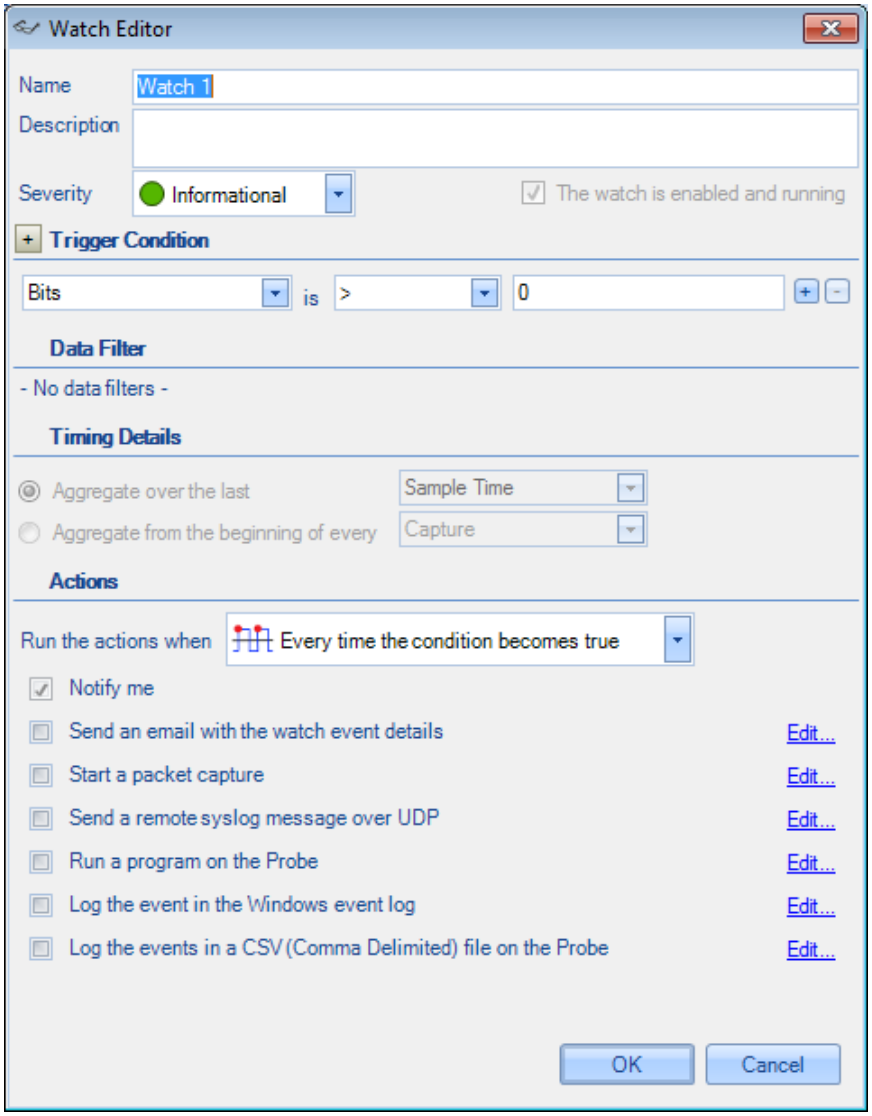


Figure 6 Watch Editor Panel

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 7 Watch Severity

The *Severity* field contains a drop-down list (see Figure 7) 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 8. Together they represent a Boolean condition; that is, an expression that evaluates to either True or False.

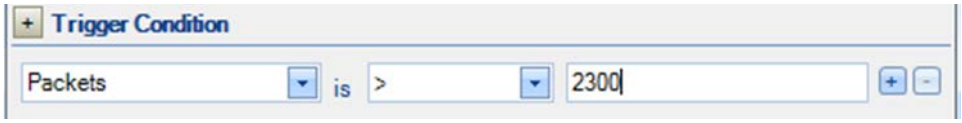


Figure 8 Trigger Condition

The left-most box contains the value to be tested. Recall that in Figure 5 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 9 for the list of operators.

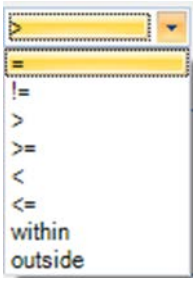


Figure 9 Relational Operators

Finally, there is the right-most box, which contains the comparison value. The Trigger Condition in the example shown in Figure 8 is true whenever Packets is greater than 2,300.

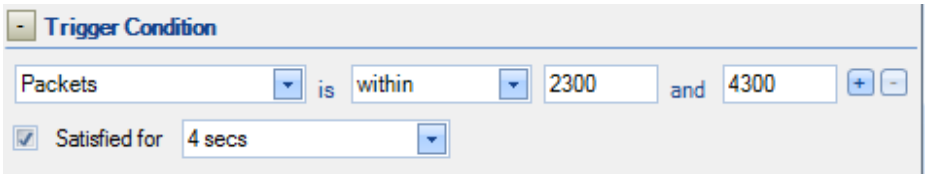


Figure 10 Trigger Condition Expanded

Figure 10 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 (>= lower limit and <= upper limit). Similarly, the "outside" condition is specified with lower and upper limits and is true when the value falls out of the specified range (<= lower limit or >= upper limit).

Entering Values in Watch Triggers

Beginning in Packet Analyzer version 10.7 (and later) an expanded set of units are available for specifying a trigger value. Values can be entered as a number and a unit that specifies a multiplier. For example, a Trigger Condition value of 1000000 now can be entered as 1M. The available units and their multiplier are listed below.

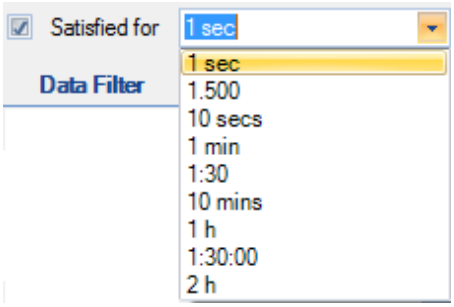
Unit	Multiplier	Multiplier value
k,K, kilo, Kilo	10^3	1000
M, mega,Mega	10^6	1000000
G, g,giga, Giga	10^9	1000000000
T,t,tera,Tera	10^{12}	1000000000000
P, peta, Peta	10^{15}	1000000000000000
E,e,exa, Exa	10^{18}	1000000000000000000
ki,Ki	2^{10}	1024
Mi,mi	2^{20}	1048576
gi, Gi	2^{30}	1073741824
Ti,ti	2^{40}	1099511627776
Pi, pi	2^{50}	1125899906842624
Ei,ei	2^{60}	1152921504606846976
m,milli, Milli	10^{-3}	0.001
u, micro, Micro	10^{-6}	0.000001
n,nano, Nano	10^{-9}	0.000000001
p, pico, Pico	10^{-12}	0.000000000001
f, femto, Femto	10^{-15}	0.000000000000001
a, atto, Atto	10^-18	0.000000000000000001

Entries for values (number times multiplier) must evaluate to integers. Engineering notion using "e" or "E" also is supported, for example, 2E6 corresponding to e*10^6 = 2000000. Time values cannot be entered using multipliers.

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 10), 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 2300 and 4300 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.



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 you can supply your own using the formats shown in the list.

Multi-line Strip Charts

In the case of a single line strip chart as in Figure 5, 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

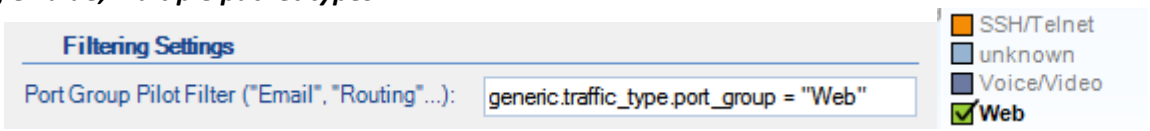


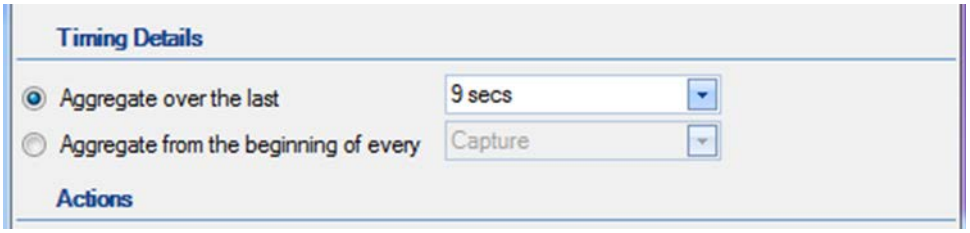
Figure 11 Multi-line Strip Chart with Filtering

Figure 11 depicts the case where the multi-line strip chart shows Port Group 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 port group for each Sample Time and generate an event for each port group for which the Trigger Condition is met. This means that there could be as many events generated at each Sample Time as there are port groups. 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 11 shows that one line, Web, has been selected. The Watch Editor acknowledges the line selection under the Data Filter section and automatically appears.

Multiple values, single packet type

Figure 12 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

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.

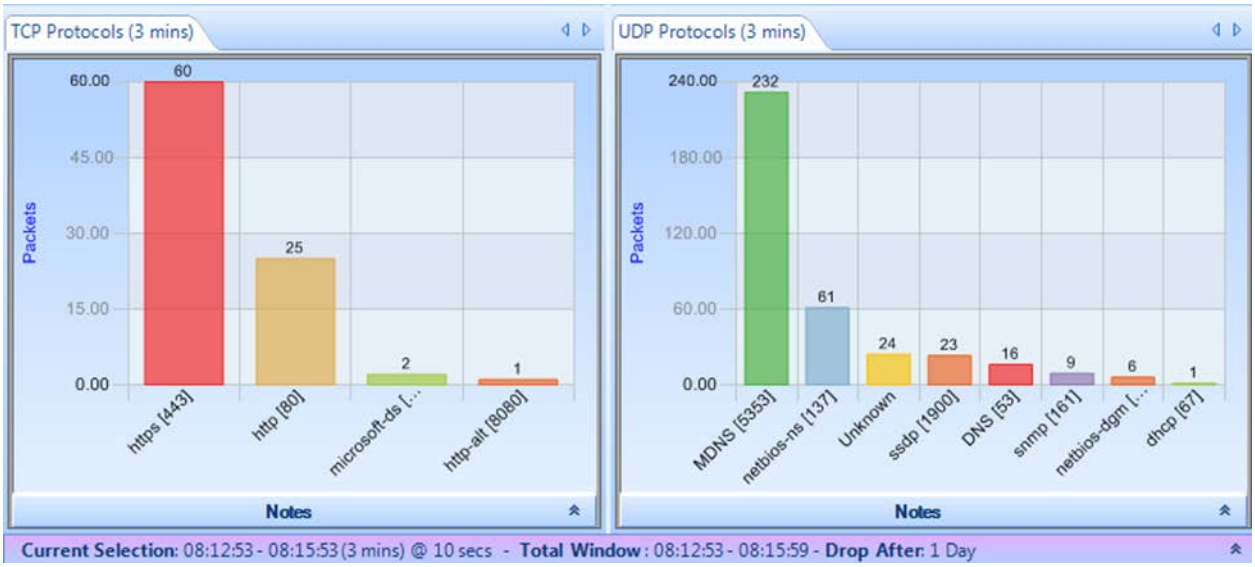


Figure 12 Aggregating Chart

The Current Selection interval in Figure 12 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 Packet Analyzer personal edition, 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

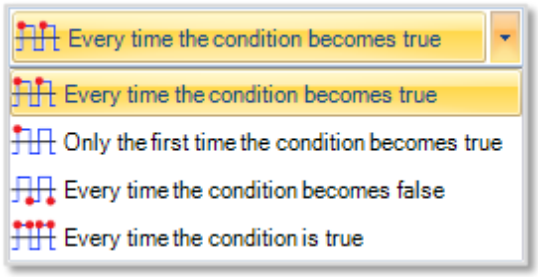


Figure 13 Transition Condition List

In Figure 13 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.

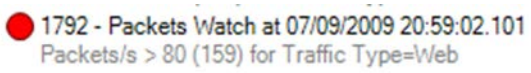
Note: ***A Trigger Condition, along with its associated transition condition, is based on a View associated with the local. Accordingly, the actions associated with the trigger condition are initiated by the local system.***

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.

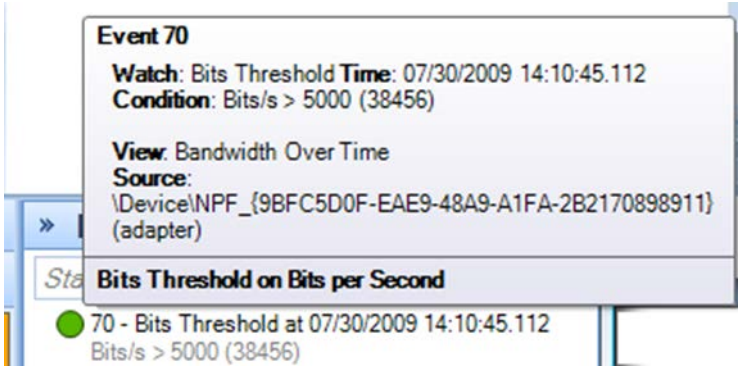
Figure 14 Event Notifications

Figure 14 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.



Event Structure

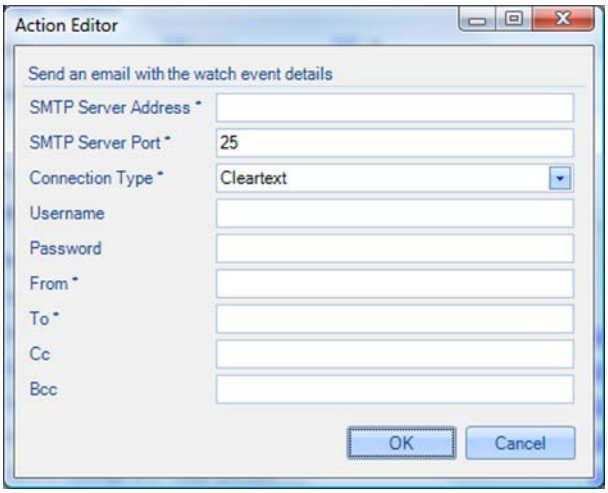
The Event Structure begins with a circle with the color corresponding to the color of the Watch Severity. The following number is the event Unique ID followed by the name of the event. This is followed by the date and time at which the event occurred. The second line begins with the Trigger Condition 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.



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.

Send an email with the watch event details



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

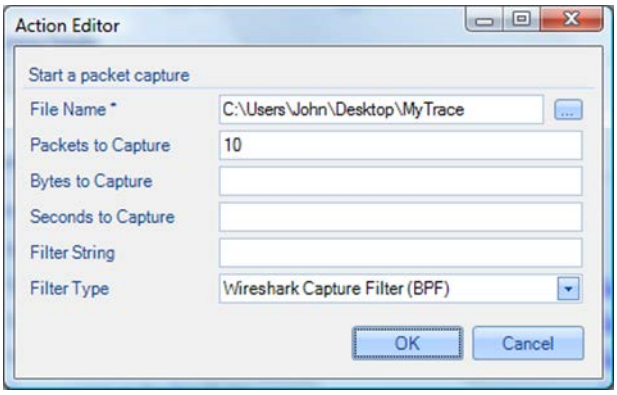
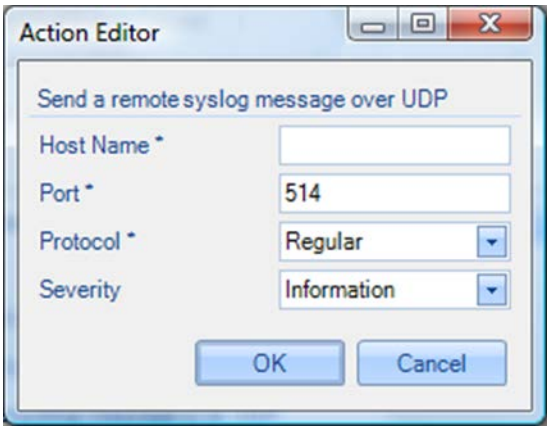


Figure 15 Capture Packets Panel

When "Start a packet capture" is selected, the panel in Figure 15 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.

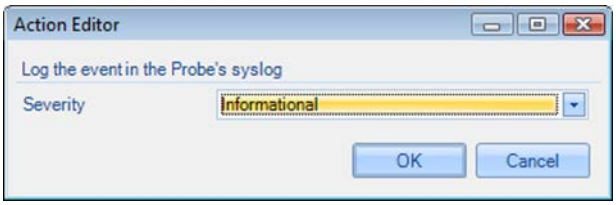
Send a remote syslog message over UDP



Send a syslog message using UDP to a remote host.

Send to Remote Syslog

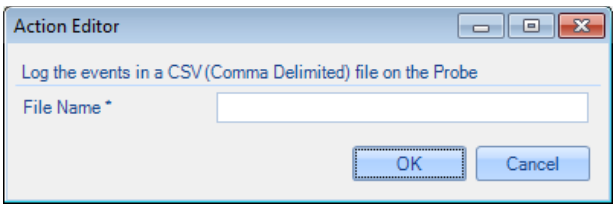
Log the events in the Probe's syslog



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

Send to Probe's syslog

Log the events in a CSV file

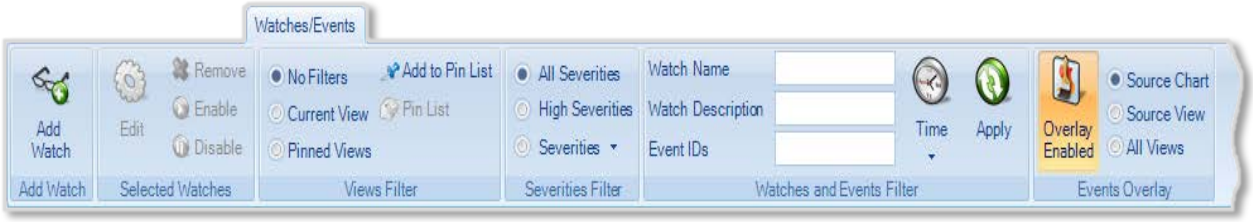


The event is written as a CSV file using the complete pathname provided in the Action Editor.

Send to CSV File

Watches/Events Ribbon

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



Watches and Events Ribbon

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

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

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

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

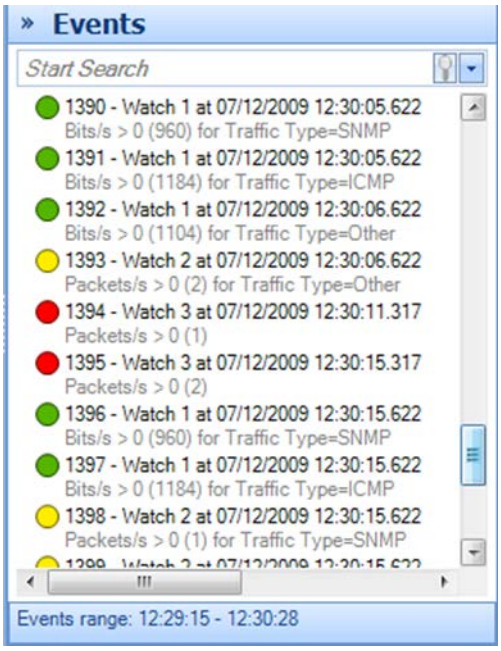
> *Note:* ***A Watch applied to a trace file cannot be enabled.***

Disable Selected Watch

With an enabled Watch selected in the Sources panel, the *Disable* 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



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 16 Event Filtering Section of the Watches/Events Ribbon

Figure 16 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."

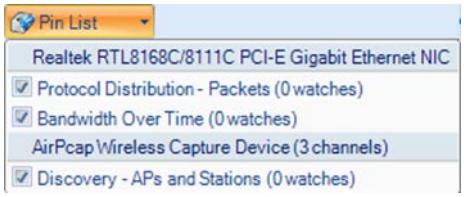
Add to Pin List

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

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



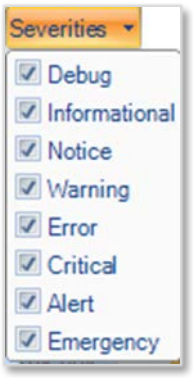
The *Pin List* itself shows the pinned views and their sources. The sources can be either live or a trace file. Views can be removed from the Pin List by clicking the corresponding check boxes.

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.

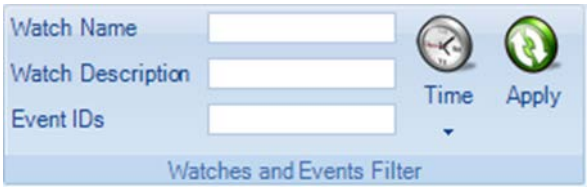
Severities List



Severities List

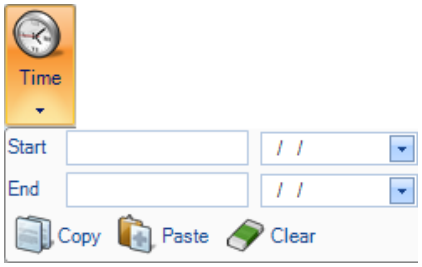
The Severities List contains the severities used by the severities filter. The selected severities are those with the checks. Severities can be selected or deselected using the check boxes.

Watches and Events Filter



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

Time Filter



Time Selection

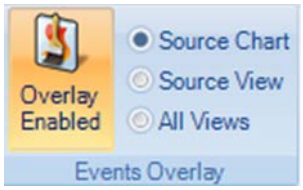
The Start and End times can be filled in manually, or the Paste operation can be used. Typically, the clipboard is carrying a time interval that was obtained using the copy operation in the Time Selection section of the Time Control Ribbon. Conversely, if the time interval is available, the Copy operation 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

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



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 17 shows the expanded Bandwidth Usage folder. Its first subfolder is called the *Bandwidth Usage Watches*.

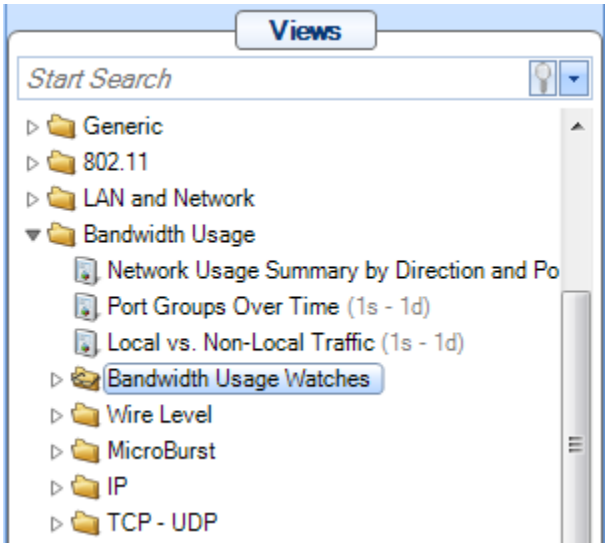


Figure 17 Predefined Watches

Opening the Bandwidth Usage Watches folder displays the following:

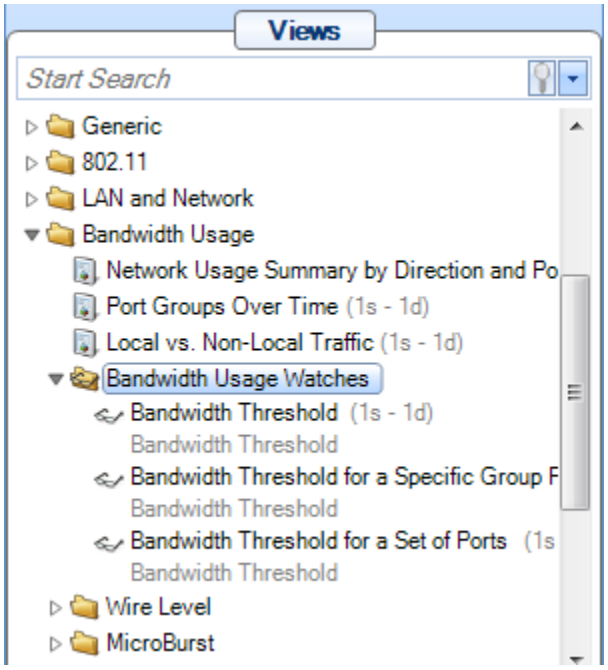


Figure 18 Expanded Bandwidth Usage Watches Folder

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 Port Group* (in Figure 18) 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.

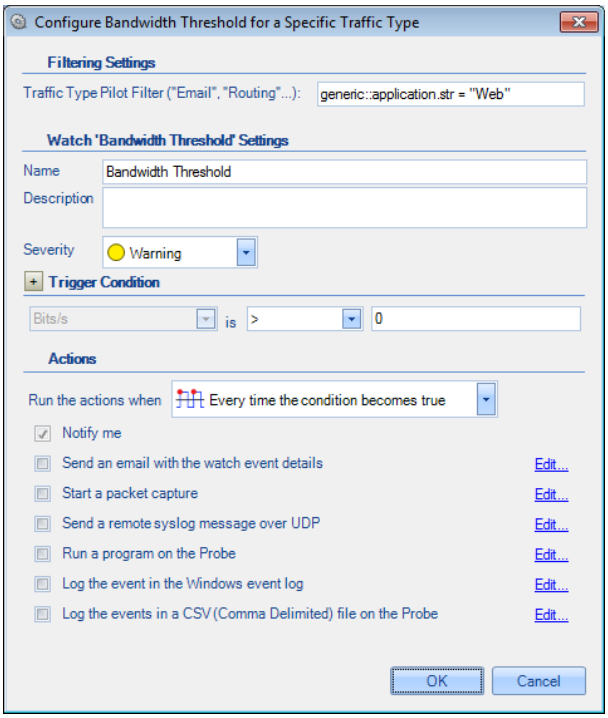


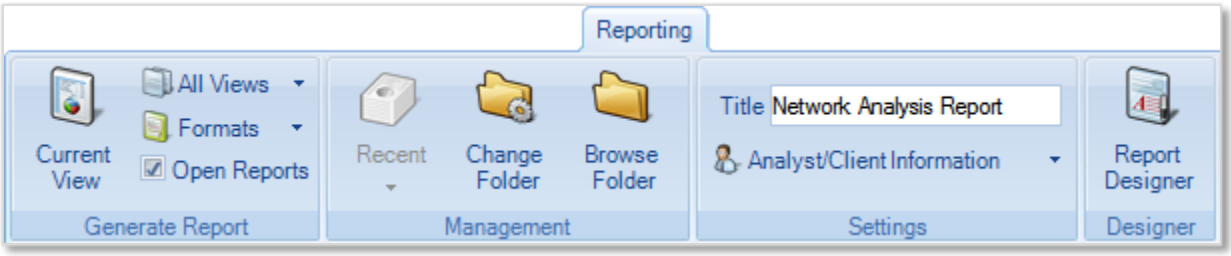
Figure 19 Watch Editor Panel with Filter Settings

Figure 19 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 port groups.

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



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.

Supported formats include:

- PDF Report
- Zip Package
- Excel Spreadsheet
- Word Document
- Text File
- HTML Page

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

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

Button

The *All Views* button gives you options for generating a report using more than one view. . 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*.

Clicking the *All Views* button directly generates a report using all views that are currently open in the main window.

Submenu

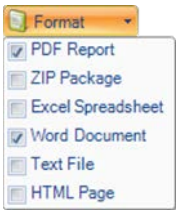
Clicking the drop-down arrow beside the *All Views* button gives you a choice of generating a report for all views or for views that are currently selected. You can select multiple views by clicking them in the Sources panel while holding down the Ctrl or Shift key.

Format

Button

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:



Submenu

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.

Excel Spreadsheet

The *Excel Spreadsheet* check box refers to a 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

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.

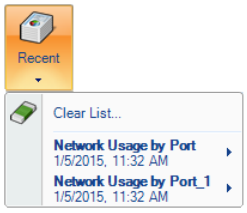
Management

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

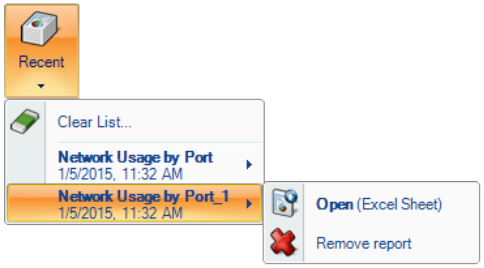
The *Recent* button opens a submenu to manage recently generated reports. By default, reports are generated, the Recent button is disabled.

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 Packet Analyzer personal edition.



Recent Reports

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



Recent Reports (Detail)

Change Folder

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

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

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

Button

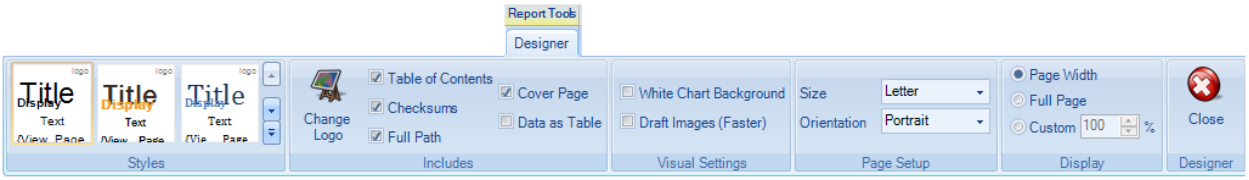
The *Analyst/Client Information* button presents a submenu that specifies what information appears on the cover page of a report. Each field is directly analogous to what appears on the cover page. Refer to the appendix on the example report for more information.

Submenu

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



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

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.

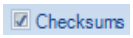
Change Logo

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

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

Checksums



The *Checksums* check box (checked by default) is used to specify whether SHA256 cryptographic digests is generated for trace files in subsequent reports. These digests are printed on the reports and placed in separate files when using the ZIP output format.

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

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

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 Packet Analyzer personal edition. 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)

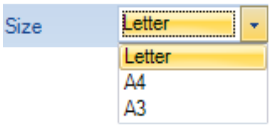
The *Draft Images (Faster)* check box (not checked by default) is used to specify the quality of the images in subsequent reports. Draft images are a suitable resolution for viewing on a computer while non-draft images are suitable for printing. Turning this feature on:

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

Page Setup

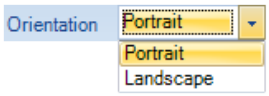
The *Page Setup* section controls the format of future generated reports.

Size



Use the *Size* drop-down menu to select the report size.

Orientation



Use the *Orientation* drop-down menu to select the report orientation.

Display

The *Display* section controls the magnification of the report template.

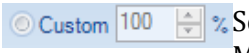
Page Width

Selecting *Page Width* changes the magnification level of the template so the width of a page matches all the space available in the tab.

Full Page

Selecting *Full Page* changes the magnification level of the template so that an entire page can be viewed.

Custom



Selecting *Custom* enables you to specify the magnification level of the template. Magnification can range from 25% to 400%. Enter a desired magnification level in the box (default is 100), or use the up or down arrow to increase or decrease the magnification by 25% each time an arrow is clicked.

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.

Sources Panel

The Sources Panel has two tabs: Devices and Files.

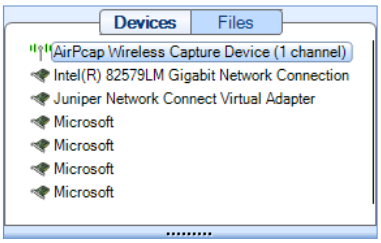


Figure 20 Sources Panel

The *Sources Panel* contains representations of live interfaces and trace files, and is one of the most important parts of Packet Analyzer personal edition.

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

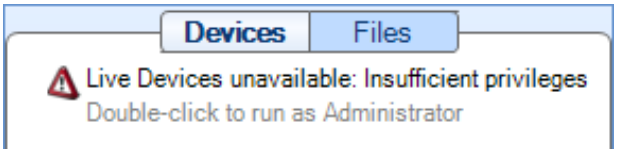
Devices
Shows local interfaces offering live sources of network traffic to Packet Analyzer personal edition.

Files
Shows local folders and trace files.

Devices

Devices on your local system require administrator privileges to capture network data.

If you are running Packet Analyzer personal edition in non-administrator mode, you will see the following prompt as Packet Analyzer personal edition initiates and tries to connect to your local resources.



If you have administrator privileges on the system, you can double-click on the prompt to make those resources available for capture jobs.

Packet Analyzer personal edition supports two basic classes of networking devices:

- Wired Ethernet
- Wireless (802.11)

Wired Ethernet Adapters

Wired Ethernet Adapter

Most wired Ethernet network interface cards work in Packet Analyzer personal edition.

Wireless Adapters

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, Packet Analyzer personal edition 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.

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

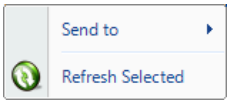
Devices Panel (No Selection)

With nothing selected, the options are as follows:

Refresh Sources

The *Refresh Sources* menu option causes Packet Analyzer personal edition to rescan the available interfaces on the local system. Additionally, the trace folders rescanned and updated to reflect whether files have been removed or modified.

With an Interface Selected



Devices Panel (Interface Selected)

With an interface selected, the options are as follows:

Send to

Wireshark

The *Wireshark* menu option instructs Packet Analyzer personal edition to start up Wireshark and send all traffic from the selected interface to Wireshark.

Wireshark with Filter

The *Wireshark with Filter* menu option instructs Packet Analyzer personal edition 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.

File

The *File* menu option instructs Packet Analyzer personal edition to send all traffic from the selected device to a user-specified trace file.

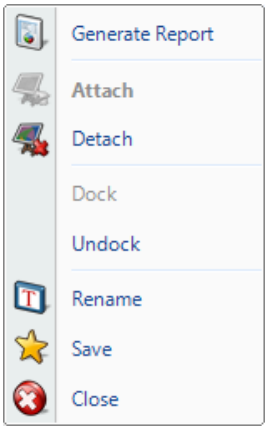
File with Filter

The *File with Filter* menu option instructs Packet Analyzer personal edition 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.

Refresh Selected

The *Refresh Selected* menu option causes Packet Analyzer personal edition to rescan the available interfaces on the local to display the currently available devices. Additionally, the trace folders associated with the Local System are rescanned and updated to reflect whether files have been removed or modified.

With a View Selected



View Selected, Local System

Generate Report

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

Attach

If the selected View is Detached, then the *Attach* menu item attaches Packet Analyzer personal edition to the View.

Detach

If the selected View is currently Attached, the *Detach* menu option detaches the selected View.

Dock

If the View has been undocked from the Main Window, the *Dock* menu option re-docks it.

Undock

If the View is docked to the Main Window, the *Undock* menu option undocks it and places it in a separate window. For more information on undockable Views, see Undockable Views on page 82.

Rename

The *Rename* menu option opens a dialog box that allows you to rename the View.

Save

The *Save* menu option saves the View as a Custom View.

Close

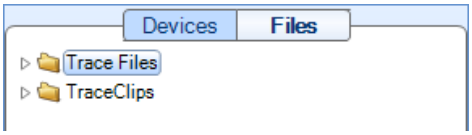
If the user is the creator of the selected View, then the *Close* menu option closes the selected View. This implies that the View will no longer be available to other users.

Files

Packet Analyzer personal edition 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.



Files Panel (closed)

Files Panel (expanded)

Trace File (PCAP)

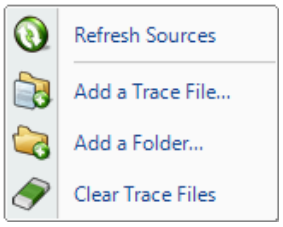
The figures show an example file panel with all the items closed and one with all of the items expanded.

[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

Context Menus in the Files Panel

The context menus for the Files Panel are described below:

With Nothing or Local System Selected



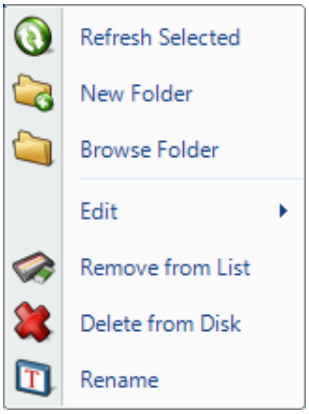
Files Panel (No Selection)

The options are as follows:

Refresh Sources

The *Refresh Sources* menu option causes Packet Analyzer personal edition to rescan the available interfaces on the local system. Additionally, the trace folders are rescanned and updated to reflect whether files have been removed or modified.

With a Trace Folder Selected



Files Panel (Trace Folder Selected)

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.

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.

Browse Folder

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

Edit

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.

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.

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.

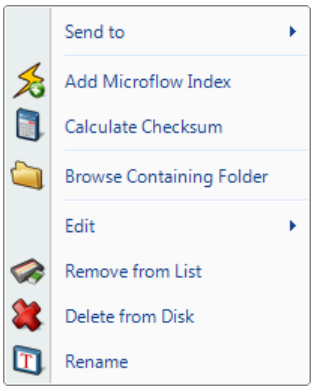
Delete From Disk

The *Delete Trace Files* menu option irrevocably deletes from the local system disk all trace files from the selected folder that do not have a view open on them.

Rename

The *Rename* menu option opens a dialog box that allows you to rename the View.

With a Trace File Selected



Files Panel (Trace File Selected)

Send to

Wireshark

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

Wireshark with Filter

The *Send to Wireshark with Filter* menu option instructs Packet Analyzer personal edition 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.

File

The *File* menu option instructs Packet Analyzer personal edition to send all traffic from the selected trace file to a user-specified trace file.

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.

Add Microflow Index

The *Add Microflow Index* option adds microflow index information to the selected file or trace. For more information, please refer to the Indexing chapter, page 75.

Calculate Checksum

The *Calculate Checksum* menu option calculates the SHA256 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.

Browse Containing Folder

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

Edit

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.

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 copies a previously Cut or Copied file to the selected “paste” location.

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.

Delete from Disk

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

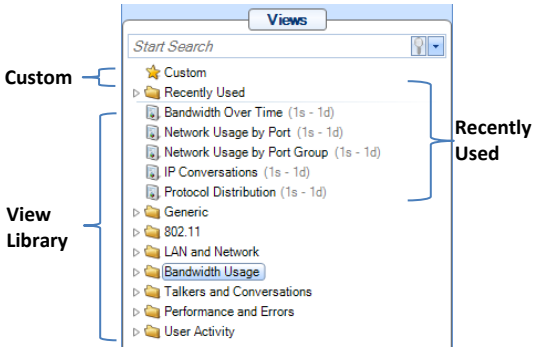
Rename

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

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 Library

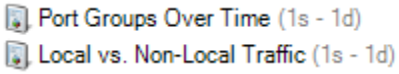


Figure 21 Instance of a View

A Packet Analyzer personal edition 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])

Figure 21 shows two example views.

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

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 22: Apply Icon

- Figure 22 means the view metric can be applied to the source

Figure 23:Do Not Apply Icon

- Figure 23 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 24: Apply Icon

- Figure 24 means the view metric can be applied with filter to the source

Figure 25:Do Not Apply Icon

- Figure 25 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 Packet Analyzer personal edition.

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

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.

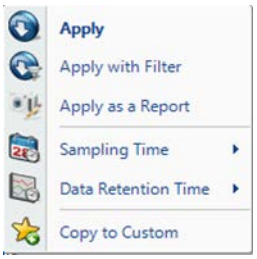
Apply as a Report

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.

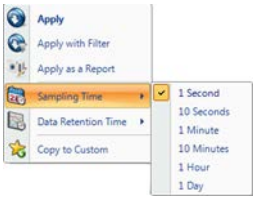
Copy to Custom

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

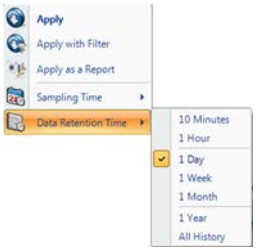
View



View Library View



Sampling Time



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

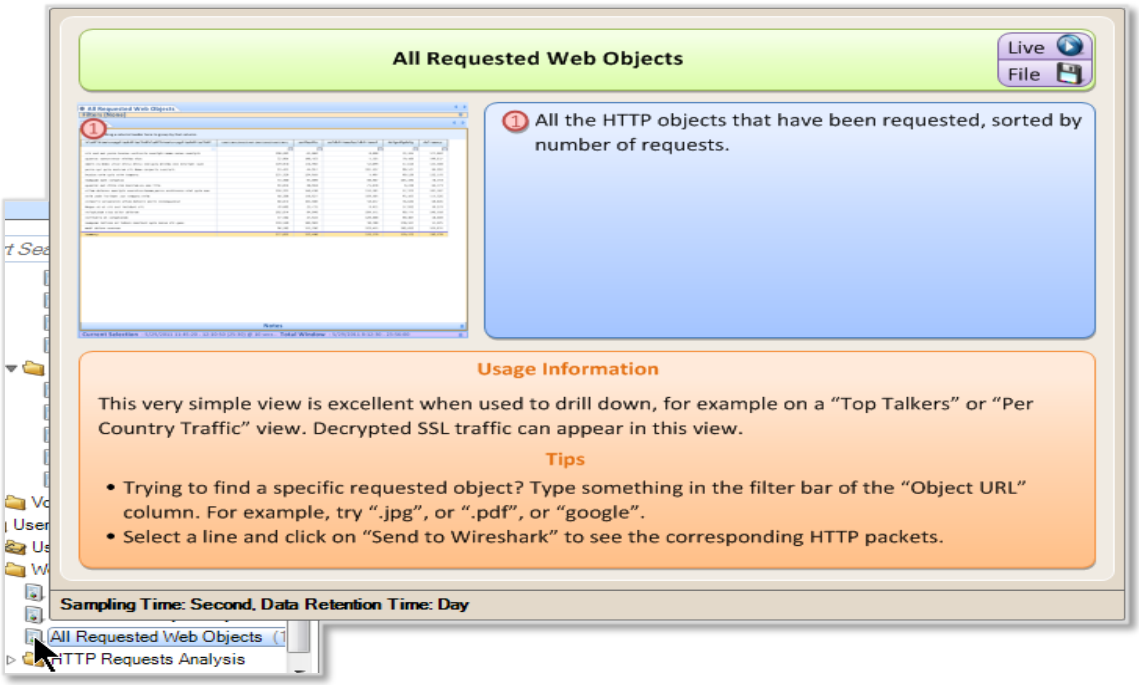
The *Data Retention Time* value specifies the time period for the View metric history that is retained for a View applied to a live source. Once the Data Retention Time is reached, the oldest metrics are discarded as new sample points are calculated. The Data Retention time has no effect on the duration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

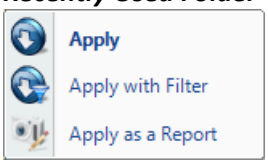
The Recently Used folder contains the five most recently used views. The Recently Used folder is not shown when the folder is empty, as is the case when Packet Analyzer personal edition is started.

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



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

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.

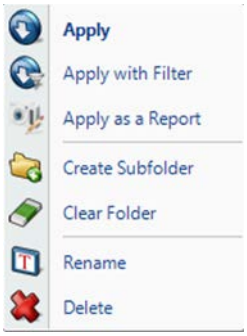
Create Subfolder

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



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.

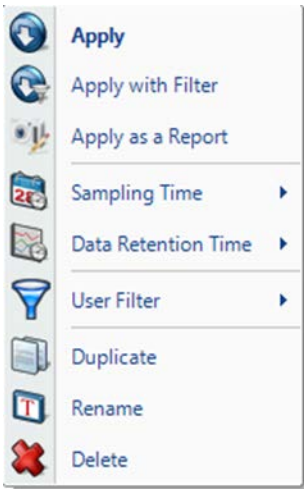
Rename

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)



Custom View

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

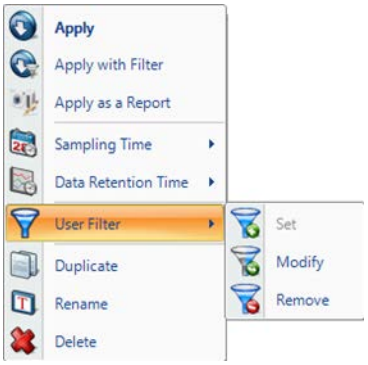
The *Apply as a Report* menu option automatically creates a report with the "Current View" option as the selected view for the file selected in the Files panel. The *Apply as a Report* menu option cannot be applied to a device.

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

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.

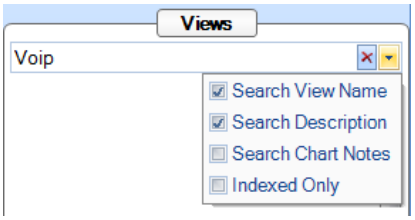
Rename

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



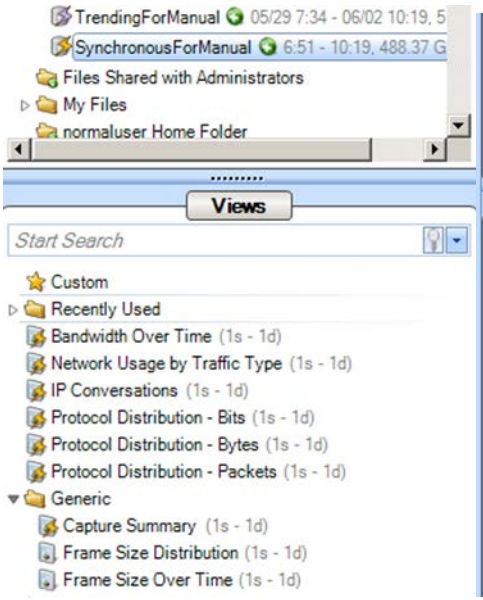
View Panel Search

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.

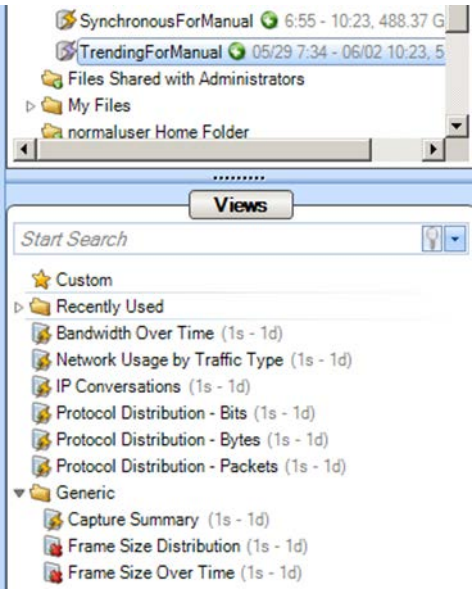
The Search box is a convenient way to find the View that you are looking for. In a sense, it provides an alternative ways of organizing the View Library.

Regular Views, Fast Views, and Forbidden Views

When some Views are applied to Sources that have associated Microflow 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 Microflow Indexing data alone. The ordinary views are those that cannot be run with the Microflow Indexing data alone, but the actual packets are available for the View calculation.



Fast Views



Disallowed Views

Microflow Indexing

Indexing a Trace File

Indexing a trace file can improve the performance of several views by a factor of 100x to 1000x. Creating a Microflow 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.

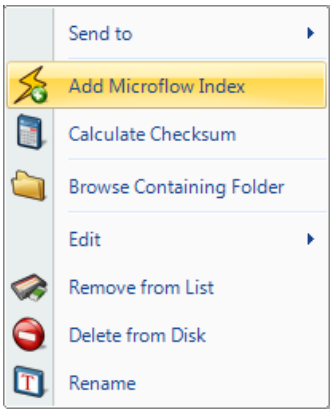
Microflow Indexes can be applied to all types of trace files except Wi-Fi capture files. When an index is successfully created, the indexed file shows a small yellow lightning icon on it. If, for any reason, the index is not completely loaded, a red lighting arrow appears on the top of the trace file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

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

Context Menu

Add Microflow Index



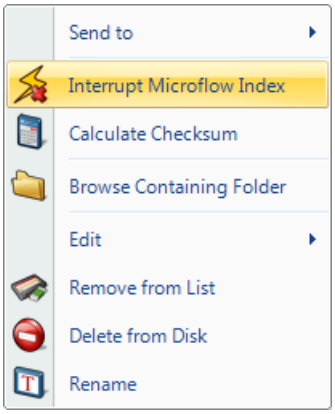
Add Trace Index context menu

Add Microflow Index

The context menu for a Trace File without index shows:

Add Microflow Index
The *Add Microflow Index* menu option creates a Microflow Index on the selected file.

Interrupt Microflow Index



Interrupt Trace Index context menu

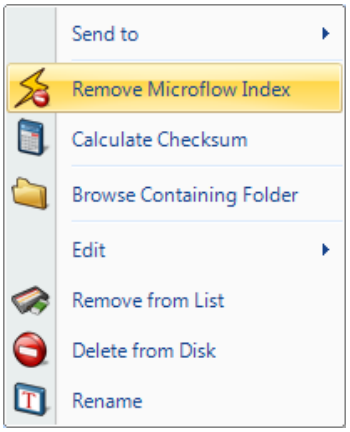
The context menu while the index on a Trace File is created shows:

Interrupt Indexing

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

Interrupt Indexing

Remove Microflow Index



Remove an Index context menu

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

Remove Microflow Index

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

Remove Microflow Index

Index Icons on Trace Files

Index Applied

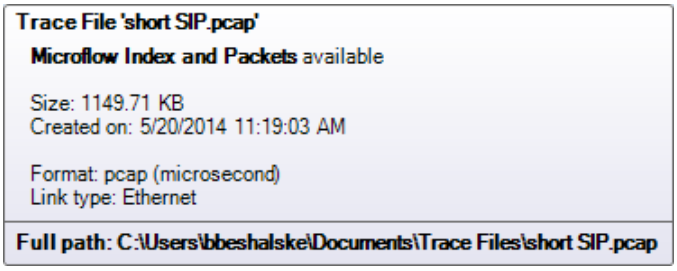
Index Applied means that the index has been applied successfully and thus many views will be accelerated.

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



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:

Trace File
The name of the file.

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

Size
The size of the trace file in kilobytes.

Created On
The date the trace file was created.

Format
The type of trace file.

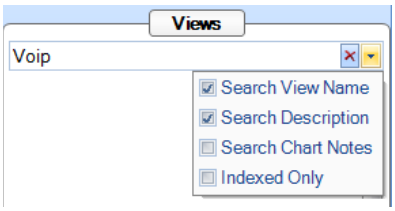
Link Type
The link type of the trace file. This is important because not all views can be applied on all files. In particular, if the Link type is PPI, then the index cannot be created.

Full path
The location of the file.

Drag and Drop Cursors for Indexed Trace Files

When dragging and dropping a view that supports indexed files, the *Drag and Drop cursor* includes a yellow lightning bolt when dragged over an indexed file to indicate that the index will be used

Search Text Box

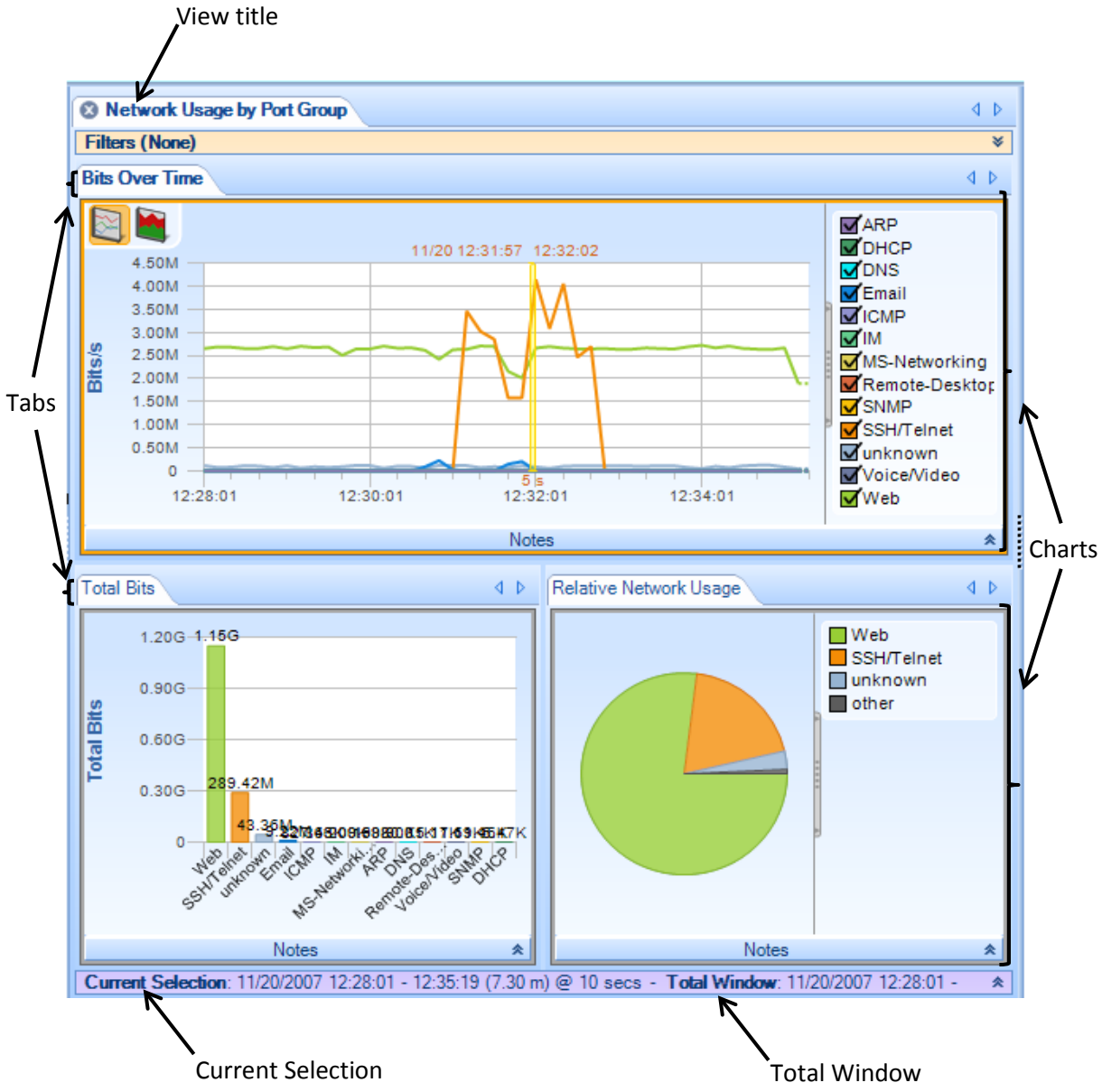


View Panel Search

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.



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

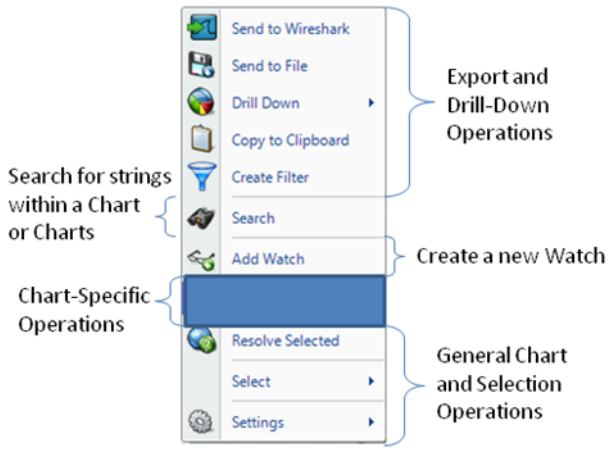


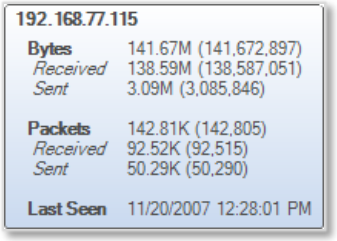
Chart Context Menu Overview

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:

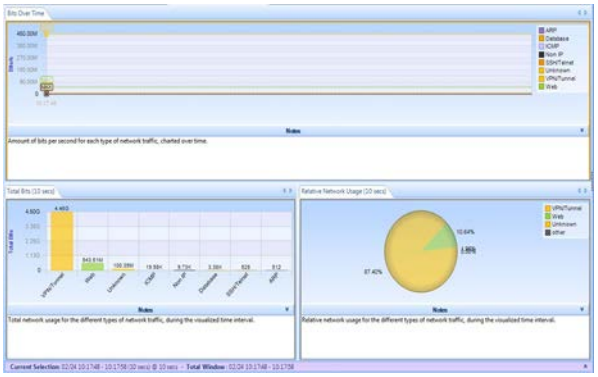
- Export and Drill Down Operations
- Search over Charts
- Add Watch (only for Strip Charts and Bar Charts)
- Chart-Specific Operations
- General Chart and Selection Operations

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. Here is an example of a tooltip from a Conversation Ring view. This tooltip provides more details on a selected endpoint in the chart.



Notes



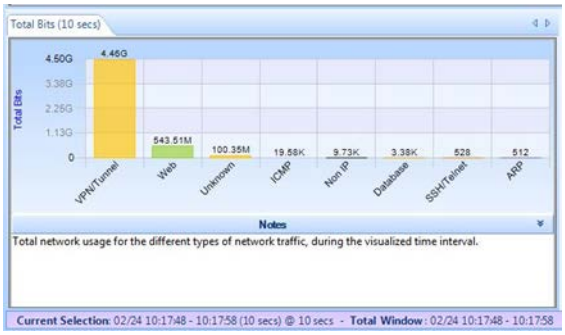
Every chart has a section that can be used to place notes that are included in a generated report and if applicable, saved in a custom view.

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

View With Collapsed Notes

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

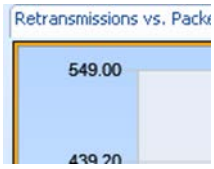
View Notes Toggle Button



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.

View With Expanded Notes

Selection



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.

Chart Selected

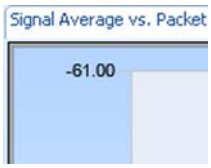
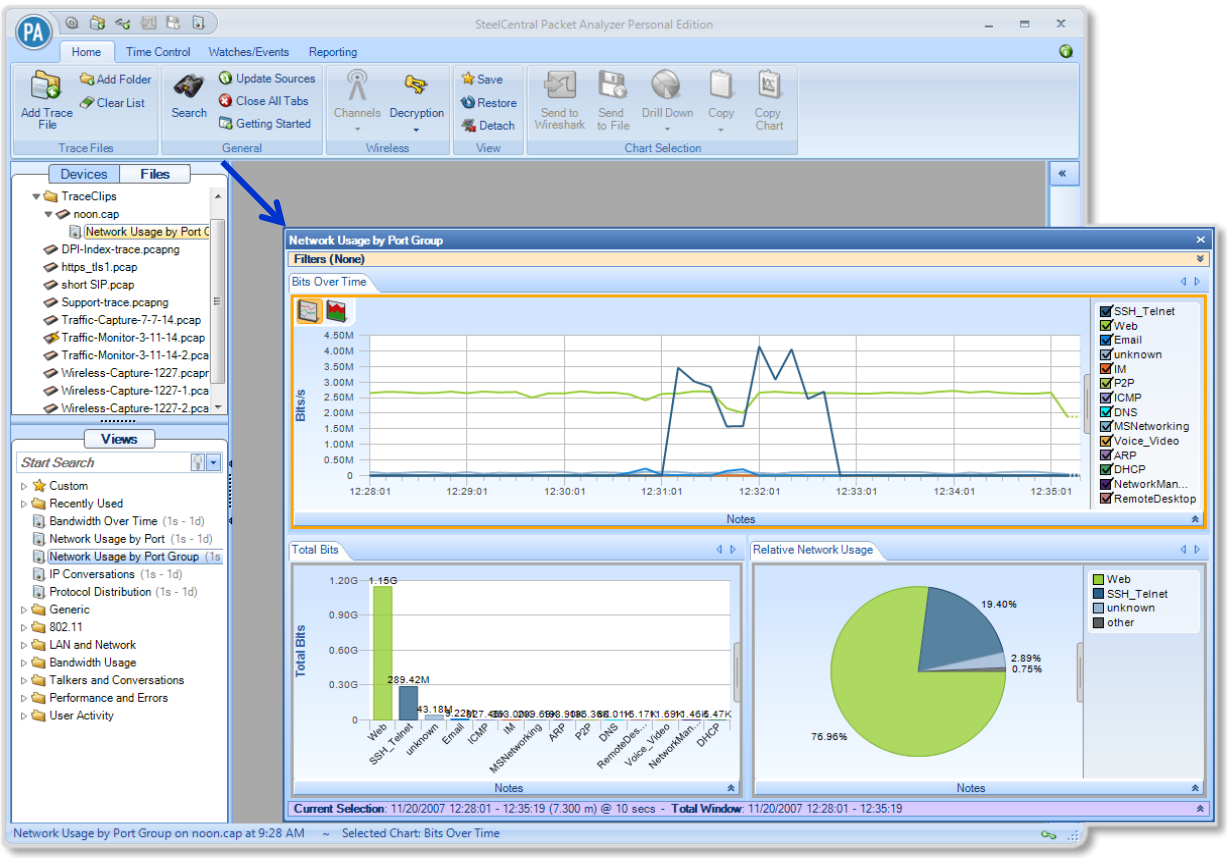


Chart Not Selected

Undocking Views

By default, a view is docked in the main window. You can undock a view so that it occupies a separate floating window. As with other windows, you can resize the window by dragging on the borders, and you can relocate it anywhere on the screen, even on a different monitor.

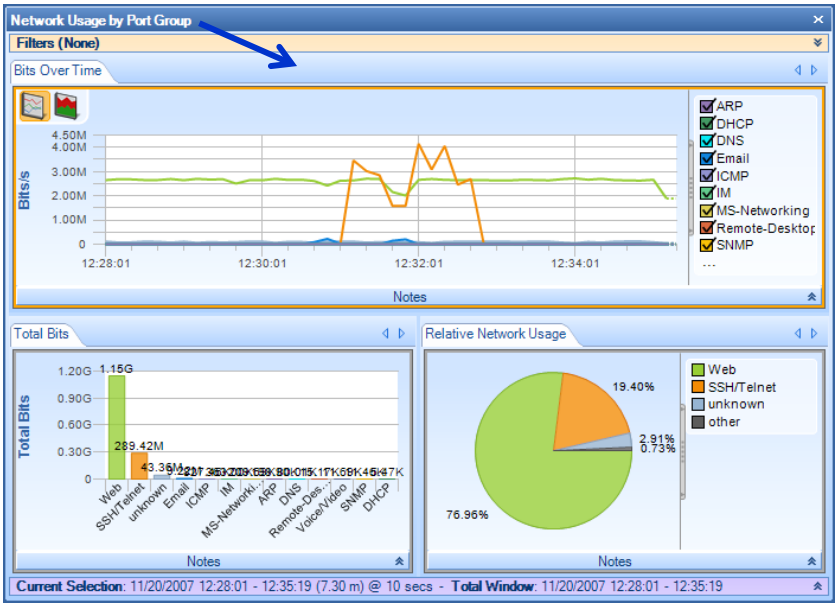


Typical undocked view

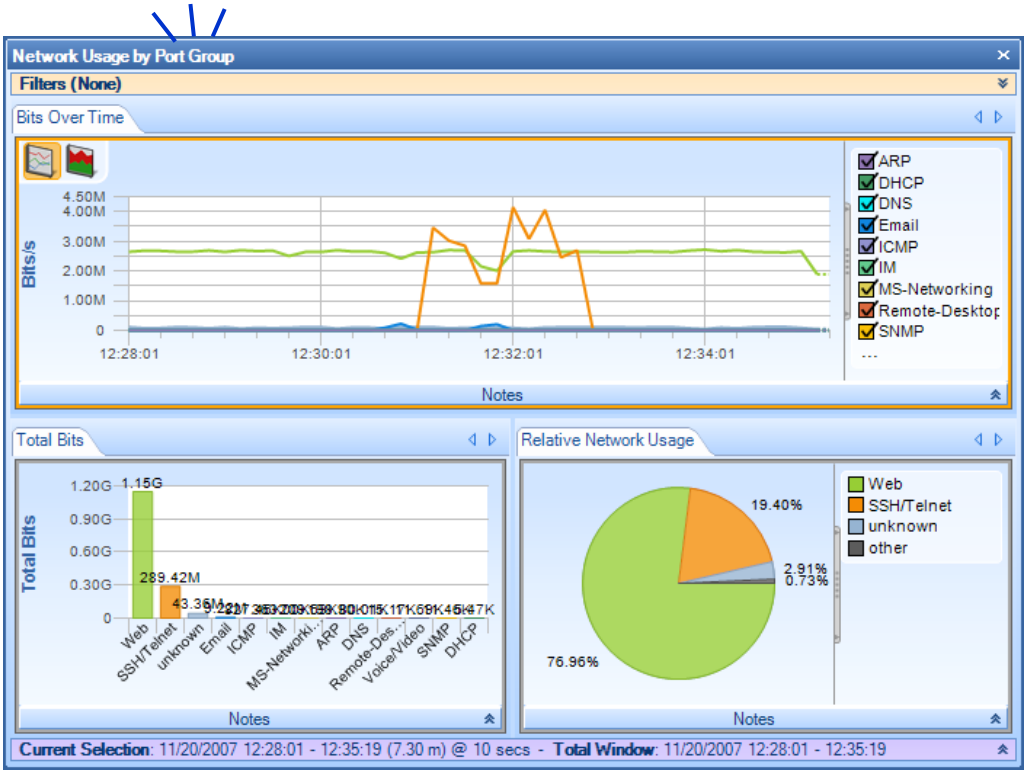
Undocking a View

There are three ways to undock a view:

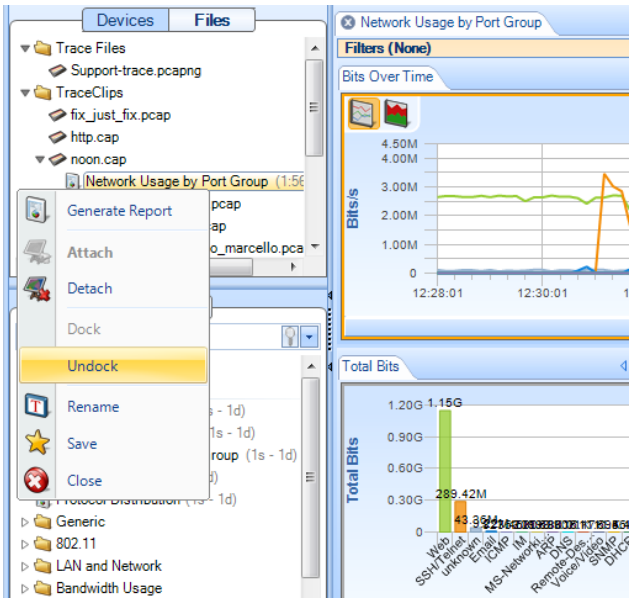
- Drag the view's tab.



Double-click the view's tab



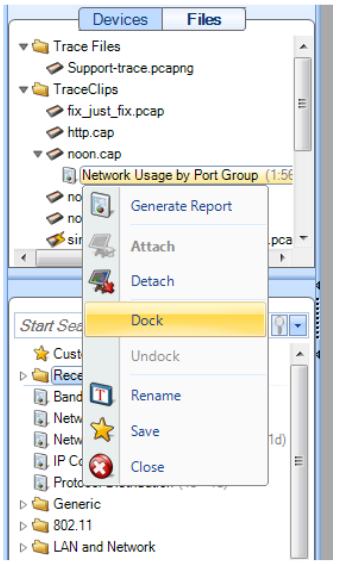
- Right-click the applied view in the Devices/Files panel and select **Undock** from the context menu.



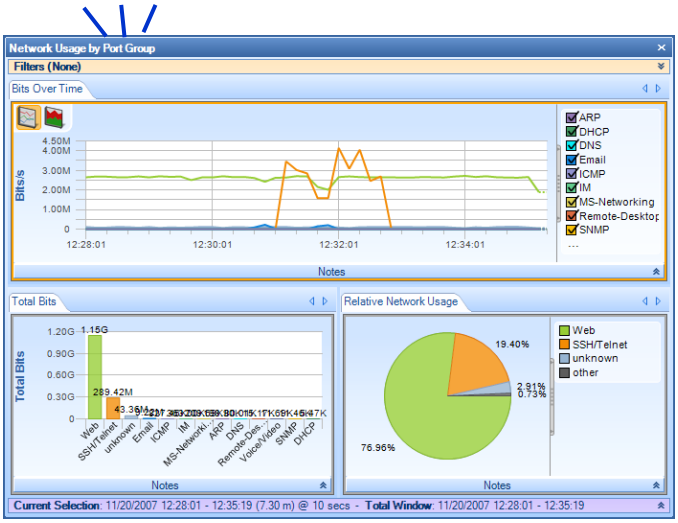
Docking a View

There are three ways to dock an undocked view:

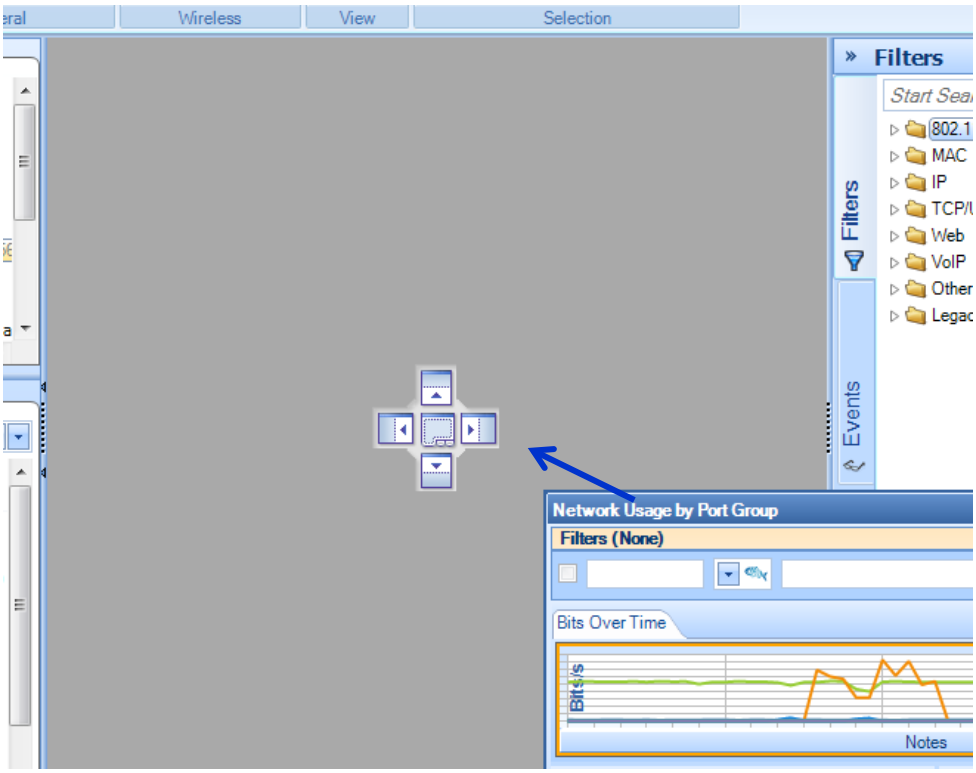
- Right-click the applied view in the Devices/Files panel and select **Dock** from the context menu.



- Double-click the main bar of the floating window.



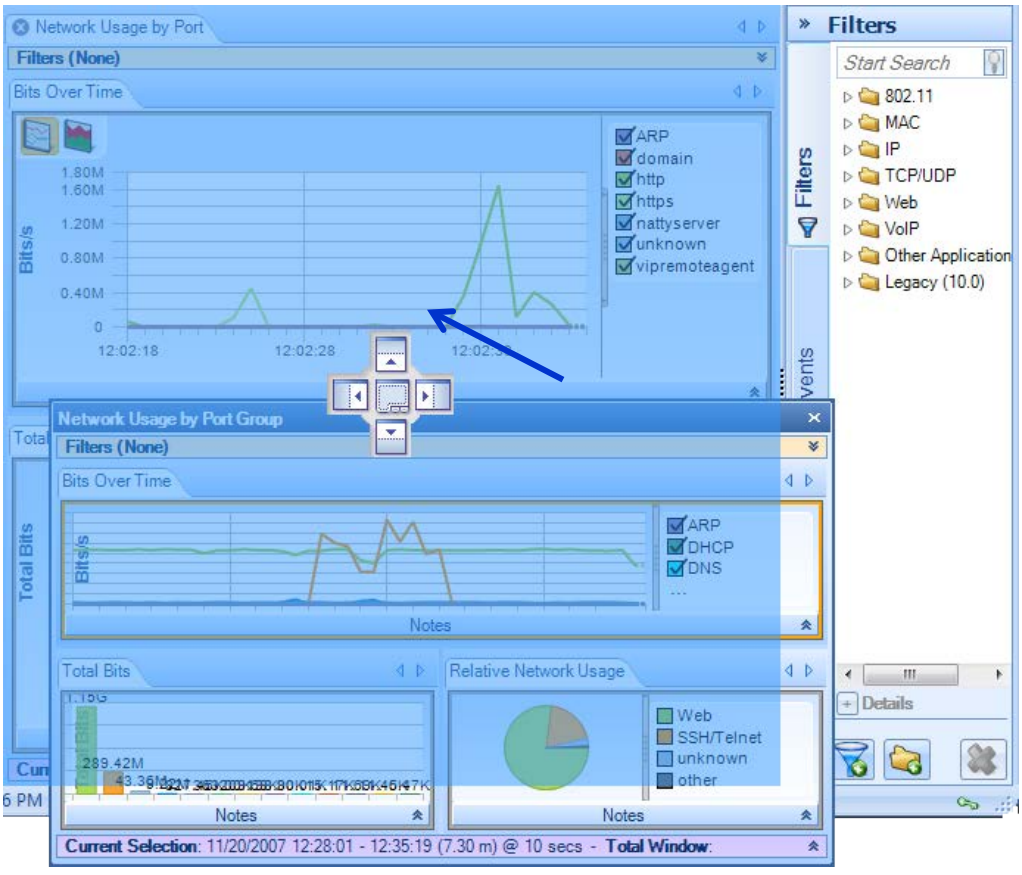
- Drag the floating window onto the Packet Analyzer personal edition main window. When the mouse cursor hovers over the docking control, the main window turns blue and you can drop the floating window onto it.



If the main window is empty, the floating window will dock and fill the entire main window. If another view occupies the main window, the result depends on interaction between the mouse cursor and the docking control.

Docking control

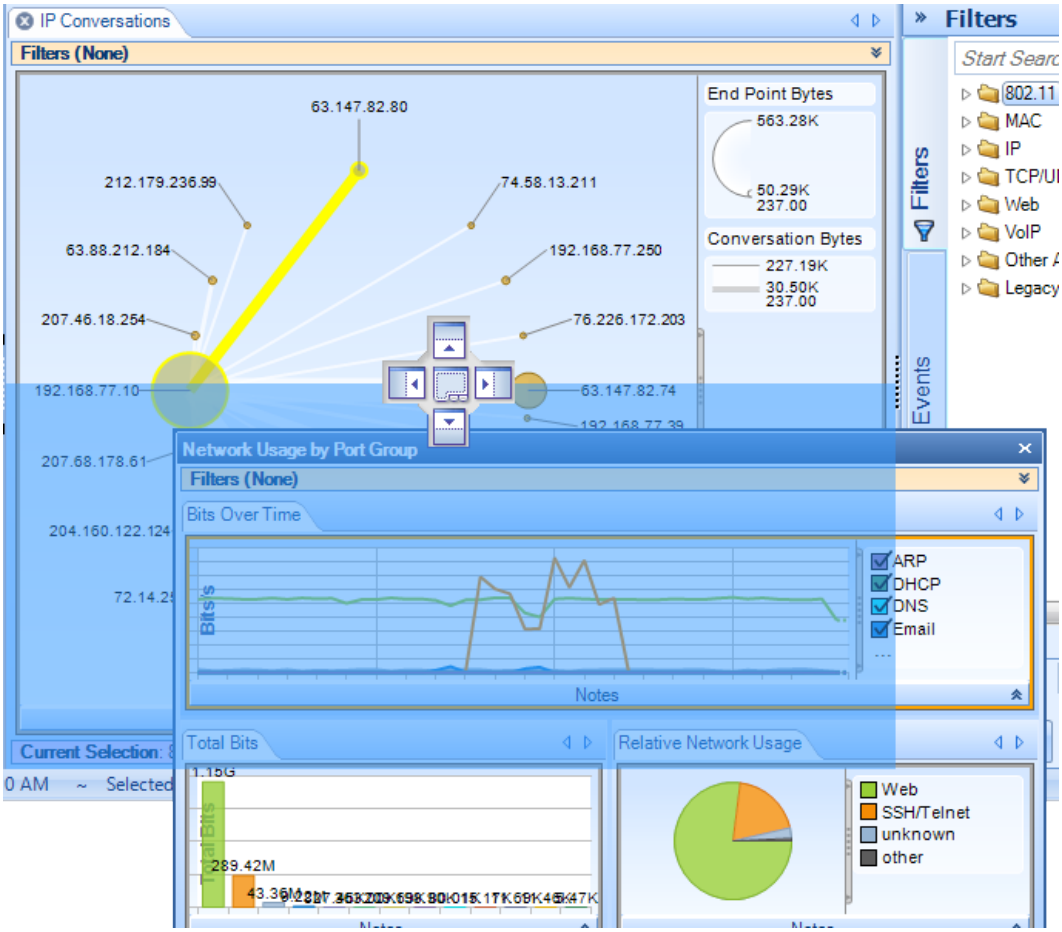
If the mouse cursor hovers over the center icon of the docking control, the entire main window turns blue. When you click the mouse, the floating window drops into the main window and replaces the view that was there. (The previous view is still available. Click its tab to bring it to the front of the main window.)



Docking into the entire main window

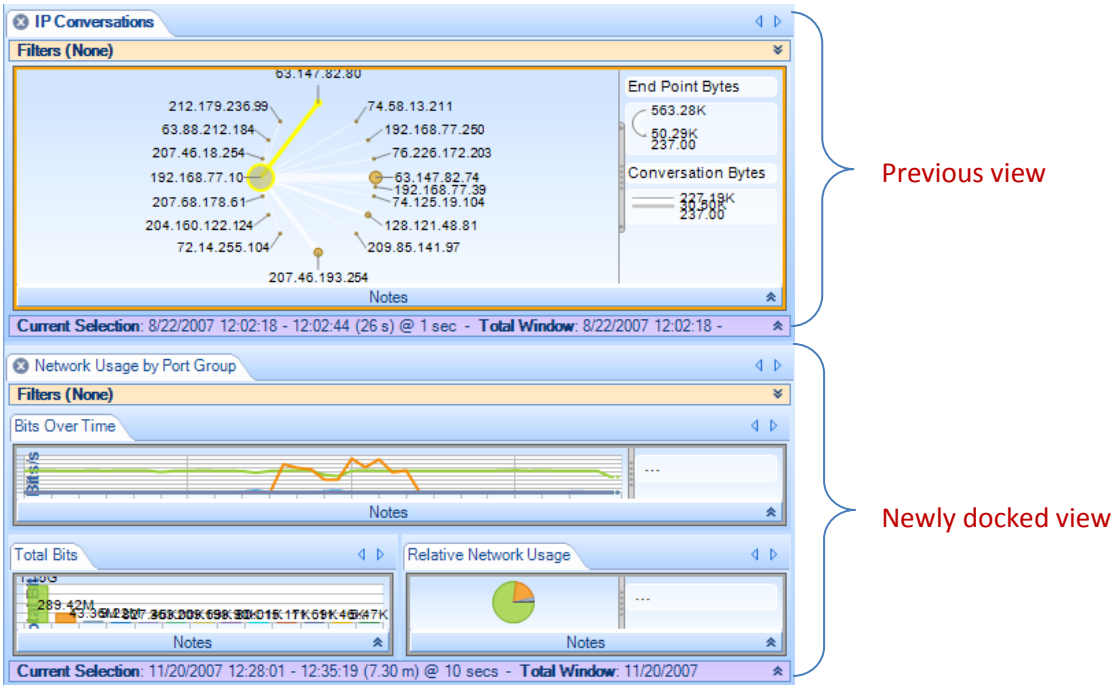
If the mouse cursor hovers over one of the outside icons of the docking control, a portion of the main window turns blue. When you click the mouse, the floating window drops into that portion of the main window and shares the main window with the view that was there.

For example, in the illustration below, the mouse cursor is hovering over the bottom icon of the docking control, and the bottom half of the main window is shaded blue.



Docking into a portion of the main window

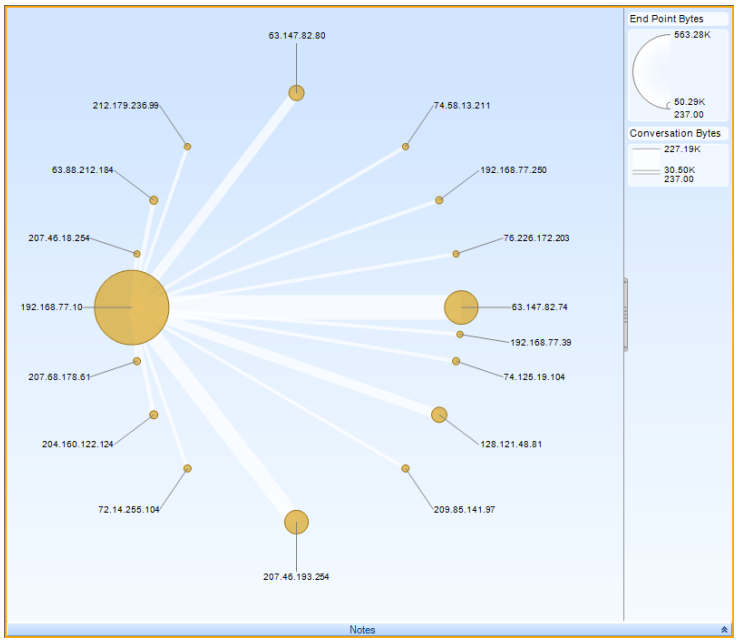
When the mouse cursor is clicked, the floating window drops into the bottom half of the main window.



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



Conversation Ring

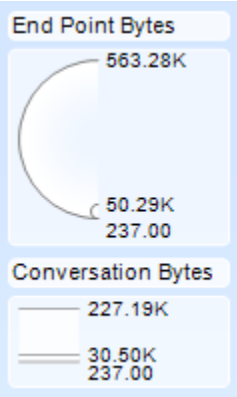
Along with the "Sampling Time" and "Data Retention Time" options previously described, the Conversation Ring is customizable in the following ways:

- Show endpoint labels
- Endpoint color
- Name resolution
- Choose metric to display
- Toggle legend visibility

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

- Scroll Wheel
- Hover
- Selection

Size Legends



Size Legends in a Conversation Ring

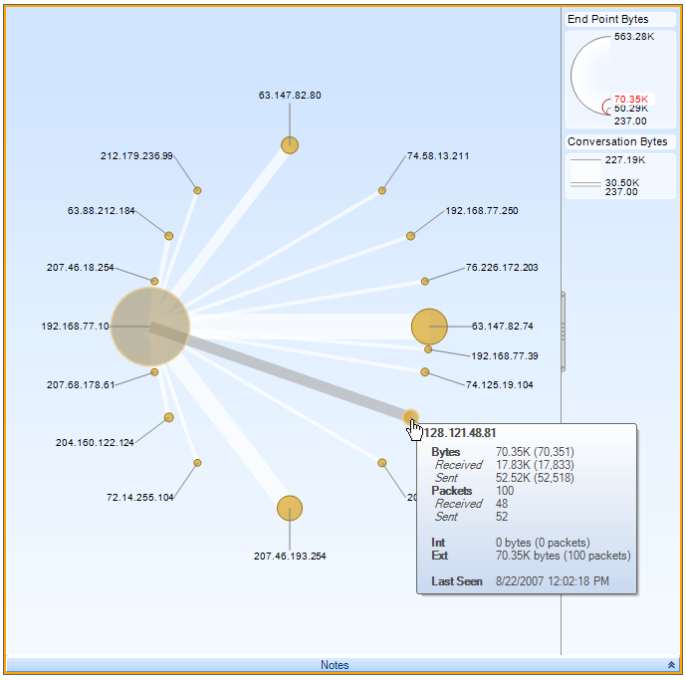
In the upper right corner of the view are two size legends that depict the maximum, average and the minimum traffic in all displayed endnotes and conversations. An example is shown in the figure on the left.

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.

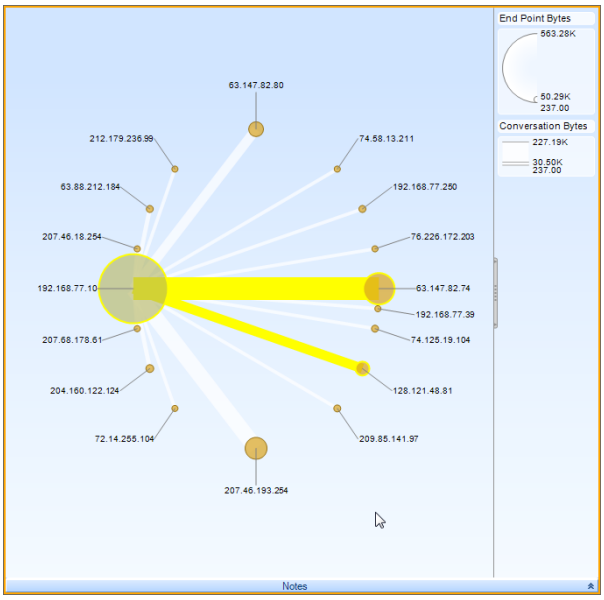
Hover with Tooltip

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.



Conversation Ring Hover

Selected



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.

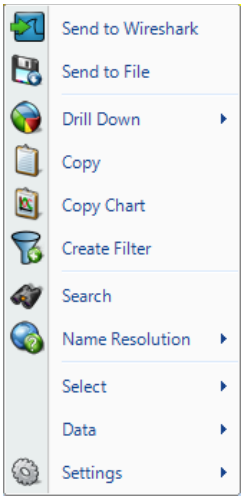
Clicking with Control key pressed is supported for multiple endpoint or connection based selections (which can be mixed).

Top Conversations

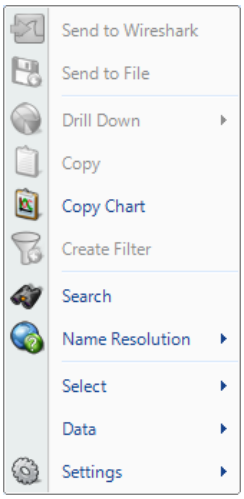
Conversation Ring Top Conversations

When there is not enough space to display all of the conversations clearly in a single ring, Packet Analyzer personal edition 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. Endpoint labels can always be shown using the Settings item in the context menu.

Context Menu



Conversation Ring (Selection)



Conversation Ring (No Selection)

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.

Copy

The *Copy* 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.

Copy Chart

The Copy Chart menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

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.

Name Resolution

The Name Resolution menu option tries to identify unresolved IP addresses, ports, or MAC addresses from all or the selected endpoints and/or conversations. Default is from Settings menu.
Enabled
Turns on auto resolution of current and new addresses.
Resolve Selected
Resolve only selected addresses.
Clear Selected and *Clear All*
Resolved names not displayed.

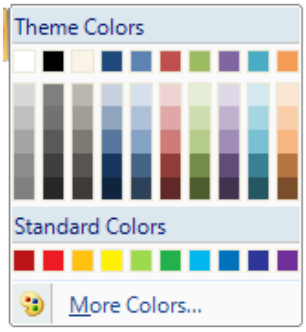
The Conversation Ring has the following contextual submenus:

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).

Data Conversation Ring Sub-Menu

The Data submenu sets what data are displayed from the available metrics.



Endpoint Color

The *Settings* submenu option opens up a submenu with three items:

Show Legend
Toggles Legend display
Always Show Labels
Forces all endpoint labels to be shown.
Endpoint Color
Color choices to change the color of the endpoints for the chart.

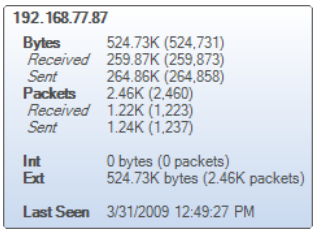
Tooltips

The conversation ring has two kinds of tooltips:

- Connection Based
- Endpoint Based

Tooltips provide information on the metrics used in the conversation ring chart. In the examples given below, the chart metrics are Bytes and Packets. Your tooltips may differ as they will reflect the metrics you used in your conversation ring chart.

Endpoint



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.

Bytes

The *Bytes* value refers to the total number of bytes that have been either sent from or received at that endpoint, i.e. the sum of Received and Sent bytes.

Received

The *Received* value 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.

Sent

The *Sent* value 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.

Packets

The *Packets* value refers to the total number of packets that have been either sent from or received at that endpoint, i.e. the sum of Received and Sent packets

Received

The *Received* value 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.

Sent

The *Sent* value 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.

Int

Int refers to bytes and packets that are sent from the host to itself (i.e. the IP source is the same as the destination).

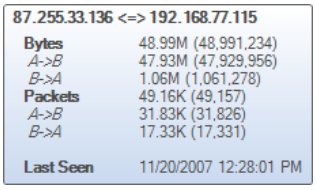
Ext

Ext refers to bytes and packets that are sent to or received from other hosts.

Last Seen

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

Conversation



Conversation Ring Conversation

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

Address(A)

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

Address(B)

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

Bytes

The *Bytes* value refers to the total number of bytes sent between the source and destination addresses over the given sample period and is the sum of *A->B* and *B->A*.

A->B

The *A->B* value refers to the total number of bytes sent from the source address to the destination address over the view's sample period.

B->A

The *B->A* value refers to the total number of bytes sent from the destination address to the source address over the view's sample period.

Packets

The *Packets* value refers to the total number of packets sent between the source and destination addresses over the given sample period and is the sum of *A->B* and *B->A*.

A->B

The *A->B* value refers to the total number of packets sent from the source address to the destination address over the view's sample period.

B->A

The *B-A>* value refers to the total number of packets sent from the destination address to the source address 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.

Strip Chart

The Strip Chart displays quantitative data with respect to time.

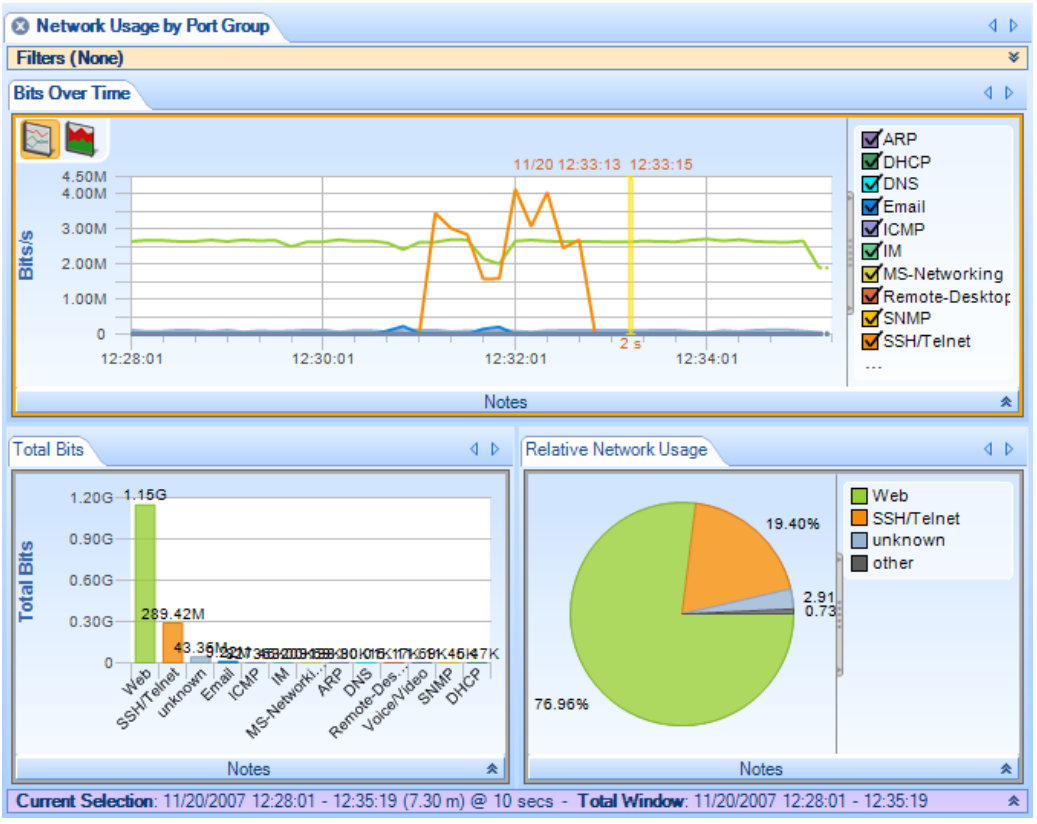
Diagram

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:



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 above shows three 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.

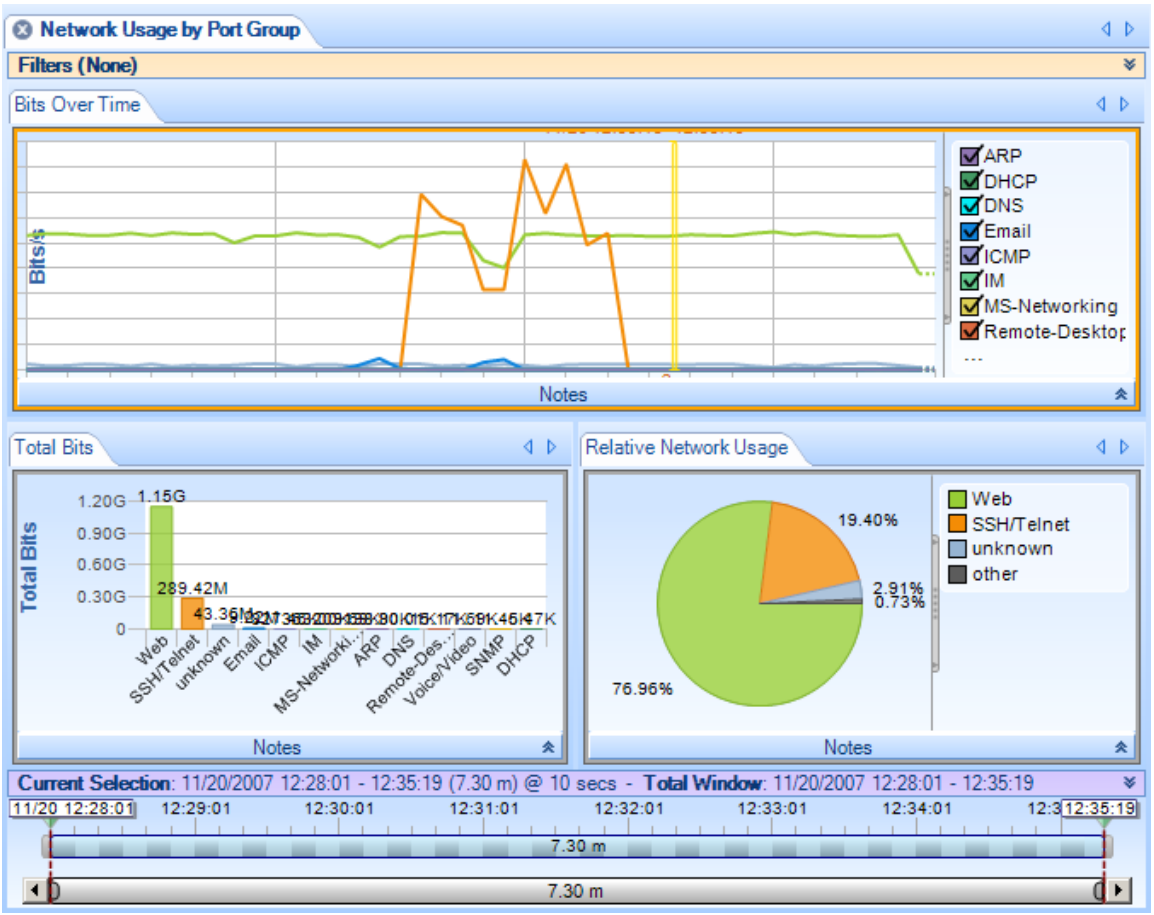


Figure 26 Strip Chart with Horizontal Zoom

Figure 26 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).

The Selection Bar (upper bar) controls the portion of the data (trace file or live capture) that is displayed in the charts. Move the triangular markers above the ends of the Selection Bar to trim the time interval that is displayed.

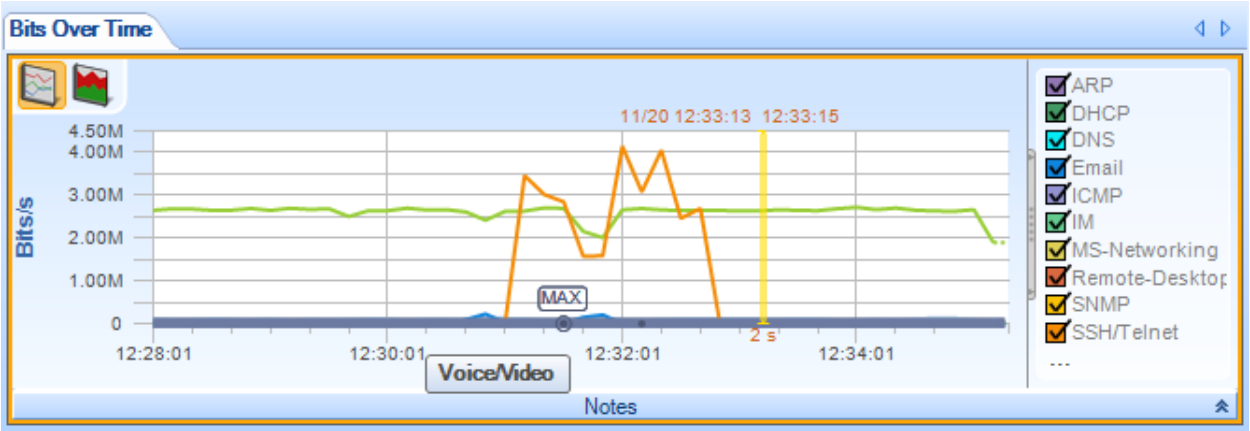
The Time Scroll Bar (lower bar) controls the resolution of the upper bar. As you bring the ends of the bar in toward the center, the time scale in the upper bar expands, allowing you to make finer selections of time intervals using the upper bar.

Along with the “Sampling Time” and “Data Retention Time” options as previously described (on page 68), the Strip Chart can be customized by:

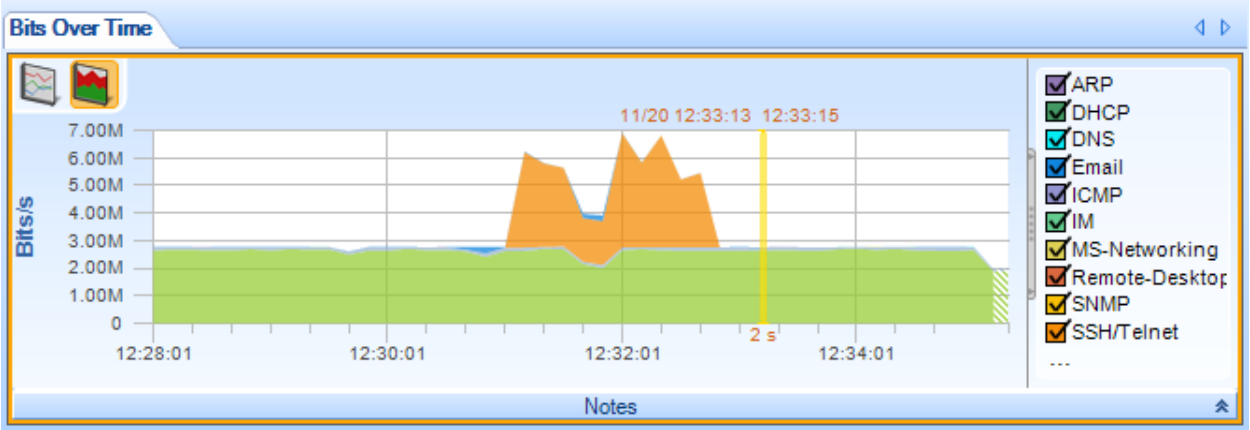
- Toggling display mode (line chart or stacked area chart)
- Selecting data sources to be displayed
- Changing the stacking order (stacked area mode only)
- Toggling legend visibility
- Displaying Min and Max values
- Rescaling Y Axis

Display Modes

There are two display modes for strip charts: normal (line) mode and stacked area mode. Normal mode is the default.



Normal strip chart



Stacked area strip chart

In the normal (line) chart, each data point's value at a given time is plotted relative to zero. In the stacked area chart, each data point's value at a given time is plotted relative to the value of the data in the layer below.

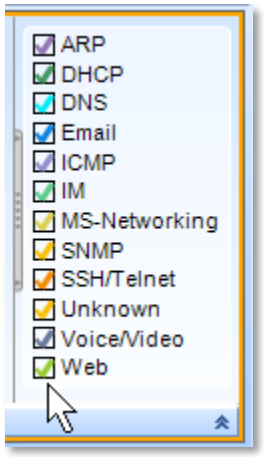
To switch from one mode to the other, click one of the display mode buttons in the upper left corner of the strip chart:

Alternatively, you can choose the display mode from the context menu (described below).

To display a strip chart in stacked area mode by default, set the view to stacked area mode and save it as a custom view. (Click the Save button in the View section of the Home tab.) When you drag the custom view onto your data of interest, the strip chart displays in stacked area mode.

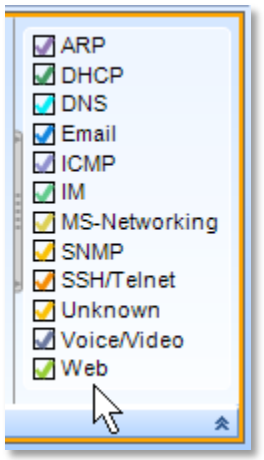
Data Display

You can show or hide lines or areas of data by checking or unchecking the boxes in the legend area to the right of the data area.



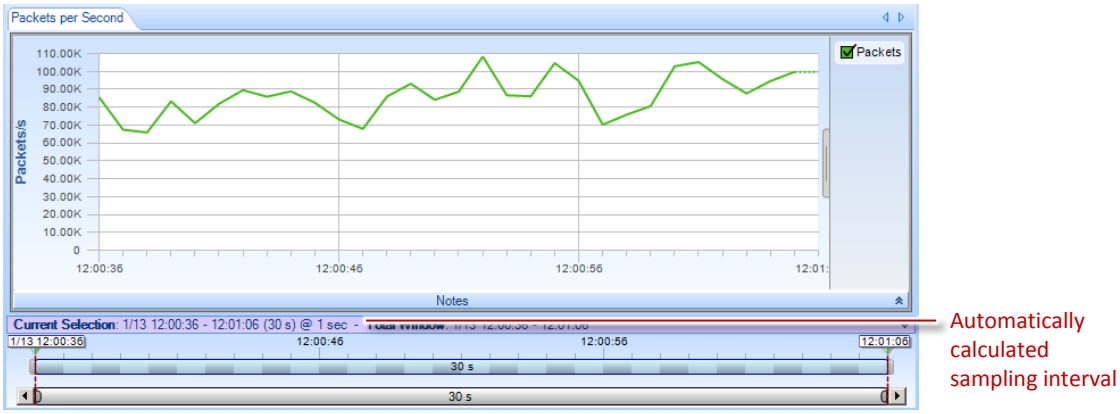
Stacking Order

You can change the stacking order of areas in a stacked area chart by dragging the labels up or down in the legend area to the right of the data area.

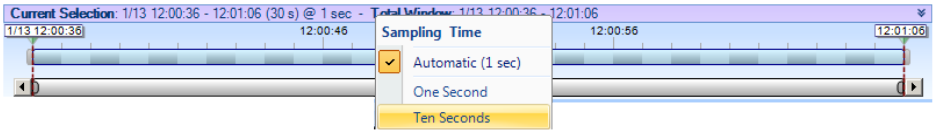


Custom sampling interval

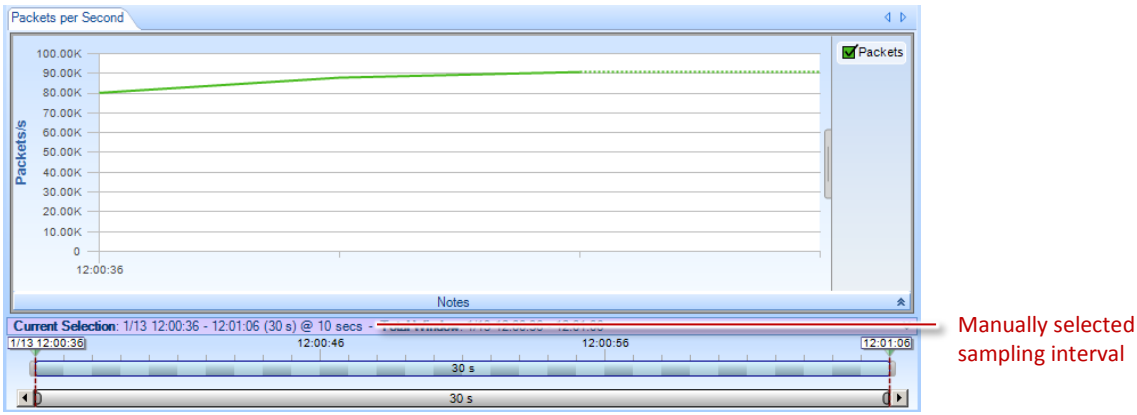
By default, the sampling interval for a strip chart is calculated automatically by Packet Analyzer personal edition.



A context menu in the time control bar shows the current sampling interval and allows you to select a different one. The allowed sampling intervals are calculated based on display considerations.



The strip chart is recalculated using the new sampling interval.



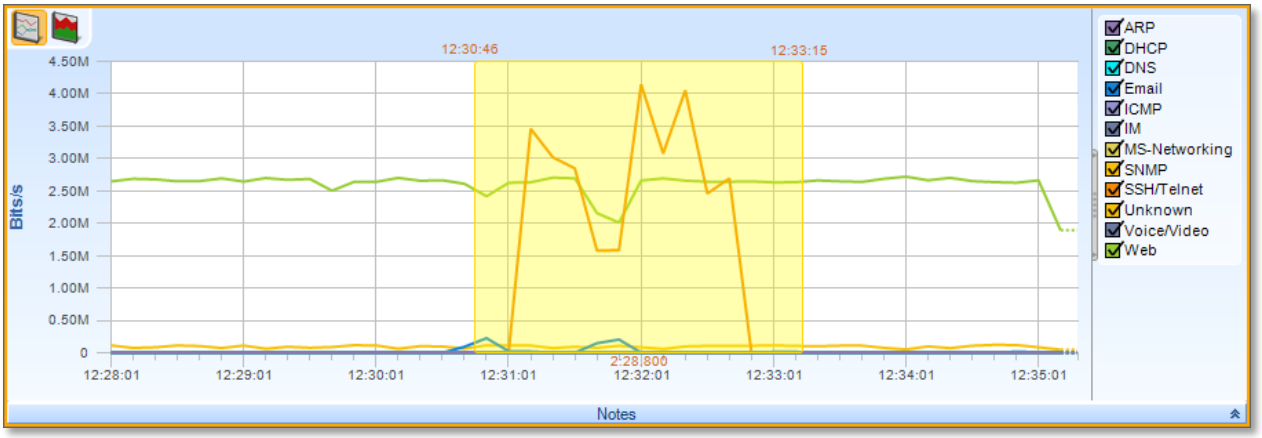
Selection

The Strip Chart supports two types of selection:

- Time-based
- Line- or area-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:

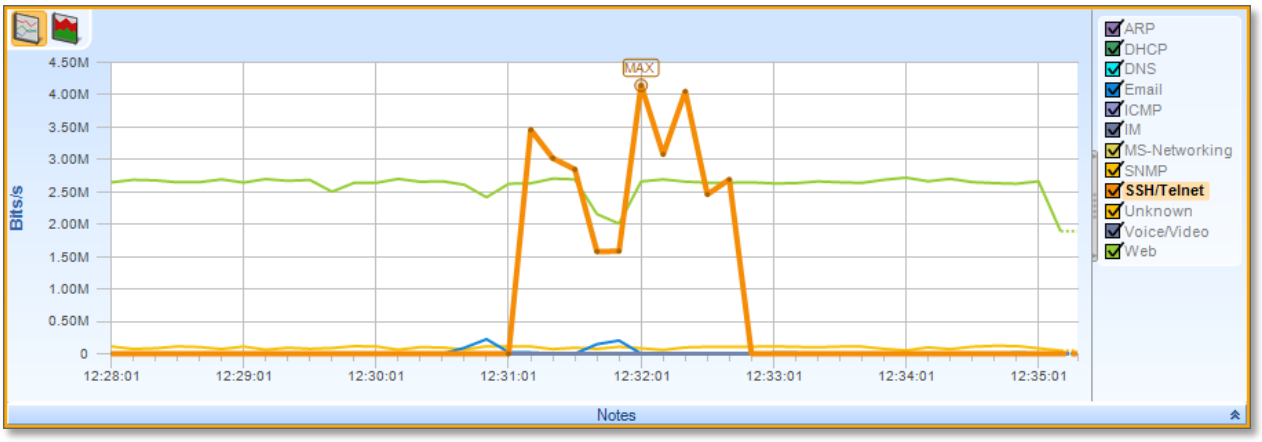


Strip Chart Selection (Time)

Note that multiple selections cannot be performed using time-based selection.

Line- or Area-Based Selection

A *Line- or Area-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:

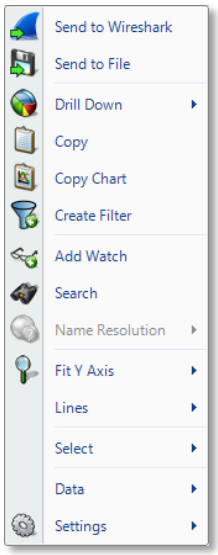


Strip Chart Selection (Element)

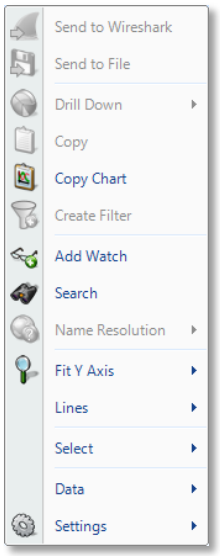
Individual lines or areas are selected by clicking either on the line or area itself, or on its representation in the legend. Multiple lines or areas can be selected by clicking with the Control key pressed.

Context Menu

The context menu for a strip chart has the following options:



Context menu (selection)



Context menu (no selection)

Send to Wireshark

Sends traffic from the selected time slice or lines/areas to Wireshark for analysis.

Send to File

Sends traffic from the selected time slice or lines/areas to a user-specified trace file that will appear, after completion, in the Files panel, for immediate analysis.

Drill Down

Applies the user-specified view to the selected time slice or lines/areas and opens a new view tab in the main workspace.

Copy

Copies a tabular form of the selected data to the system clipboard.

Copy Chart

The Copy Chart menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

Create Filter

Creates a filter based on the current selection and adds the filter to the Filter List.

Add watch

Opens 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.

Search

Opens a search dialog window that can be used to find data in the charts.

Name Resolution

The Name Resolution menu option tries to identify the port name, IP address, or MAC address of all or the selected elements in the strip chart. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Fit Y Axis

Scales the vertical height of the strip chart to fit within the chart. Default is Fit All.

Fit All

Y Axis is fit to the currently available strips.

Fit Selected Only

Y axis is fit to the selected strips. Strips must be selected before this choice is available.

Lines

The Lines submenu allows you to choose what lines are displayed.

Show All

Shows all hidden lines.

Show Selected Only

Hides all lines but the selected one(s).

Show All But Selected

Hide the selected line(s) and show all others. Note that at least two lines must be visible at all times.

Inverse

Reverses the hidden line set, by showing all hidden lines and hiding all visible ones.

Select

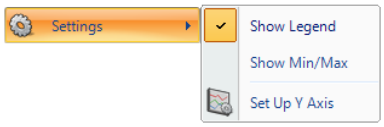
Brings up two submenu options:

Select All

Selects all lines or areas.

Select Inverse

Selects all lines or areas that are not currently selected (and deselects those that are currently selected).



Settings

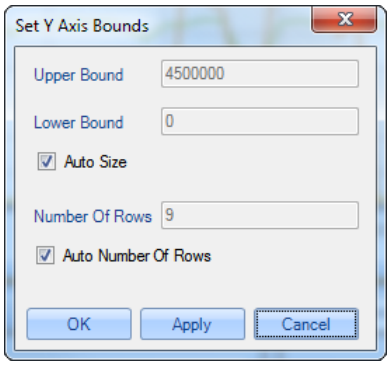
Brings up three submenu options:

Show Legend

Shows the legend area to the right of the strip chart, indicating which data sets correspond to which lines or areas.

Show Min/Max

Shows a minimum point and a maximum point for each data set on the chart:

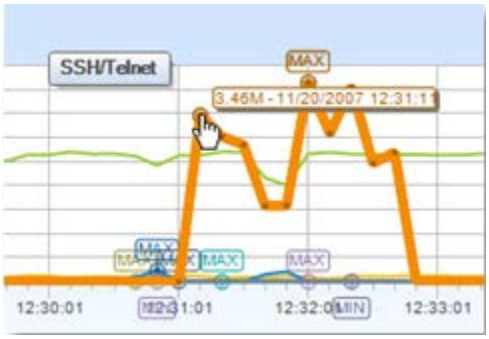


Setup Y Axis

Brings up the dialog for setting up the Y axis. You can set the upper and lower bounds of the Y axis, or choose Auto Size to let Packet Analyzer personal edition choose the bounds automatically. And you can specify the number of increments displayed on the Y axis, or choose Auto Number of Rows to let Packet Analyzer personal edition choose the number of rows 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. Hover your mouse over a sample point to see its value.



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

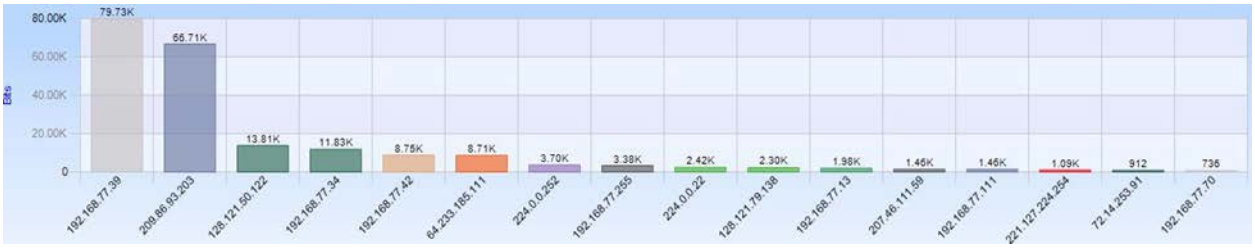
Single Bar Charts are the most basic form of Bar Charts. Each column is a single valued bar. The colors of the bars match the labels in the legend.

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

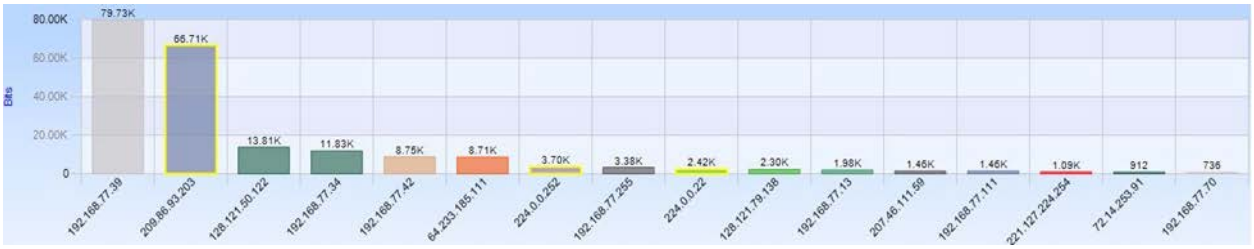
This is an example of the default view for a Single Bar Chart:



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 selections.



Bar Chart Multiple Selection

Stacked Bar Chart

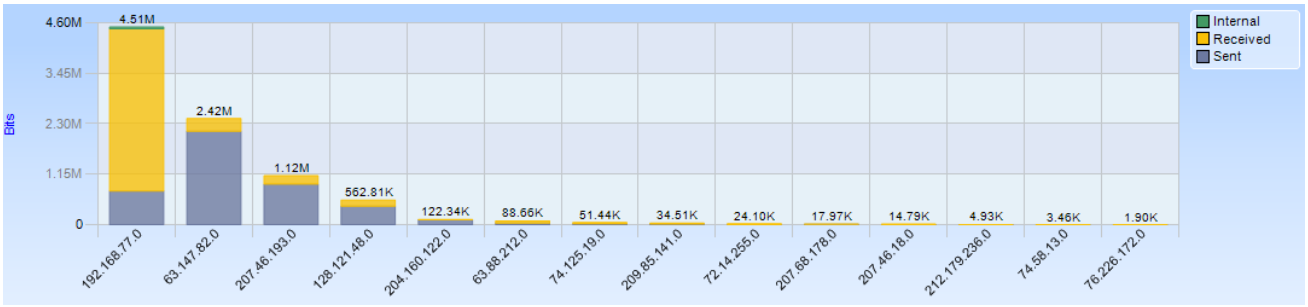
A *Stacked Bar Chart* is similar to a Single Bar Chart except that each column is subdivided into predetermined constituents. These constituent components can be selected and analyzed individually or collectively.

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:



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 selections.

Grouped Bar Chart

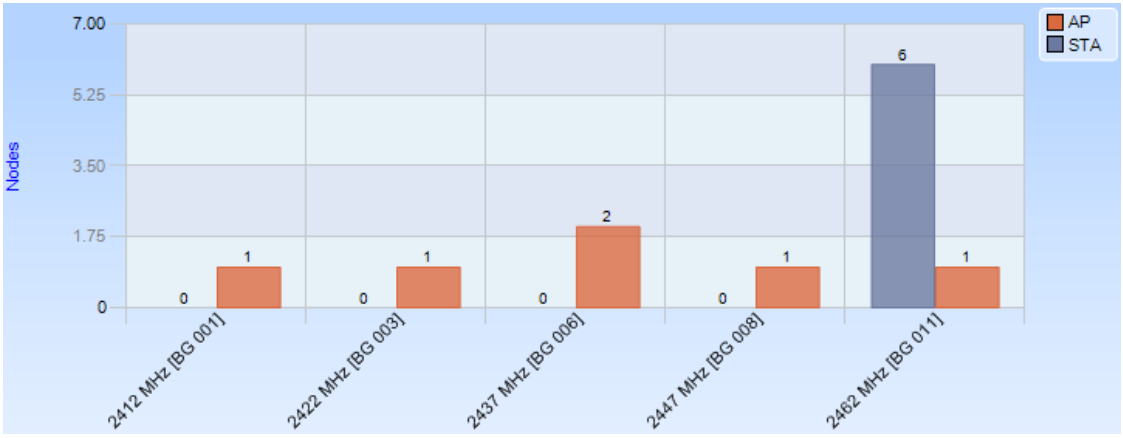
A *Grouped Bar Chart* is similar to a Single Bar Chart except that each column is subdivided into two or more sub columns.

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:



Grouped Bar Chart

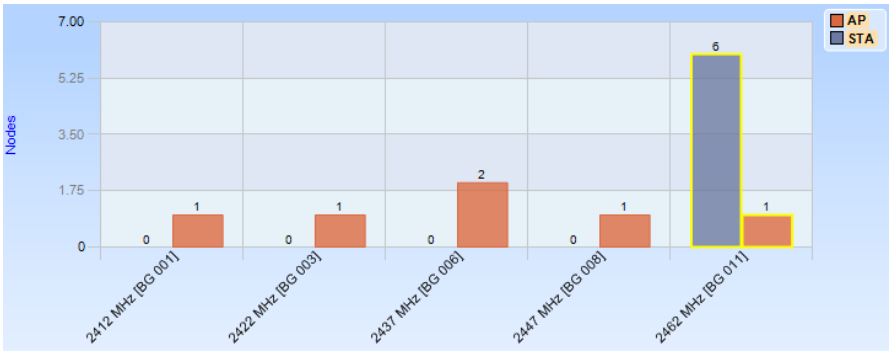
Selection

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

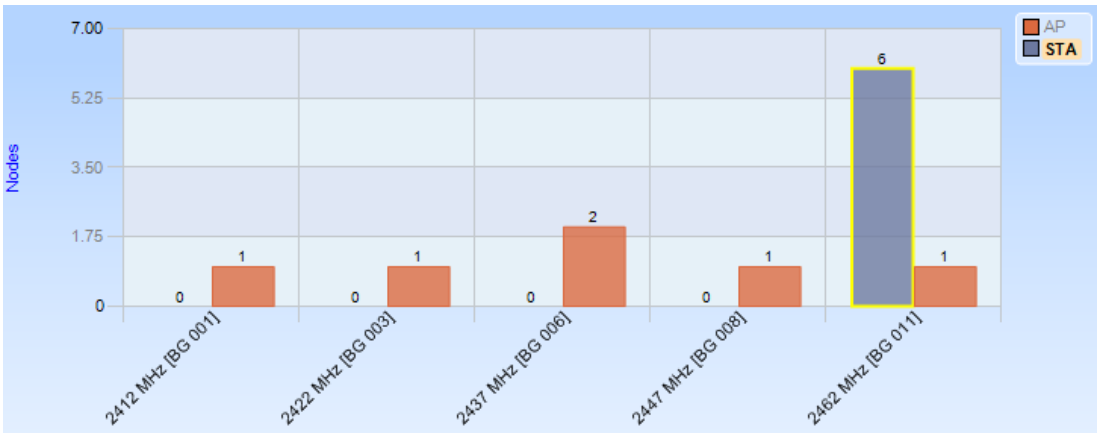
A *column based* selection selects all data corresponding to the column. This method of selection is achieved by selecting the area around the bar with respect to the desired column inside the chart, but not the bar itself.



Grouped Bar Chart Selection (Column)

Component Instance

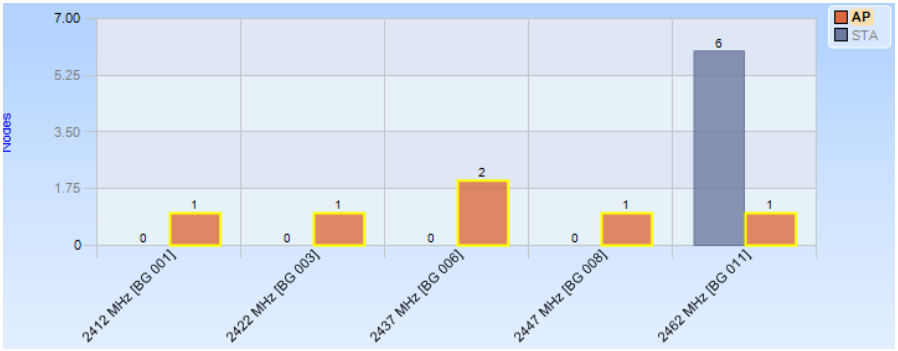
A *component instance based* selection selects a subset of the data in a particular column. This method of selection is achieved by clicking on the component.



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.



Grouped Bar Chart Selection (Component)

Navigation Through Data

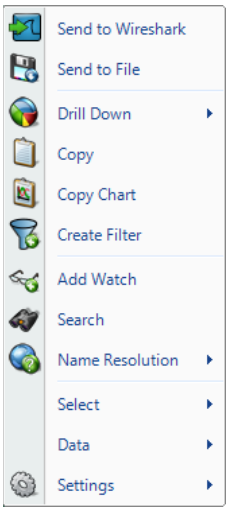
Bar chart Top Bars

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).



Bar Chart (Selection)

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

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

Copy Chart

The Copy Chart menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

Create Filter

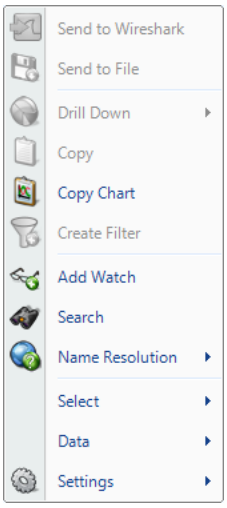
The *Create Filter* menu option creates a filter based on the current selection within the bar and adds the filter to the Filter List.

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).

Search

The *Search* menu option opens a search dialog window that can be used to



Bar Chart (No Selection)

find data in the charts.

Name Resolution

The Name Resolution menu option tries to identify unresolved IP addresses, ports, or MAC addresses from all or the selected bars. Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and *Clear All*

Resolved names not displayed.

Select

The *Select* menu option provides the option to select the bar(s) and component(s) of the Bar Chart. It is described below

Data

The *Data* menu option provides settings for the organization of the data on the Bar Chart. It is described below

Settings

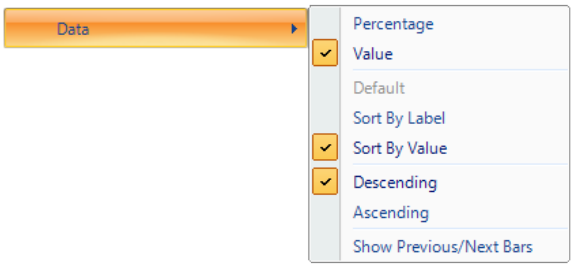
The *Settings* menu option opens up a submenu with specific settings for the chart. It is described below.

Context Sub-Menus

The Bar Charts have three contextual submenus:

- Select
- Data
- Settings

Select Submenu



Data Submenu

The *Select* submenu for the Bar Chart context menu has two options:

Select All

Select All selects all bars in the chart.

Select Inverse

Select Inverse deselects the currently selected bar(S) and selects all other bars.

The *Data* submenu for the Bar Chart context menu has several items:

Percentage

The Percentage option sorts the bars numerically by their percentage of the total traffic.

Value

The *Value* option sorts the bars numerically by their quantitative values.

Default

The *Default* option reverts to the original sorting order.

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.

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.

Show Previous/Next Bars

When there are more bars than will fit in the display area, selecting this option displays a

Previous bar and/or a Next bar. These bars show cumulative totals for all bars that come before and/or after the bars displayed in the current view.

Settings Submenu

The *Settings* submenu for the Bar Chart context menu has two items:

Show Legend

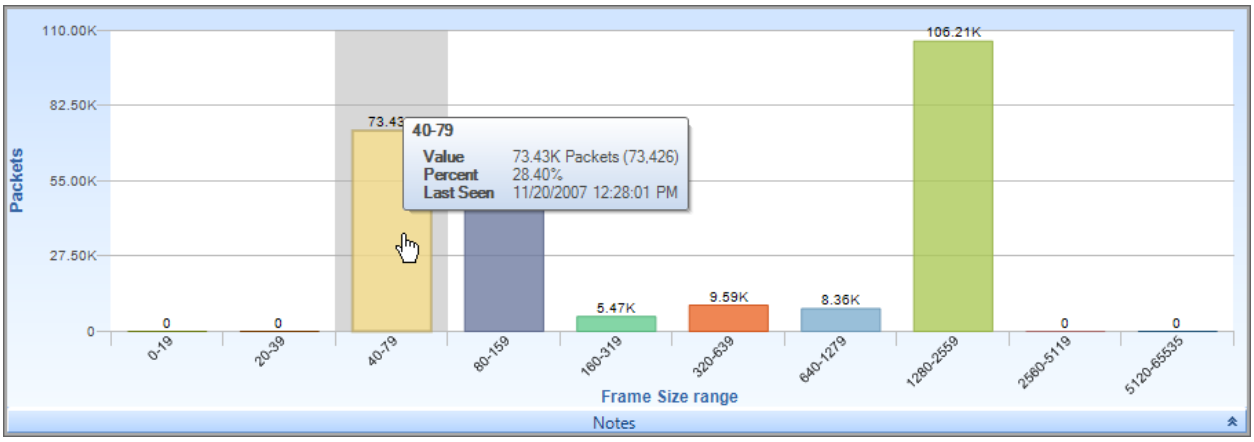
The *Show Legend* menu option toggles off or on the Bar Chart legend.

Show Labels

The *Show Bar Labels* menu option toggles off or on the Bar Chart labels.

Tooltips

The tooltips for the Bar Chart display the label of the bar over which the mouse is hovering.



Scatter Plot

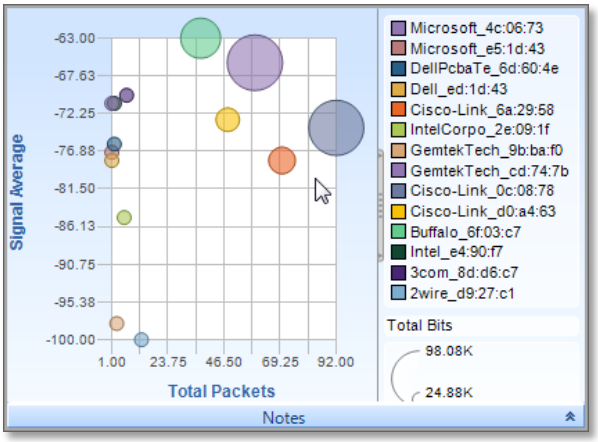
The *Scatter Plot* is a versatile and flexible chart that can display complex relationships between values using three dimensions:

- 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

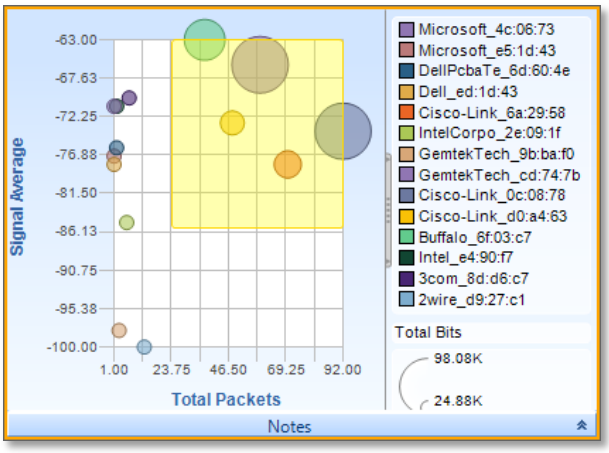


Scatter Plot

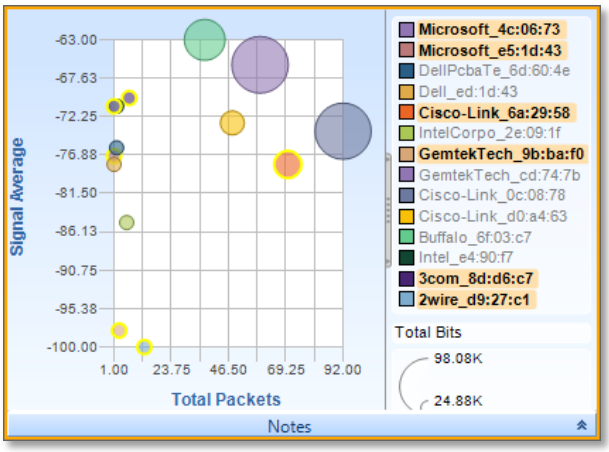
Along with the "Sampling Time" and "Data Retention Time" options previously described, the scatter plot is customizable in the following ways:

- Assignment of the dot size relation
- Assignment of X-Axis
- Assignment of Y-Axis

Selection



Scatter Diagram Draw Box



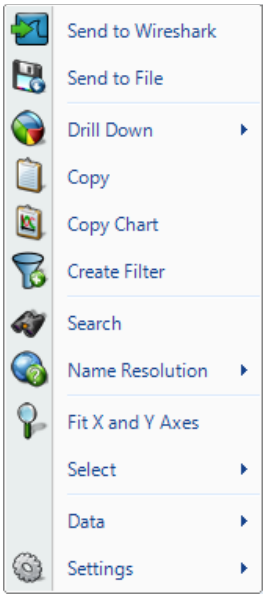
Scatter Diagram Multiple Selection

Selection in a Scatter Plot is done by one of four ways:

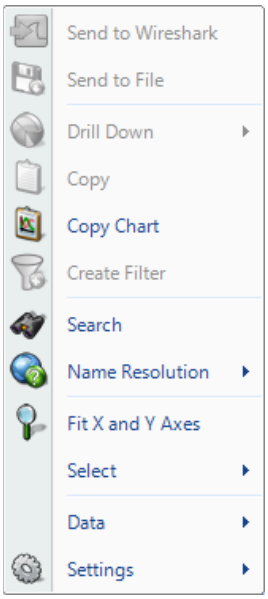
- Search operation
- Selection from the legend
- Drawing a box around the points
- Clicking on the Points to be selected

Clicking with the Control key pressed for multiple selections is supported for point based and legend based selection.

Context Menu



Scatter Plot (Selection)



Scatter Plot (No Selection)

Scatter Plot Select Submenu

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

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

Copy Chart

The Copy Chart menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

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.

Name Resolution

The Name Resolution 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). Default is from Settings menu.

Enabled

Turns on auto resolution of current and new addresses.

Resolve Selected

Resolve only selected addresses.

Clear Selected and Clear All

Resolved names not displayed.

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.

Select

The *Select* menu option has two submenu options.: *Select All* the

point(s) in the Scatter Plot, or *Select Inverse* of the selected point(s).

Data

The *Data* menu option provides choices for the data and its presentation on the Scatter Chart. It is described below.

Settings

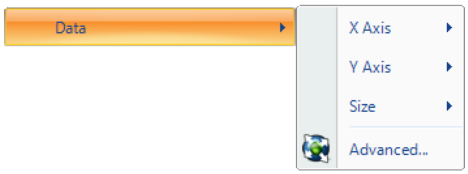
The *Settings* menu option opens up a sub-menu with specific settings for the chart. It is described below.

Context Sub-Menus

The Scatter Plot has three contextual submenus:

- Select (shown above)
- Data
- Settings

Data



Scatter Plot Data Submenu

The Data submenu for the Scatter Plot context menu has four items:

X Axis

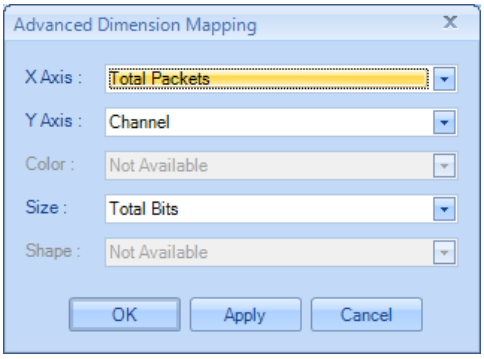
The *X Axis* menu option presents all possible choices for the metric of the X-Axis. Some charts may only have one option, while others may have multiple; for instance, "Bits/s" versus "Bytes/s" or "Packets/s."

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 where drop-done lists provide options for a chart's format.

Settings

Scatter Plot Settings

The Settings submenu for the Scatter Plot context menu has three items:

Show Legend

The *Show Legend* check box menu option toggles off or on the Scatter Plot legend.

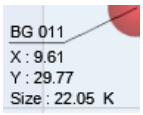
Show Labels

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



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.

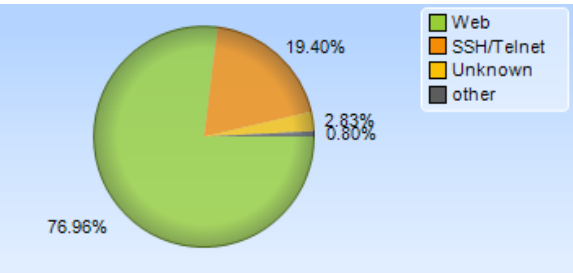
Size

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



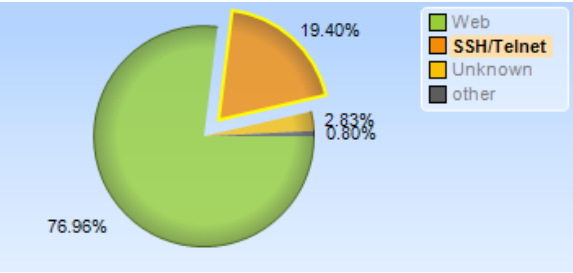
Pie Chart

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.

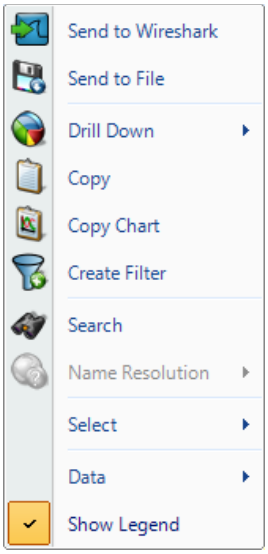
Selection



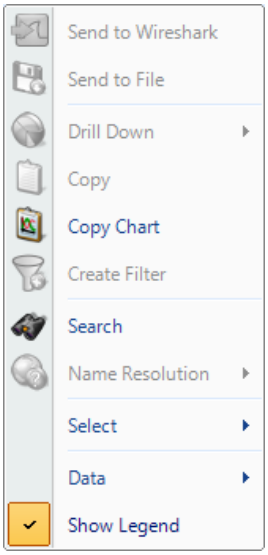
Pie Chart Selection

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.

Context Menu



Pie Chart (Selection)



Pie Chart (No Selection)

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

Copy Chart
The Copy Chart menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

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.

Name Resolution
The Name Resolution menu option resolves, when applicable, the Port Name, IP Address, or MAC Address of the slice(s) in the Pie Chart. Default is from Settings menu.
Enabled
Turns on auto resolution of current and new addresses.
Resolve Selected
Resolve only selected addresses.
Clear Selected and *Clear All*
Resolved names not displayed.

Select
The *Select* menu option has two submenu options, described below.

Data
The *Data* menu option is described below.

Show Legend

The Show Legend check box menu option toggles off or on the Pie Chart legend.

Context Sub-Menus

The Pie Chart has two contextual submenus:

- Select
- Data

Select

Pie Chart Select

The settings submenu for the Pie Chart context menu has two items:

Select All

The *Select All* menu option selects all slices in the pie chart.

Select Inverse

The *Select Inverse* menu option deselects the currently selected slice(s) and selects all others.

Data

Pie Chart Data

The *Data* submenu for the Pie Chart context menu has two items:

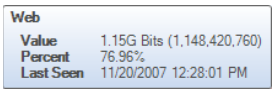
Percentage

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



Pie Chart Tooltip

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.

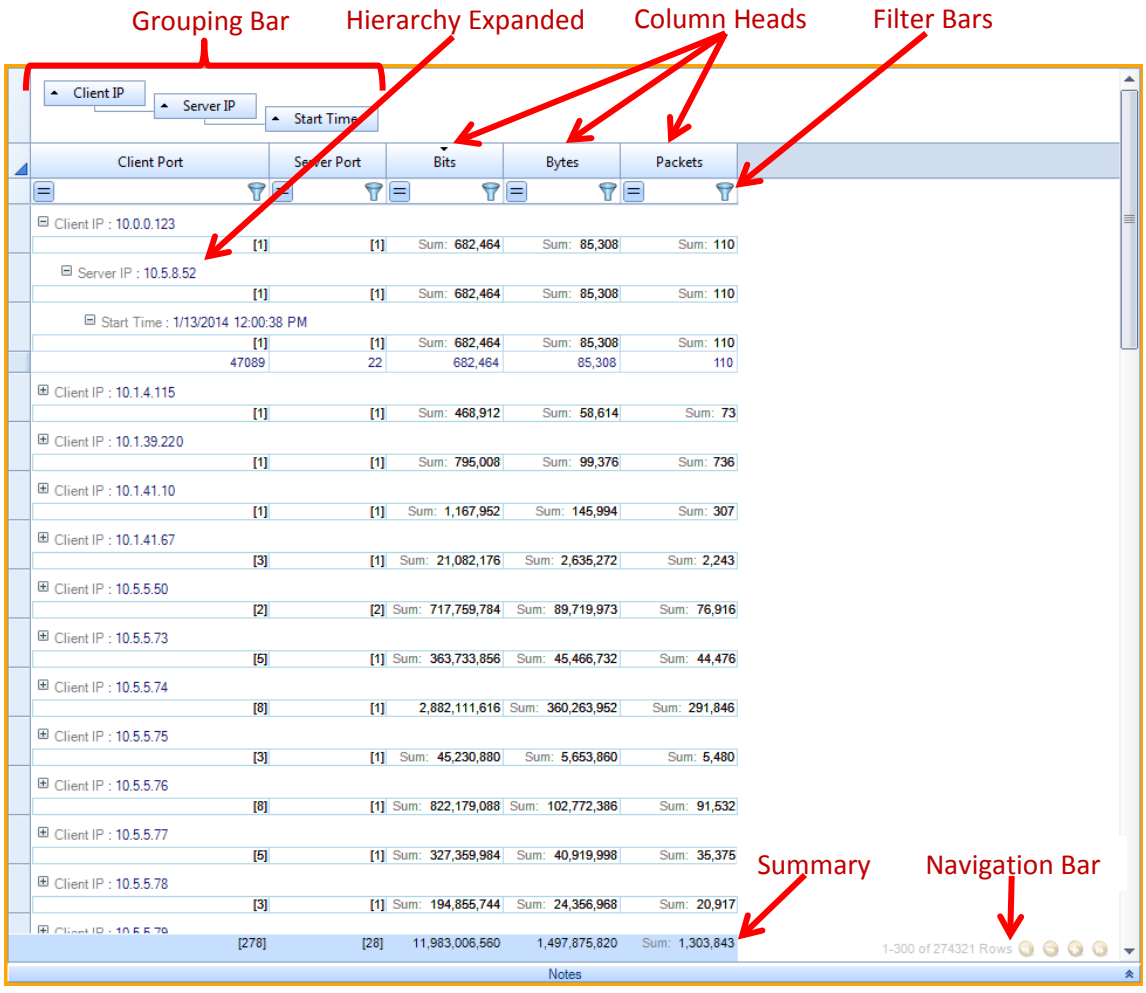
The columns can be:

- Rearranged in any order
- Resized
- Hidden and shown

The rows can be:

- Filtered
- Sorted by one or multiple columns simultaneously
- Hierarchically grouped
- Summarized by selection, group, or the entire table.

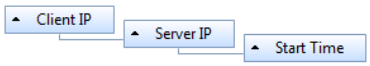
The figure below shows an example grid with a number of features enabled and some grid components identified.



Grid

Grouping Bar

The elements of the *Grouping Bar*, called groups, determine the row hierarchy. In the above example, columns in the view Performance and Errors>TCP>Connections and Requests> TCP Traffic Details by Connection have been dragged into the Grouping Bar to group the TCP traffic connections and metrics. The root level contains the Client IP. Each Client IP can be expanded to show the Server IP, which can in turn be expanded to show the Start Time.



Grid Grouping Bar

Each element of the Grouping Bar also has a triangle before each group that specifies the sorting order of that level of the hierarchy. The order can be toggled by clicking on the group itself.

Additionally, grouping can be changed by dragging group headers into a different order, and groups can be removed from the hierarchy by dragging them back to the grid.

The data grid rows organized in a multi-tiered tree using the grouping bar can be fully expanded and collapsed using the context menu. The "+/-" box next to a grid row can also be used to expand a group.

Column Headers

Column Headers refers to columns which can be shown or not shown using the Columns item in the right-click context menu. Column headers dragged to the top of the chart group rows in the hierarchy specified in the Grouping Bar. Grouped rows appear under the left-most column header.

Sorting

One or more column headers can be used to sort table rows. Clicking a column head sorts the rows by that column. An arrow appears above the column name indicating it is being used to sort the rows and the type of sort, ascending or descending, being performed. Click a column to change the type of sort done. Sort rows using additional columns by shift-clicking columns in the desired sort order. The sort type can be changed by shift-clicking on the column.

Grid data is sorted as follows:

- Text fields – alphabetically
- IP addresses – numerically by each address component, left to right.
- Numbers – numerically
- Time – by time value

Note: Sorting is done on the displayed value of the cell in each row of a column. The precision of a value may be higher than that of the displayed value, resulting in cells in some rows appearing to be the same when they are in fact different.

When using groups, sorting on a grouped column sorts the groups; sorting on a non-grouped column sorts the rows within each group.

Filter Bars

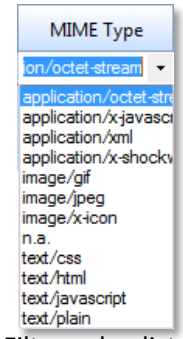
A Data Grid *Filter Bar* enables the filtering of data rows by a column. A filter is made up of two elements :

- A value
- An operator

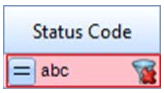
Click in a column's filter bar to enter a filter. Hold down the shift key and click in a column's filter bar to enter additional filters.

Values

A filter value can be entered in the filter bar or selected from a list of the column's contents by clicking the funnel icon on the right side of the filter bar. Here is an example of selecting a value from a MIME Type column. The drop down list contains all MIME types present in the grid rows.



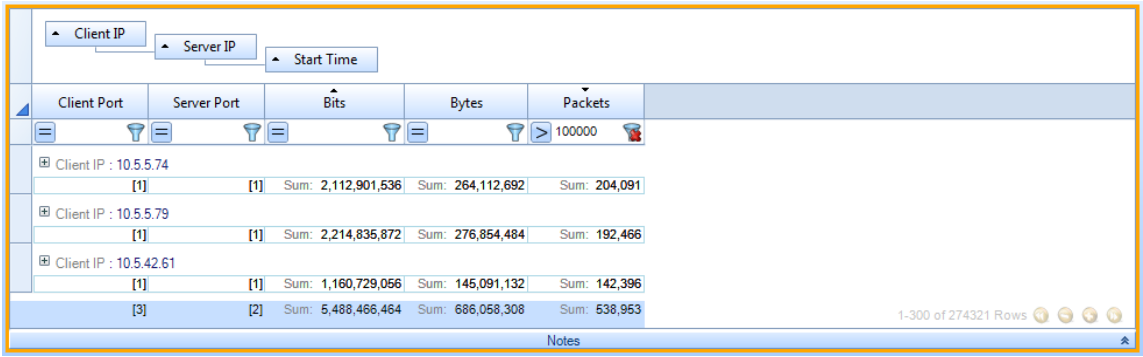
Filter value list



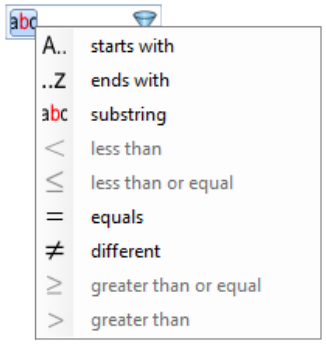
Invalid Filter value

Entered values are evaluated as the same value type as the column's values. For example, in a column of time values, the entries "2m" or "120s" are evaluated to the same value. Invalid entries, for example, text entered in a numeric column, are highlighted in red as shown in the figure above. All filtering is done on the displayed values, so different values can be displayed as the same and will be filtered as the same value. Note: Only rows can be selected in a grid table, not cells, so you cannot cut-and-paste the value in a cell for use in a filter. However, a cell's value can be selected from the drop down list displayed when you click the funnel icon in a column's filter bar.

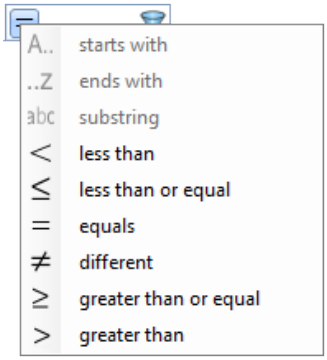
When a filter is applied, a red X appears over the funnel icon. Click the X to remove the filter.



Operators



For strings or IP addresses



For numbers or time values

A filter *Operator* is selected by clicking the icon on the left side of a column's Filter Bar. A drop down list opens that lists the operators available based on the type of content in the column (strings, IP addresses, numbers or time values). After an operator is selected, rows not satisfying the filter are hidden.

A filter bar has a default operator based on the type of content in the column. If you enter a value without selecting an operator, the default operator is used:

- Substring for text or IP addresses
- = for numbers or time values

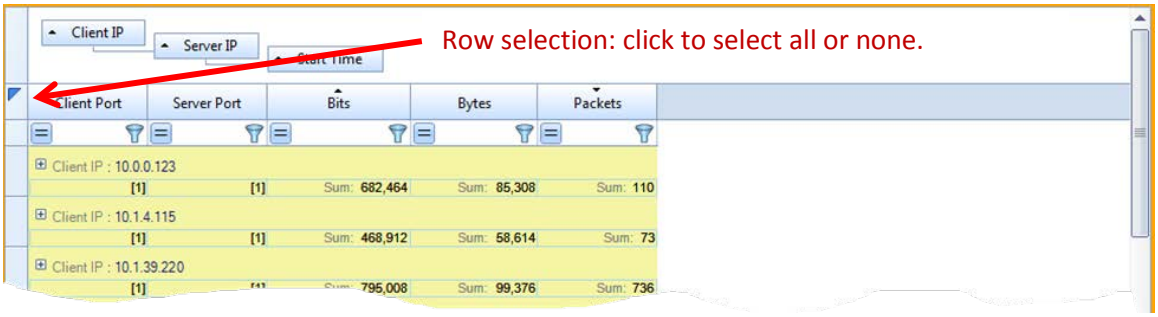
Further filters can be applied. The funnel now only lists the values from the rows that are not filtered out.

Operators Drop Down

Once a value and an operator are specified, the filter is enabled.

Selection

Select all or select none can be performed by clicking the cell at the left end of the column header row. The icon changes when the cell is clicked to indicate whether all or none of the rows will be selected.

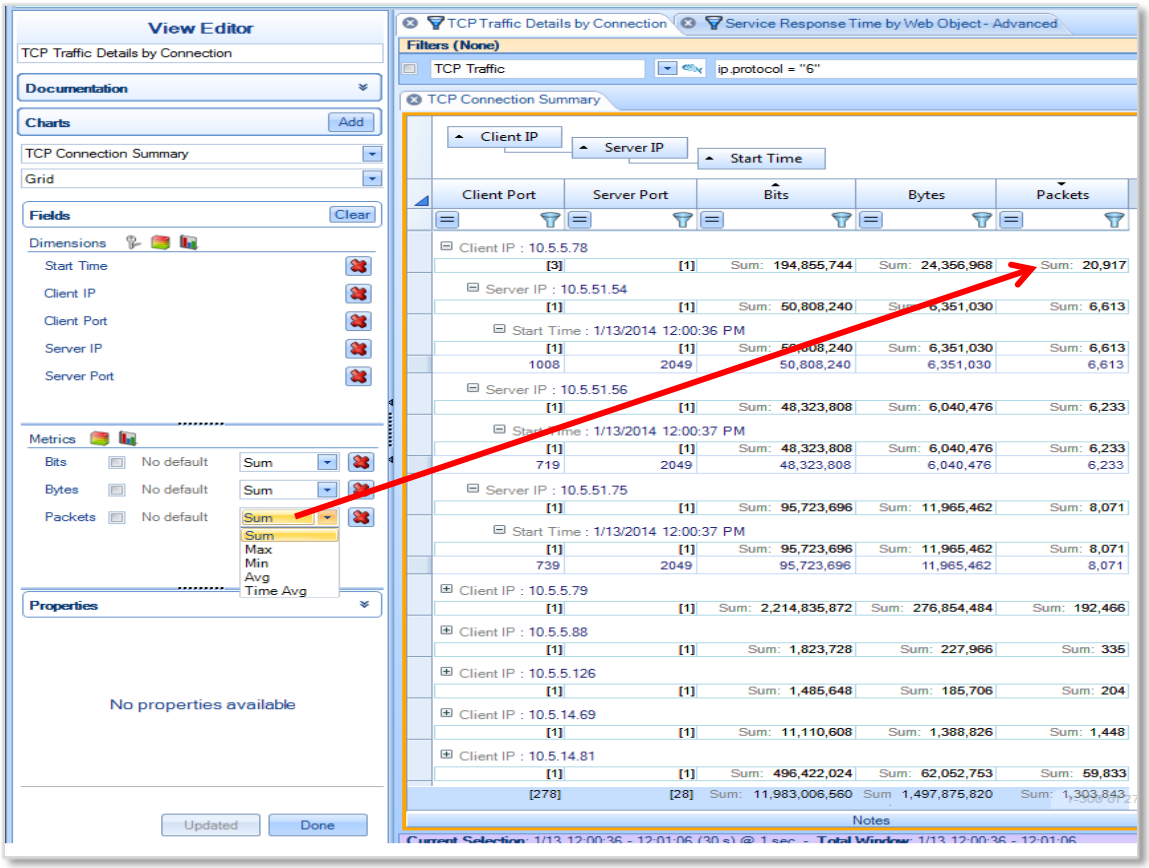


Any combination of rows or groups can be selected although selecting rows when the parent group is already selected does not change the meaning of the selection. All of the standard Windows selection shortcut keys, for example, Control-A, can be used. All of the standard Windows selection shortcut keys, for example, Control-A, can be used.

The context menu provides options on how selected content can be used.

Summaries

A table summary appears at the bottom of each table, providing item counts for unique values in a dimension column and calculated values for a metric column. The type of value calculated is set in the view and can be changed using the view editor. Right-click the view applied to the traffic source and click the Edit item. Set the type of calculation you want under Metrics. Below is the example grid we have been using as shown in the View Editor:



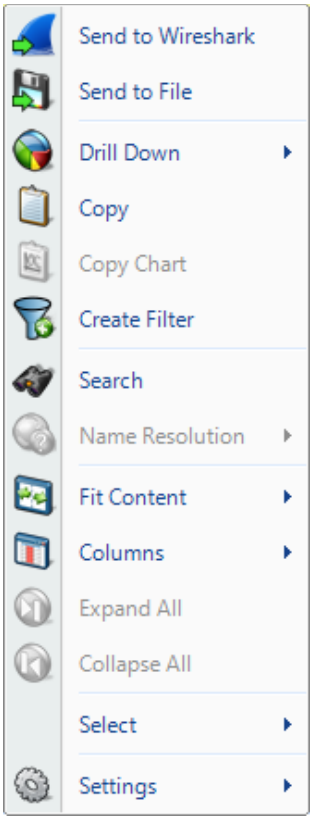
If no rows or groups are selected, the summary table includes all table rows and groups. If specific rows or groups are selected, the summary only includes the selected items. Selected rows that appear in a selected group are not double counted.

A group summary is provided for each group. A grid with three groups, such as our example, will have a summary shown for each group. Our example includes a summary for Client IP. A summary for Server IP, and a summary for Start Time, as shown above.

Note: If a grid has 300 or more rows, a navigation pane appears in the lower right corner of the screen. The table summary includes the rows indicated by the navigation pane, which could be less than the number of rows in the entire table.

To save a view with customized summary calculations, click Save in the View section of the Home ribbon. A new name must be used as standard views cannot be overwritten.

Context Menu



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) and group(s) to Wireshark for analysis.

Send to File

The *Send to File* menu option sends the traffic from the selected row(s) and group(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 group(s) and opens a new view tab in the main workspace.

Copy

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

Copy Chart

The Copy Chart menu option copies the selected chart as a metafile to the system clipboard for pasting into another application.

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

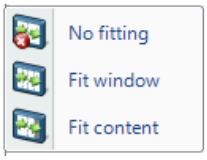
The *Search* menu option opens a search dialog window that can be used to find data in the charts.

Name Resolution

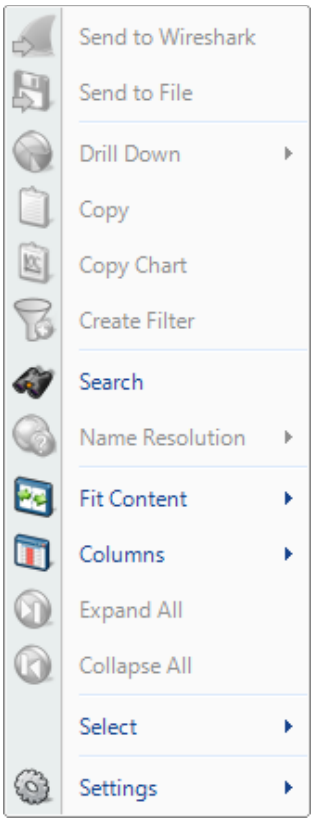
The *Name Resolution* menu option is always disabled for the grid and is included in the context menu in order to be consistent with the other charts.

Fit Content

The *Fit Content* menu provides options for resizing the table columns.



- *No fitting* - The same default width is given to each column. Column widths can be manually adjusted.
- *Fit Window* - Column widths are adjusted so they



Grid (No Selection)

use the entire horizontal space. Each column is given the same width. Column widths can be manually adjusted.

- *Fit content* - Column widths are adjusted based on the column content .Column widths cannot be manually adjusted.

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.

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.

Select

The *Select* menu option has two submenu options, described below.

Settings

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

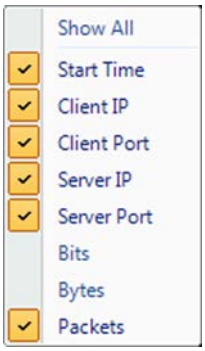
Context Sub-Menus

The Data Grid has three contextual submenus:

- Columns
- Expand All
- Collapse All
- Select
- Settings

Columns

The *Columns* menu option expands to a submenu that is used to show and hide columns in the grid. A menu shows a check box for each column. Toggling the various options will either show or hide the corresponding columns. A checkbox is also provided to show all items in a single click. Grouped columns visibility cannot be changed.



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.

Select

Grid Select

The *Select* submenu for the Data Grid context menu has two items:

Select All

The Select All menu option selects all visible rows and groups in the grid.

Select Inverse

The current selection in the grid is inverted.

Settings

Grid Settings

The *Settings* menu option provides specific settings for the chart.

Show Filter Bar
Shows or hides the filter bar on the Data Grid Chart.

Show Grouping Bar
Shows or hides the Grouping Bar on the Data Grid Chart.

Channels Button

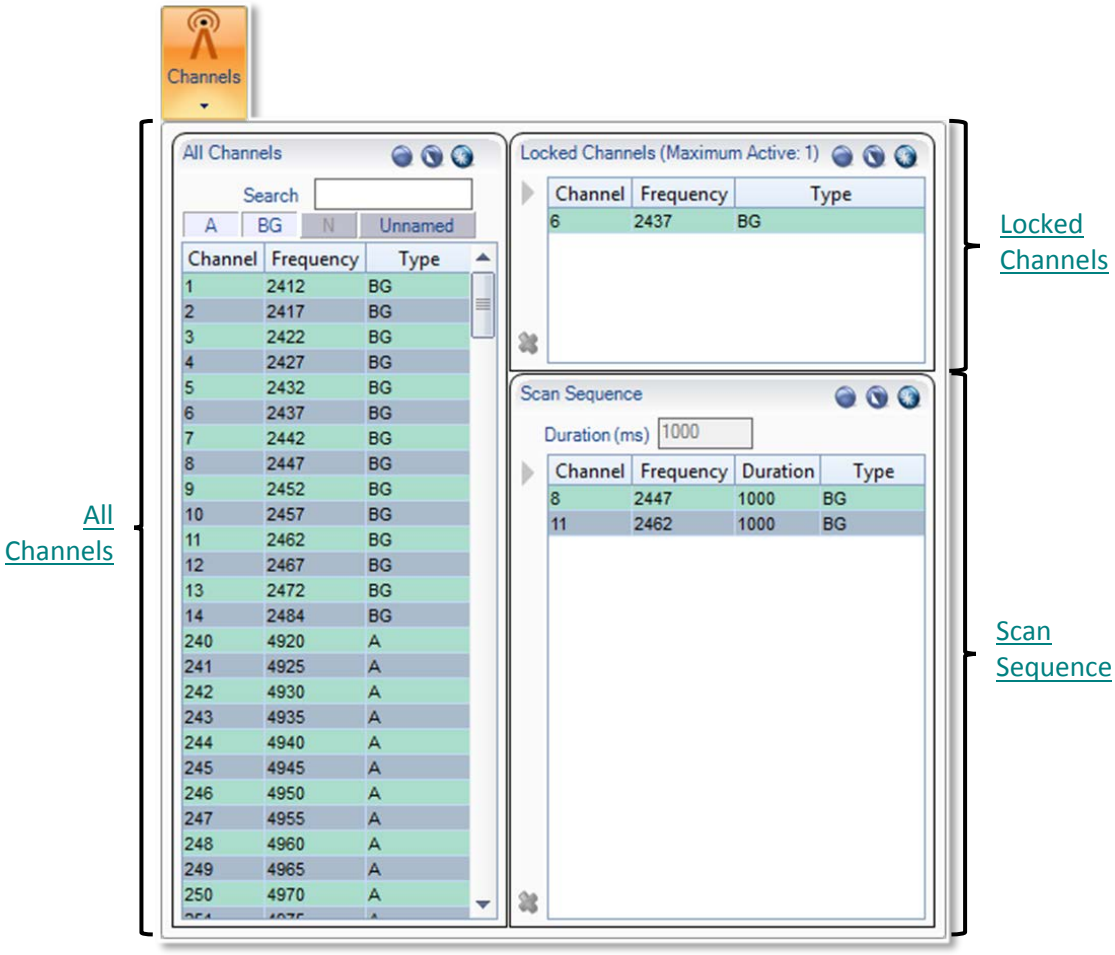
A Packet Analyzer personal edition provides 802.11 wireless analyses on live traffic using the Riverbed Technology AirPcap adapters for wireless interfaces.

Figure 27 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 27). 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.



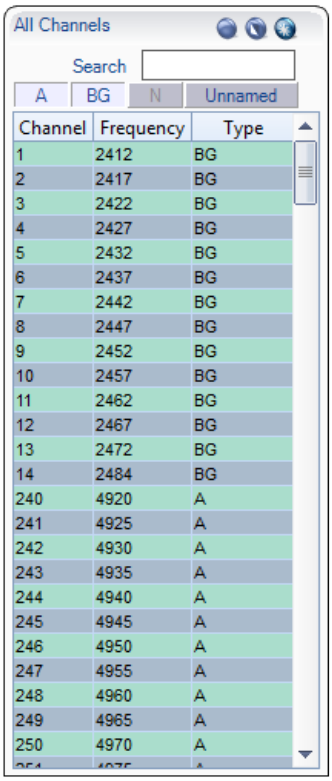
Channel Management Panel

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



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 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.

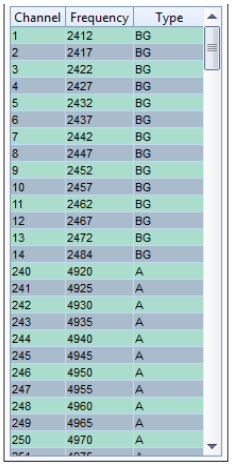
However, there are some very important restrictions that must be taken into consideration when using multiple classes of AirPcap adapters at once:

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
250	4970	A

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

Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.

Invert Selection

The *Select Inverse* button reverses the channel list selection(s).

Select All Channels

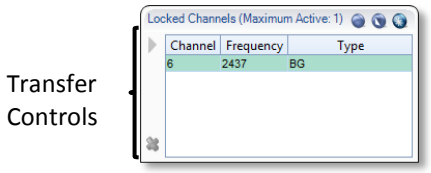
The *Select All* button selects all of the channel(s) in the channel list.

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

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 Packet Analyzer personal edition. 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

Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.

Invert Selection

The *Select Inverse* button reverses the channel list selection(s).

Select All Channels

The *Select All* button selects all channel(s) in the channel list.

Transfer Controls

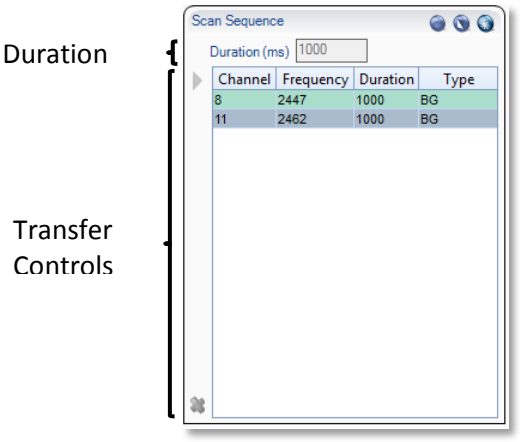
Transfer Channels

The *Right Arrow* button adds the selected channel(s) to the locked list. If the selected channel was in the Scan Sequence List, it is removed from that list.

Remove Channels

The *Remove* button removes the selected channel(s) from the lock list. The lock list can be empty..

Scan Sequence



Scan Sequence

The *Scan Sequence* is a list of channels that the wireless adapter(s) will listen on occasionally. It contains four elements:

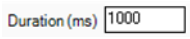
- Duration
- Selection controls
- Transfer controls
- Channel list

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, for example, 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



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

Select No Channels

The *Select None* button deselects all channel(s) in the channel list, if applicable.

Invert Selection

The Select Inverse button reverses the channel list selection(s).

Select All Channels

The *Select All* button selects all channel(s) in the channel list.

Transfer Controls

Transfer Channels

The *Right Arrow* button adds the selected channel(s) to the scan sequence list. If the selected channel was in the locked list, it is removed from that list. Durations of previous, deleted channel(s) are not saved if they are retransferred. Channels are removed from the Locked Channels section when they are transferred.

Remove Channels

The *Remove* button removes the selected channel(s) from the scan list. The scan list can be empty.

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 channel will be scanned before moving on to the next. Each channel can have a different duration value.

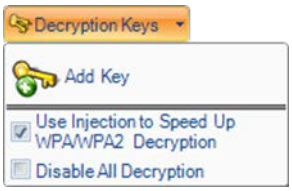
Decryption

Packet Analyzer personal edition 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



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.

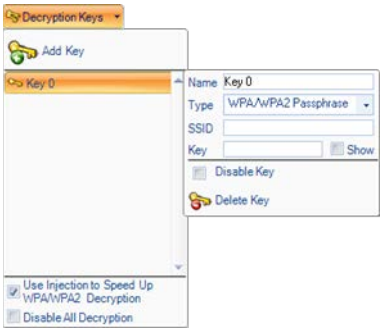
Disable All Decryption

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

Decryption Keys with Key



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.

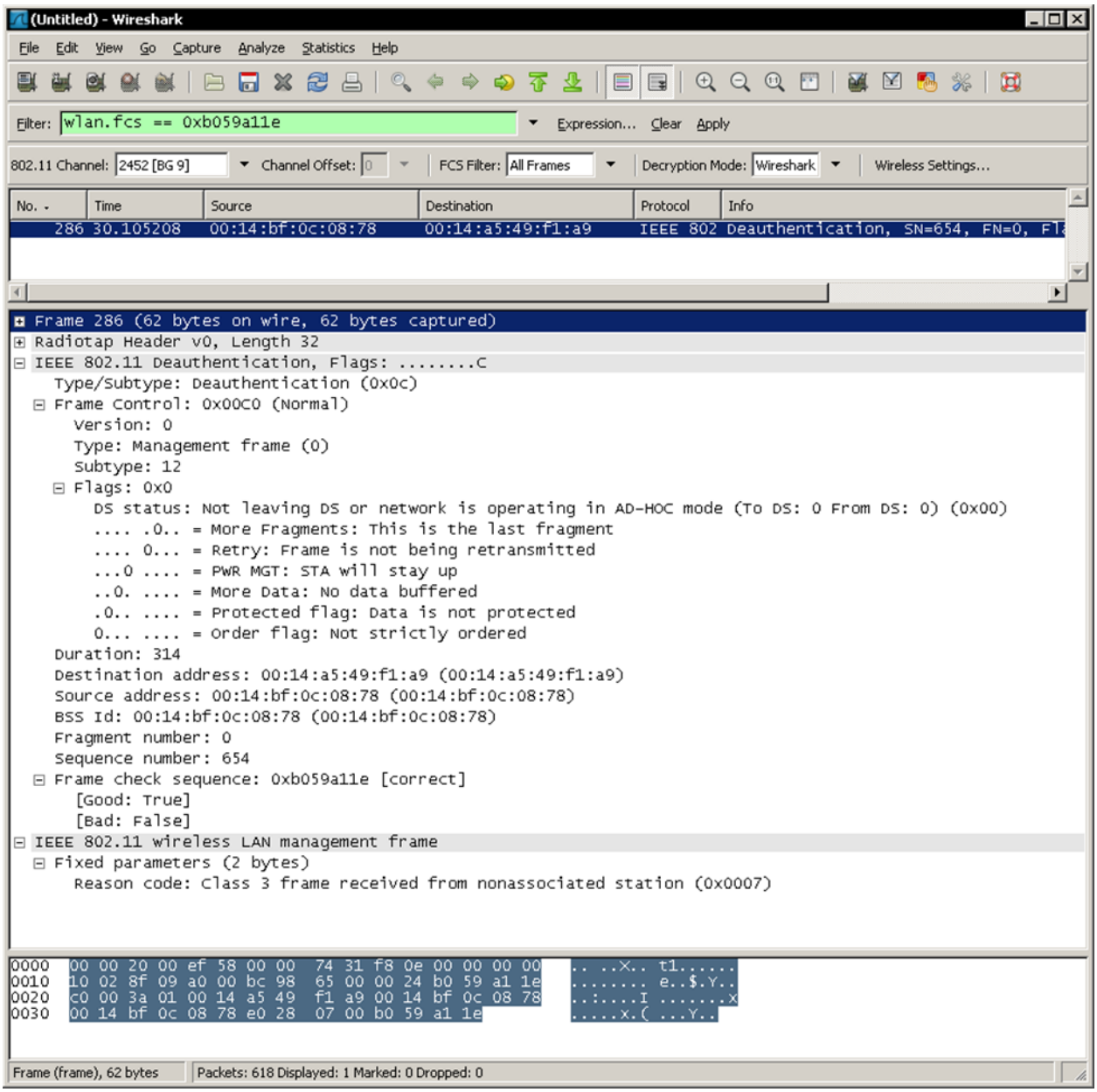
In order to successfully decrypt WPA traffic then, even with a valid decryption key, the setup of this link needs to be captured. However, because stations may not authenticate for hours or possibly longer, in order to view traffic without waiting a long time, the hosts need to re-associate with their 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:



Wireshark analyzing a Packet Analyzer personal edition generated Deauthentication frame

Drill Down

Drill Down enables data to be analyzed at various levels of detail by iteratively applying views to visually selected subsets of the data.

How to

A drill down can be done in three ways:

- Make a selection in a chart and click the Drill Down button in the Chart Selection section of the Home Ribbon.
- Right-click a selection in any chart and select Drill Down from the context menu.
- Drag a view from the Views Panel over a selection in a chart.

Every chart has a means of selecting data subsets to enable a drill down operation.

The following operating rules apply to drill down operations:

- If you can create a filter using a selected item, you also can drill down on the selected item.
- Drill down is not available for a time selection in a view applied to a live source.
- Drill down is chart specific. Drill down may be available in some charts in a view, but not others.

Examples

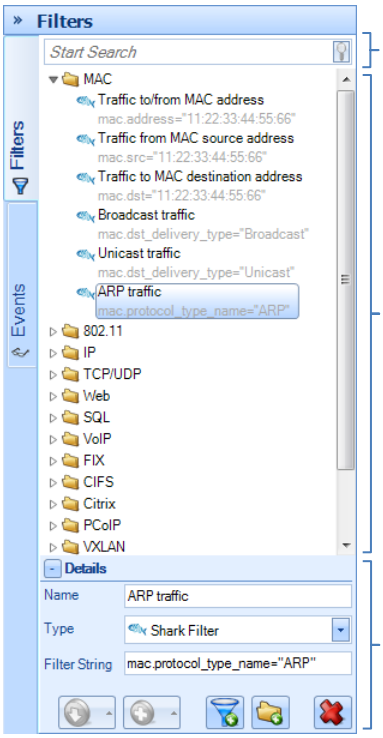
For examples of Drill Down sequences and operations, please refer to the tutorial videos. Click Getting Started in the General section of the Home Ribbon

Filtering

Packet Analyzer personal edition 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 Packet Analyzer personal edition user interface in the tabbed navigation panel, displays and organizes the set of filters. The panel is composed of three elements.



Filter Search Box

Filter Library

Filter Editor

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:

- NetShark 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 *Not Selected*	Selected filters are applied in place of applied filter of the same type.
... and selected *... and not selected* *... or selected* *... or not selected*	Selected filters are applied to the currently applied filter of the same type and the new filter value depends on the chosen operator.

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 Packet Analyzer personal edition 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 Packet Analyzer personal edition, 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.

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 types* 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 a chart's master time controller to apply it. It can be dragged over a Strip Chart 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 a Strip Chart or a chart's master time controller onto the Filter panel.

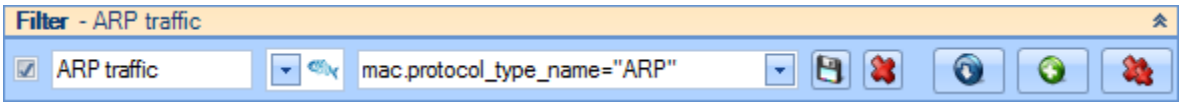
Shortcuts
Some of the operations can be performed by keyboard shortcuts:

- **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 Packet Analyzer personal edition 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 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.

Filter panel - Filter bar interaction

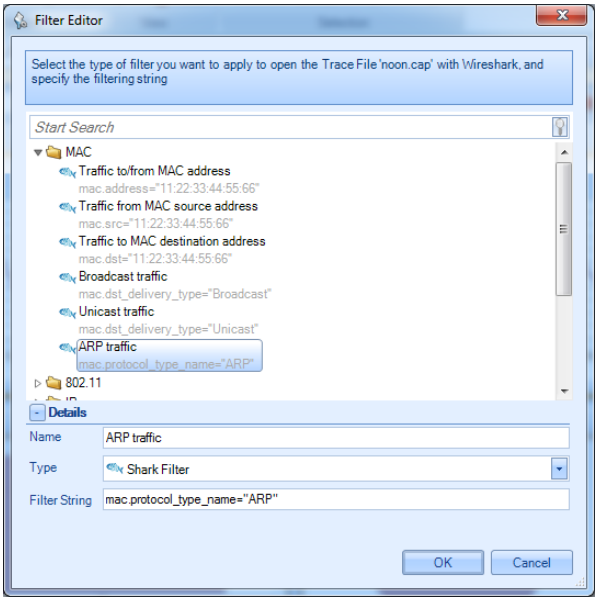
As mentioned above, any filter can be dragged over the Filter Bar to instantly apply it. See the previous section for a description of the various options for applying filters using drag & drop.

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

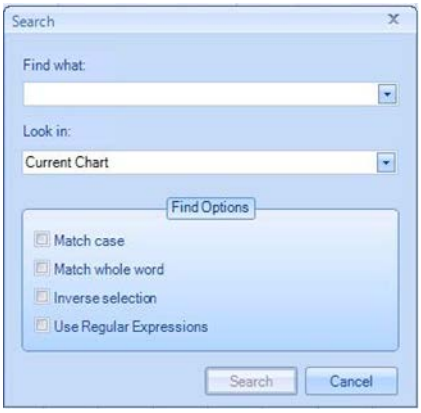


Filter Dialog

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



Search Dialog

The *Search* dialog can be activated either by clicking on the binocular icon labeled Search in the Home 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

Packet Analyzer personal edition 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)
```

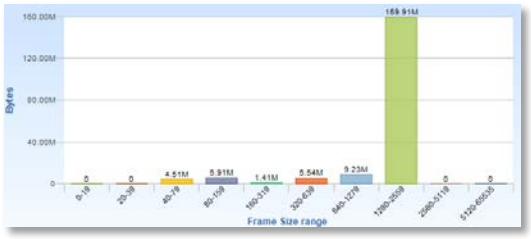
Security Disclosures

Please carefully read the following important disclosures.

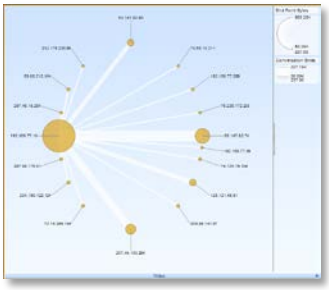
- Unlike with Wireshark, once a valid decryption key is defined, all relevant subsequent traffic is automatically decrypted, and, if saved, will be stored decrypted to disk.
- Regardless of whether decryption keys are shown or hidden, they are stored on disk in plain text. Exporting a configuration file will export the plain text decryption keys that have been entered.

Appendix A Chart Types

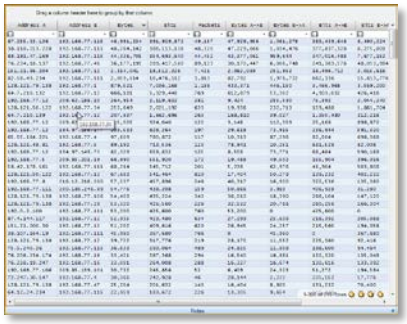
The names for the various chart types are as follows.



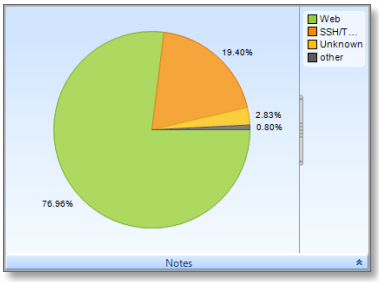
Bar Chart



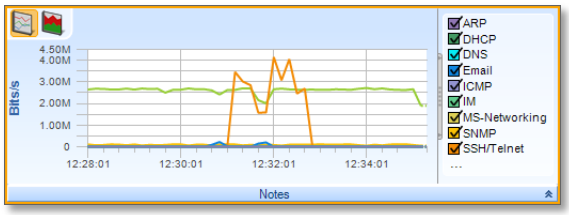
Conversation Ring



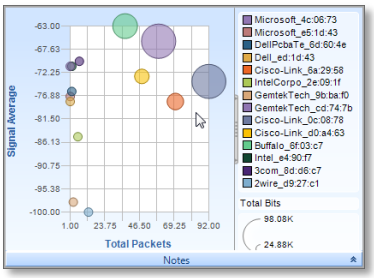
Data Grid



Pie Chart

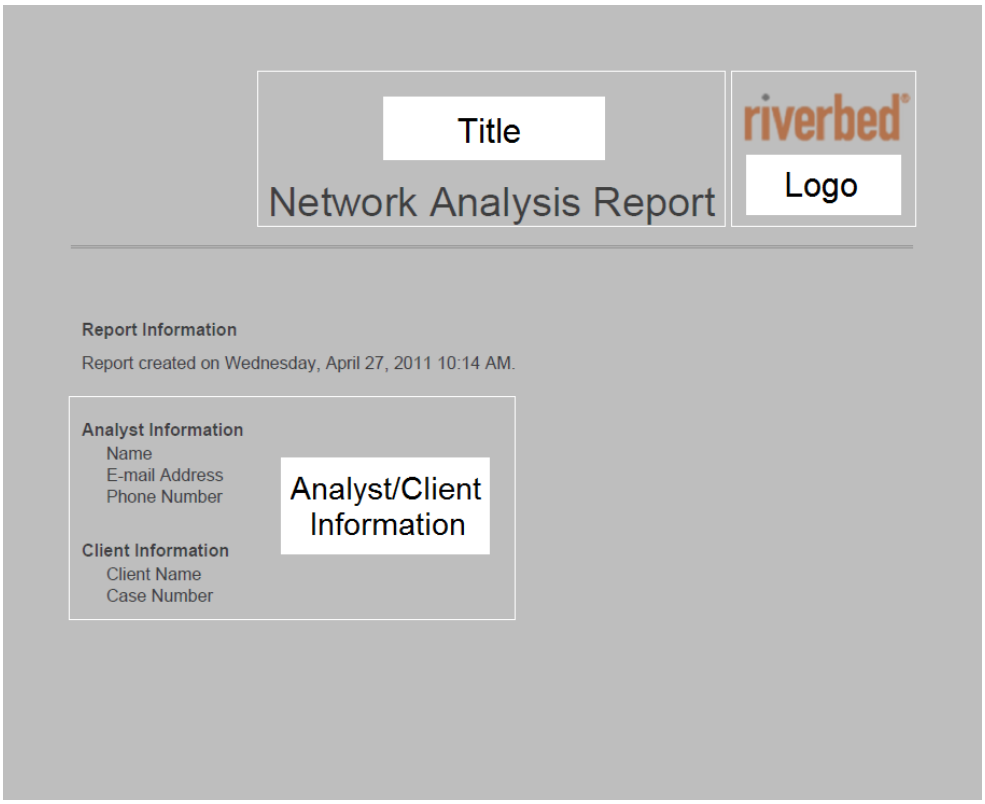


Strip Chart

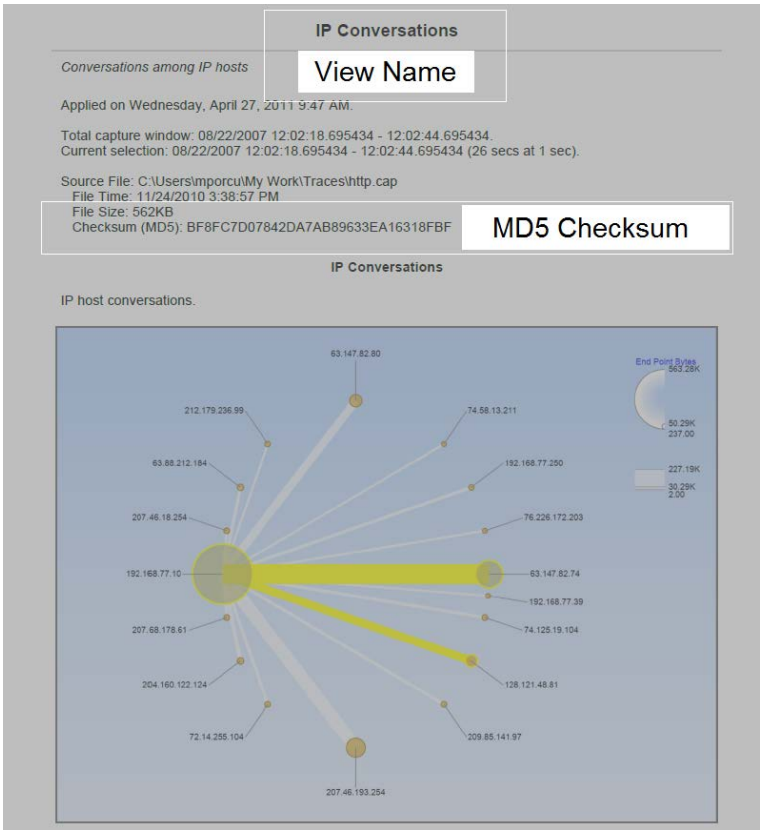


Scatter Plot

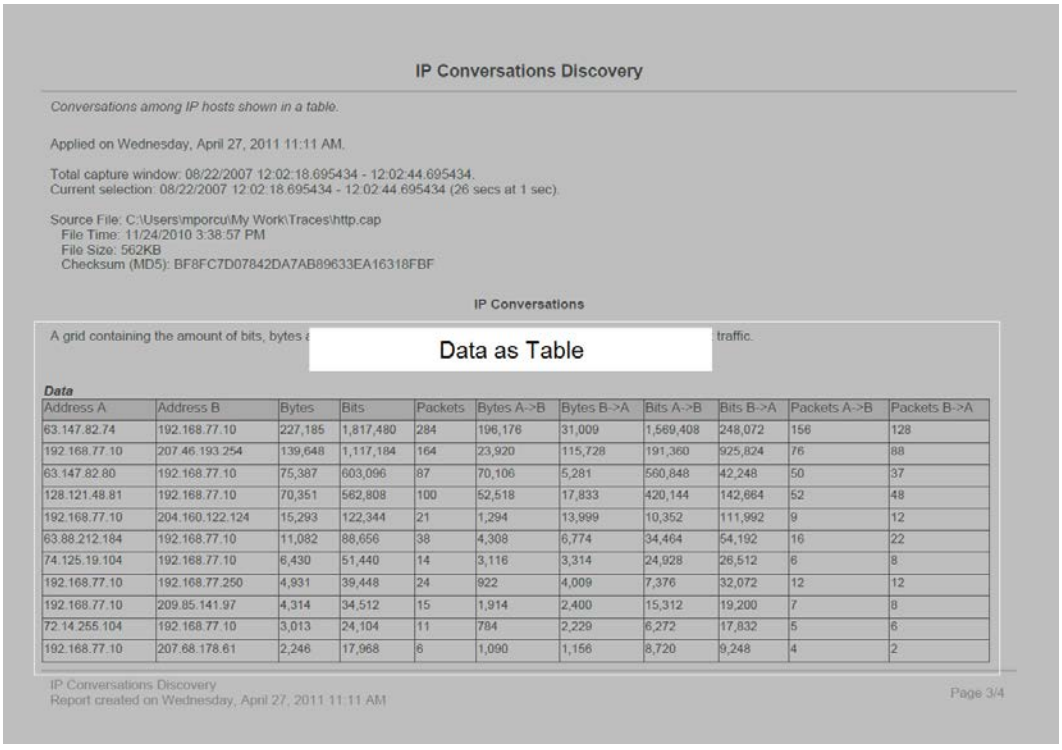
Appendix B Report Example Breakdown



Report layout



IP Conversations layout



IP Conversations Discovery layout

Riverbed Technology
680 Folsom St.
San Francisco, CA 94107

Phone: 415 247 8800
Fax: 415 247 8801
www.riverbed.com