TAKE CONTROL
IT'S YOUR SECURITY

TAMOSOFT

CommView® for WiFi

Wireless Network Monitor and Analyzer

Help Documentation
Version 7.3

Contents

Introduction

About CommView for WiFi

CommView for WiFi is a special edition of CommView designed for capturing and analyzing network packets on wireless 802.11 a/b/g/n/ac/ax networks. CommView for WiFi gathers information from the wireless adapter and decodes the analyzed data.

With CommView for WiFi, you can see the list of network connections and vital IP statistics and examine individual packets. Packets can be decrypted utilizing user-defined WEP or WPA-PSK keys and are decoded down to the lowest layer, with full analysis of the most widespread protocols. Full access to raw data is also provided. Captured packets can be saved to log files for future analysis. A flexible system of filters makes it possible to drop unnecessary packets or capture the essential packets. Configurable alarms can notify the user about important events such as suspicious packets, high bandwidth utilization, or unknown addresses.

CommView for WiFi includes a VoIP module for in-depth analysis, recording, and playback of SIP and H.323 voice communications.

CommView for WiFi is a helpful tool for WLAN administrators, security professionals, network programmers, or anyone who wants to see the full picture of their WLAN traffic. This application requires a compatible wireless network adapter. For the list of supported adapters, please visit our Web site.

What's New

Version 7.3

- Per-packet info on MCS index, channel width, guard interval, and number of streams.
- New capture log format, NCFX.
- Support for Killer Wi-Fi 6 AX1650w, AX1650x, and AX1650s adapters.

Version 7.2

- Improved identification of WLAN encryption and authorization methods.
- Support for 802.11ax adapters
- New icons.

Version 7.1

- Quick filters for the Nodes and Channels tabs: filter packets by node, channel, packet type, or data rate with a single click.
- Support for Windows 10.
- Updated IP allocation map and MAC-to-vendor database.

Version 7.0

- A major interface update: new Nodes and Channels tabs, new charts and statistics.
- Integration with Wi-Spy for spectrum analysis.

Version 6.5

- A completely reworked protocol decoder: more supported protocols and a summary for each packet.

Version 6.3

- Support for USB adapters: Ubiquiti SR71-USB (802.11 a/b/g/n), Proxim ORiNOCO 8494 (802.11 a/b/g/n), TP-Link TL-WN821N (802.11 b/g/n), NETGEAR WN111 v2 (802.11 b/g/n).

Version 6.2

- New wireless adapters supported (Windows Vista or 7 required): Intel 3945, 4965, 5100, 5150, 5300, 5350.
- UDP stream reconstruction.
- A few improvements in the protocol decoder.

Version 6.1

- New operating systems supported: Windows XP 64-bit Edition, Windows Vista 64-bit Edition, Windows Server 2008 32-bit and 64-bit Editions.
- Decreased RAM utilization in the VoIP analysis module. The new version can handle more simultaneous calls using less RAM.
- Adjustable jitter buffer for realistic simulation of real-live VoIP phone sound quality.
- Improved "Find" dialog: Search direction and Unicode search (UTF-8, UTF-16) are now supported.

- Noise level is now displayed on the "Channels" tab.
- More flexible decoder tree options: You can now set the number of nodes to be expanded.
- Many other improvements and bug fixes.

Version 6.0

- VoIP module for advanced in-depth analysis, recording, and playback of SIP and H.323 voice communications.
- Visual TCP session analysis that graphically displays session diagrams.
- Visual packet builder that facilitates packet construction in Packet Generator.

Using the Program

Driver Installation

CommView for WiFi is a tool for monitoring wireless 802.11 a/b/g/n/ac/ax networks. You must have a compatible wireless adapter to use this product. In order to enable the monitoring features of your wireless adapter, you will need to use the special drivers that come with this product. When CommView for WiFi is not running, your adapter will be able to connect and communicate with other wireless hosts or access points, as it normally does. When CommView for WiFi is running, your adapter will be put in passive, promiscuous monitoring mode with no connectivity.

Prior to installing the new driver for your wireless adapter, be sure that your adapter is compatible with this product. The list of compatible adapters can be found at the following URL:

http://www.tamos.com/products/commwifi/

CommView for WiFi may support other adapters. If your adapter is not listed above, please refer to the FAQ chapter for up-to-date information.

For detailed, illustrated driver installation instructions, please launch the program, click **Help => Driver Installation Guide** in the program's menu, and scroll down to the bottom of the window.

Overview

The program interface consists of several tabs that allow you to view data and perform various actions with captured packets. The functionality of these tabs is described in the table below.

Tab Name	Description
Nodes	Controls packet capture, displays detailed information on access points and associated stations, channel utilization statistics, and graphical representation of the wireless spectrum.
Channels	Displays detailed per-channel statistics, as well as the top nodes, Mbytes per second, and packets per second charts.
Latest IP Connections	Displays detailed information on the latest IP connections between the WLAN nodes. This information is available when the WLAN being monitored does not use encryption or when you have entered the correct WPA or WEP key.
Packets	Lists captured packets; allows you to examine them and view their contents.
VoIP	Provides in-depth VoIP analysis of the captured traffic. Note that this tab is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.
Logging	Allows you to save captured packets to log files in a number of formats and configure automatic logging.
Rules	Provides access to packet filters that allow you to capture/ignore packets based on various criteria, such as IP address or port number.
Alarms	Allows you to create alarms that can notify you about important events, such as suspicious packets, high bandwidth utilization, unknown addresses, etc.

You can change some of the settings, such as fonts, colors, and buffer size by selecting Settings from the menu. For more information, see Setting Options.

Main Menu

The application menu commands are described below.

File

Start/Stop Capture – starts/stops capturing packets.
Suspend/Resume Packet Output – stops/resumes the real-time packet output on the **Packets** tab.
Remote Monitoring Mode – shows or hides the remote monitoring toolbar that allows you to connect to remote capture devices: Remote Agent for WiFi, RPCAP, or Aruba Remote Capture.
Save Nodes As – allows you to save the contents of the Nodes tab.
Save Channels As – allows you to save the contents of the Channels tab.
Save Latest IP Connections As – allows you to save the contents of the Latest IP Connections tab.
Save Packet Log As – allows you to save the contents of the Packets tab in different formats. Use the Logging tab for advanced saving options.
Log Viewer – opens a new Log Viewer window.
VoIP Log Viewer – opens a new VoIP Log Viewer window.
Clear Nodes – clears the **Nodes** tab.
Clear Channels – clears the **Channels** tab.
Clear Latest IP Connections – clears the **Latest IP Connections** tab.
Clear Packet Buffer – clears the contents of the program's buffer and the **Packets** tab.
Clear VoIP Data – clears the contents of the **VoIP** tab.
Performance Data – displays the program's performance statistics: the number of packets captured and dropped by the device driver.
Exit – closes the program.

Search

Find Packet – shows a dialog that allows you to find packets matching a specific text.
Go to Packet Number - shows a dialog that allows you to jump to a packet with the specified number.

View

Statistics – shows a window with data transfer and protocol distribution statistics.
Port Reference – shows a window with port reference information.
Log Directory – opens the directory to which logs are saved by default.
Nodes Columns – shows/hides the Nodes tab columns.
Channels Columns – shows/hides the Channels tab columns.
Latest IP Connections Columns – shows/hides the Latest IP Connections tab columns.
Packets Columns – shows/hides the Packets tab columns.
Channels and Spectrum – shows/hides the Channels and Spectrum pane at the bottom of the Nodes tab.

Tools

Packet Generator – opens the Packet Generator window.
Reconstruct TCP Session – allows you to reconstruct a TCP session starting from the selected packet; it opens a window that displays the entire conversation between two hosts.
Reconstruct UDP Stream – allows you to reconstruct a UDP stream starting from the selected packet; it opens a window that displays the entire conversation between two hosts.
NIC Vendor Identifier – opens a window where you can identify a network adapter vendor by MAC address.
Scheduler – allows you to add or remove scheduled capturing tasks.
Node Reassociation – opens the Node Reassociation window.

Settings

Fonts – shows the submenu for setting the fonts of the interface elements.
WEP/WPA Keys – opens a window that allows you to enter WEP/WPA keys.
MAC Aliases – brings up a window where you can assign easy-to-remember aliases to MAC addresses.
IP Aliases – brings up a window where you can assign easy-to-remember aliases to IP addresses.
Options – brings up the Options window where additional advanced program options can be set.
Language – allows you to change the interface language. Be sure to restart the program once you have changed the language. The CommView for WiFi installation package may not include all available language files for the interface. Clicking on the **Other Languages** menu item opens the additional languages download page on our Web site where you can download your language file if it is available for the current version.

Rules

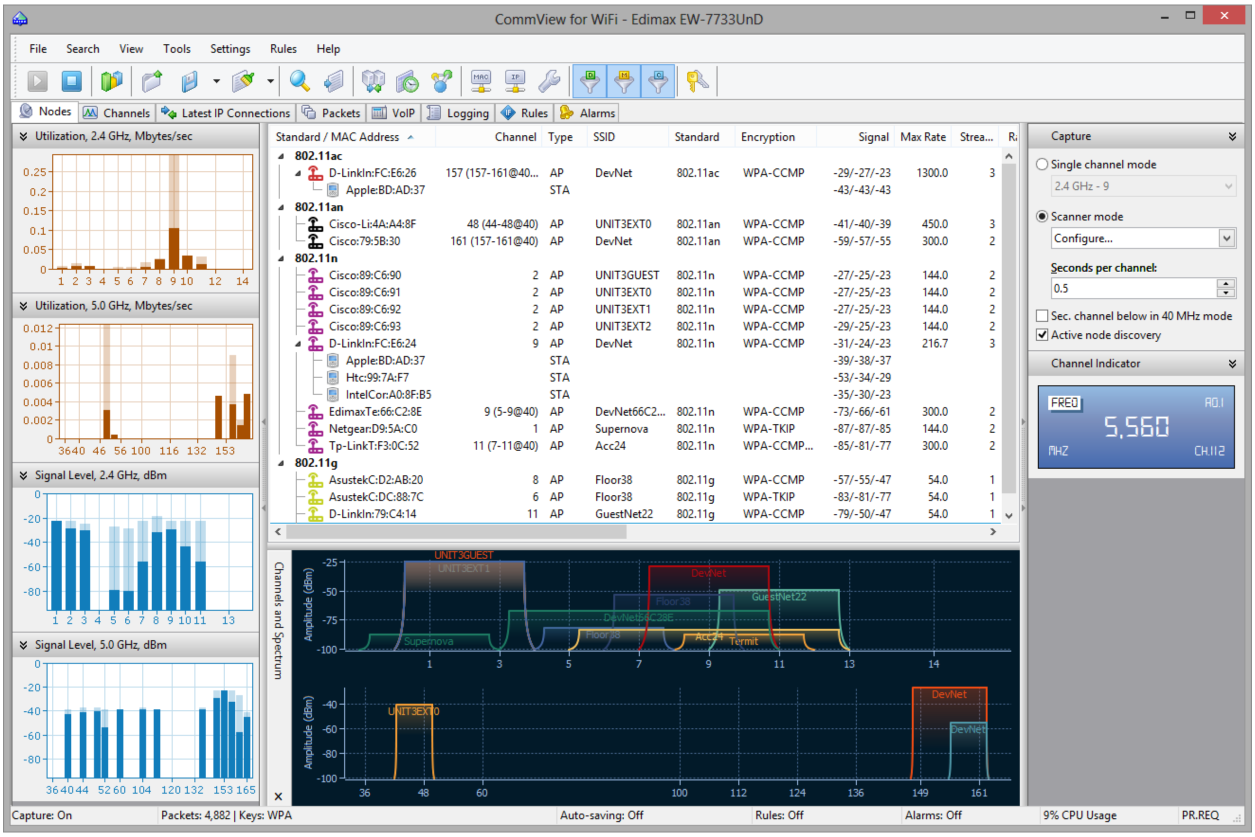
Capture Data Packets – check or uncheck this item to enable/disable capturing of packets of the type "Data."
Capture Management Packets – check or uncheck this item to enable/disable capturing of packets of the type "Management."
Capture Control Packets – check or uncheck this item to enable/disable capturing of packets of the type "Control."
Ignore Beacons - check or uncheck this item to enable/disable capturing of management packets of the type "Beacon."
Save Current Rules As – allows you to save current rules configuration to a file.
Load Rules From – allows you to load a previously saved rules configuration from a file.
Reset All – clears all existing rules (if any).

Help

Contents – launches CommView for WiFi help.
Search For Help On… – shows CommView for WiFi help index.
Driver Installation Guide… – shows detailed driver installation instructions.
Check for an Update on the Web – opens the update wizard. Please follow the instructions on the screen to download and install the latest upgrade for CommView for WiFi from the TamoSoft Web site.
Activation – allows you to activate your software license or check the current activation status.
About – shows information about the program.

Nodes

This is the main application tab that is used for controlling packet capture, displaying detailed information on access points and associated stations, channel utilization statistics, and graphical representation of the wireless spectrum.



Standard / MAC Address	Channel	Type	SSID	Standard	Encryption	Signal	Max Rate	Strea...
802.11ac								
D-LinkIn:FC:E6:26	157 (157-161@40...	AP	DevNet	802.11ac	WPA-CCMP	-29/-27/-23	1300.0	3
Apple:BD:AD:37		STA				-43/-43/-43		
802.11an								
Cisco-Li:4A:A4:8F	48 (44-48@40)	AP	UNIT3EXT0	802.11an	WPA-CCMP	-41/-40/-39	450.0	3
Cisco:79:5B:30	161 (157-161@40)	AP	DevNet	802.11an	WPA-CCMP	-59/-57/-55	300.0	2
802.11n								
Cisco:89:C6:90	2	AP	UNIT3GUEST	802.11n	WPA-CCMP	-27/-25/-23	144.0	2
Cisco:89:C6:91	2	AP	UNIT3EXT0	802.11n	WPA-CCMP	-27/-25/-23	144.0	2
Cisco:89:C6:92	2	AP	UNIT3EXT1	802.11n	WPA-CCMP	-27/-25/-23	144.0	2
Cisco:89:C6:93	2	AP	UNIT3EXT2	802.11n	WPA-CCMP	-29/-25/-23	144.0	2
D-LinkIn:FC:E6:24	9	AP	DevNet	802.11n	WPA-CCMP	-31/-24/-23	216.7	3
Apple:BD:AD:37		STA				-39/-38/-37		
Htc:99:7A:F7		STA				-53/-34/-29		
IntelCor:A0:8F:B5		STA				-35/-30/-23		
EdimaxTe:66:C2:8E	9 (5-9@40)	AP	DevNet66C2...	802.11n	WPA-CCMP	-73/-66/-61	300.0	2
Netgear:D9:5A:C0	1	AP	Supernova	802.11n	WPA-TKIP	-87/-87/-85	144.0	2
Tp-LinkT:F3:0C:52	11 (7-11@40)	AP	Acc24	802.11n	WPA-CCMP...	-85/-81/-77	300.0	2
802.11g								
AsustekC:D2:AB:20	8	AP	Floor38	802.11g	WPA-CCMP	-57/-55/-47	54.0	1
AsustekC:DC:88:7C	6	AP	Floor38	802.11g	WPA-TKIP	-83/-81/-77	54.0	1
D-LinkIn:79:C4:14	11	AP	GuestNet22	802.11g	WPA-CCMP	-79/-50/-47	54.0	1

Capture

○ Single channel mode
2.4 GHz - 9

● Scanner mode
Configure...

Seconds per channel:
0.5

□ Sec. channel below in 40 MHz mode
☑ Active node discovery

Capture: On | Packets: 4,882 | Keys: WPA | Auto-saving: Off | Rules: Off | Alarms: Off | 9% CPU Usage | PR.REQ

This window consists of several resizable panes that are overviewed below.

Capture and Channel Indicator Panes

This **Capture** pane allows you to choose between the two capturing modes: **Single channel mode** or **Scanner mode**. If you select the **Single channel mode**, the application captures packets on a single channel (or several channels, if you use several supported USB cards; more information is given below) that you can select from the drop-down list. If you select the **Scanner mode**, the application will sweep through the channels in a loop, i.e. it will capture on the first channel, switch to the next channel thereafter, and so forth, until it reaches the last channel, after which a new scanning cycle will begin. To configure the set of channels to be scanned, click **Configure** and use the check boxes to select or unselect specific channels. Depending on the country and regulatory domain set in your adapter, the list of supported channels may vary. This is discussed in the FAQ chapter in detail. To configure the time the application spends on each channel, use the **Seconds per channel** edit box.

You can also see two other options at the bottom of this pane that control packet capture. The **Sec. channel below in 40 MHz mode** check box determines the position of the secondary channel when channel bonding is used in the 2.4 GHz band. By default, the secondary channel in 40 MHz 802.11 networks has a higher frequency than the primary channel. If you are capturing packets in a network environment that has a lower frequency secondary channel, check this box. Checking this box has no effect if the secondary channel cannot be positioned below the primary one, which is the case when, for example, you are capturing on 2.4 GHz channel 1, 2, 3, or 4. This option is available only if your adapter supports capturing on 40 MHz channels. The **Active node discovery** box makes the application send PROBE REQUEST packets periodically. Such packets facilitate the discovery of those APs that do not broadcast their SSID. This option is available only if your adapter supports packet generation.

Once you have configured the capture options, click the **Start Capture** button on the tool bar. If you want to switch to a new channel while you are in the **Single channel mode** or switch to the **Scanner mode**, you can do so without stopping capturing. The **Channel Indicator** pane displays the current channel and frequency while the application is capturing packets.

Using Multiple Adapters for Multi-Channel Capturing

If you need to capture packets on multiple channels simultaneously, you can do so by using multiple USB adapters. In this mode, the channel selection drop-down list becomes a multi-select control that allows you to select several channels by holding down the **Ctrl** key. The **Channel Indicator** pane will then display several channel/frequency indicators. Note that using multiple adapters is supported only for a limited set of adapter models. Please refer to the Multi-channel Capturing chapter for the detailed information.

Node List

Once you have started capturing, the program begins to populate the node list with detected wireless nodes. The packet analysis mechanism used in the program lists all the access points found on the given channel(s) and stations in ad hoc mode, as well as associated stations in infrastructure mode. It is important to understand that the radio used in a wireless adapter can receive data on only one channel at a time. Therefore, when you have selected a certain channel for monitoring, this table will contain data on the APs and stations transmitting data on the selected channel only. You can, however, select a different channel without resetting data in the table or select the **Scanner mode** to make the application sweep through the channels so that you can see active nodes on different channels.

The meaning of the table columns is explained below:

SSID/Band/Channel – Depending on the grouping method that you selected (accessible via the **Group by** context menu), the first column lists wireless nodes grouped by SSID, 802.11 standard, or channel. Each wireless node is represented by its MAC addresses or alias. The stations associated to APs are shown as "child" items linked to the "parent" item representing the AP.
Channel – the channel the given AP works on. If the AP uses channel bonding (40, 80, or 160 MHz channels), the primary channel is listed first, followed by information on the additional channels in parentheses.
Type – node type. Possible values are AP (for access points), STA (for stations in infrastructure mode) and AD HOC (for stations in ad hoc mode).
SSID – Service Set Identifier; a unique string that differentiates one WLAN from another.
Standard – 802.11 standard of the AP. Possible values are 802.11a, 802.11b, 802.11g, 802.11n, 802.11an, and 802.11ac.
Encryption – shows whether the node is using WEP or WPA encryption. For access points, this column shows available encryption methods being "advertised" by the access point.
Signal – signal level in the min/average/max format. The average value is calculated since the data in this table was last reset. Please refer to the Understanding Signal Strength chapter for more information.
Max Rate – the maximum PHY data rate the AP can provide.
Streams – the number of spatial streams supported by the AP.
Rate (Tx and **Rx)** – data transfer rate in the min/average/max format. The average value is calculated since the data in this table was last reset.

Bytes (Tx and **Rx)** – the number of bytes sent and received by the node.
Packets (Tx and **Rx)** – the number of packets sent and received by the node.
Retry (Tx and **Rx)** – the number of packets where the Retry flag was set.
Fragmented (Tx and **Rx)** – the number of packets where the Fragmented flag was set.

You can show or hide individual columns by right-clicking on list header or using the **View** => **Nodes Columns** menu. The column order can be changed by dragging the column header to a new location. Right-clicking on the node list brings up a menu with the following commands:

Details – displays an AP and Station Details window.
Quick Filter – finds the packets sent to/from the selected node, as well as the packets where the MAC address of the selected node equals the BSSID address, and displays them in a new window.
Copy MAC Address – copies the selected node MAC address to the clipboard.
Create Alias – displays a window where you can assign an easy-to-remember alias to the selected MAC address.
Save Nodes As – allows you to save the contents of the Nodes tab as an HTML report.
Clear Nodes – clears the table.
More Statistics – shows a window with data transfer and protocol distribution statistics.
Group by – groups the list by SSID, channel, or band.

Utilization and Signal Level Panes

Located on the left side of the **Nodes** tab, these panes display per-channel utilization charts (two separate charts for 2.4 GHz and 5 GHz channels) and per-channel signal level charts (again, two separate charts for 2.4 GHz and 5 GHz channels). In addition to the current levels, these charts also display historic high levels, which are illustrated in a pale color.

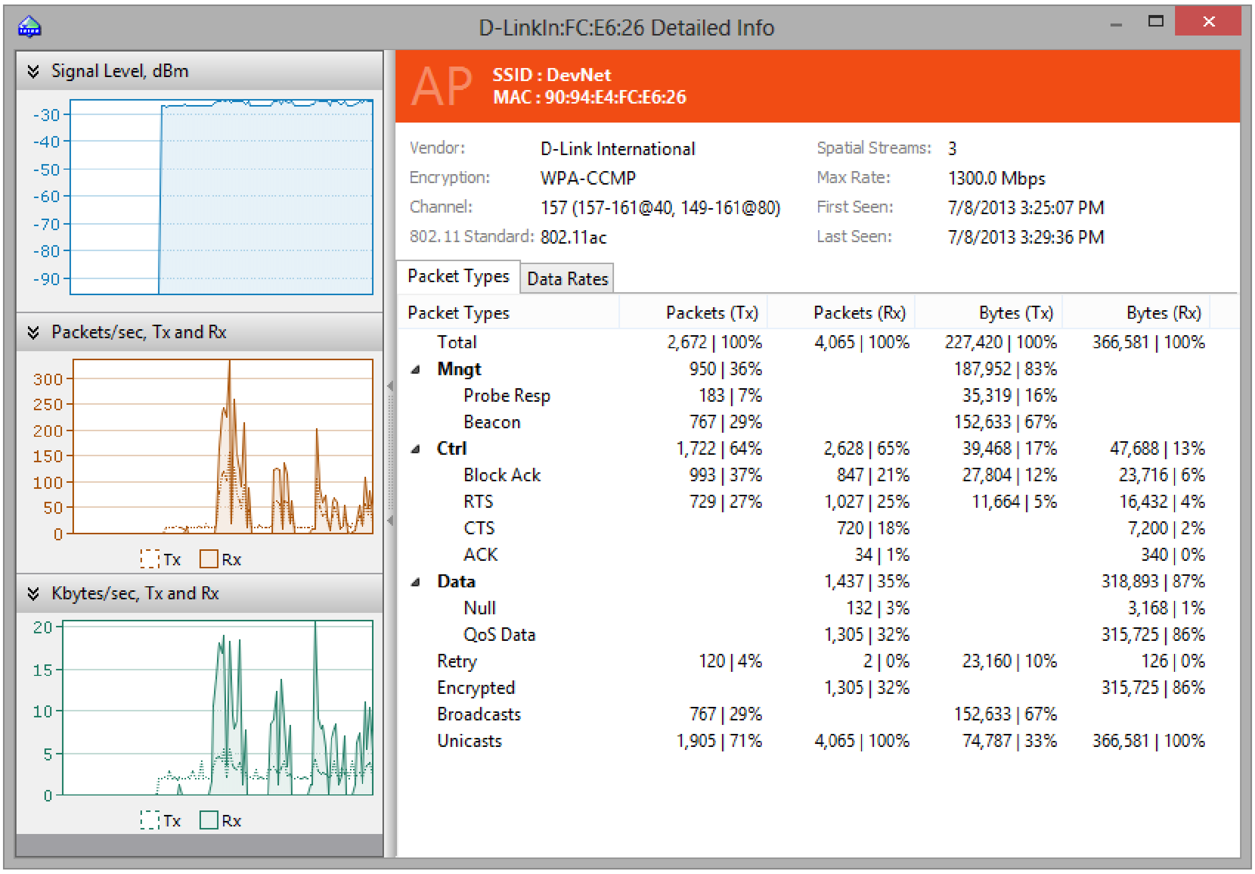
Channels and Spectrum Pane

Located at the bottom of the **Nodes** tab, this pane has dual functionality:

- It provides a graphical representation of the active APs, where each AP is shown using a line that approximates its spectrum mask. The mask width depends on the channel width supported by the AP and the mask height depends on the current signal strength.
- It can display spectrum data if you plug in a USB-based spectrum analyzer, Wi-Spy by MetaGeek. A spectrum analyzer listens to and analyzes the frequency bands utilized by Wi-Fi devices. Because these bands are unlicensed, they are often shared with non-Wi-Fi sources of RF signals, such as wireless video cameras, microwave ovens, or cordless phones, which cause interference. The purpose of spectrum analysis is to detect and identify such sources of interference, eliminate them, and/or identify the WLAN channels with minimal interference. For more information, please refer to the Spectrum Analysis chapter.

AP and Station Details Window

When you double-click on an AP or a station shown on the Nodes tab, CommView for WiFi displays a window that contains detailed data on the selected node, as illustrated below.



SSID : DevNet
MAC : 90:94:E4:FC:E6:26

Vendor: D-Link International
Encryption: WPA-CCMP
Channel: 157 (157-161@40, 149-161@80)
802.11 Standard: 802.11ac
Spatial Streams: 3
Max Rate: 1300.0 Mbps
First Seen: 7/8/2013 3:25:07 PM
Last Seen: 7/8/2013 3:29:36 PM

Packet Types | Data Rates

Packet Types	Packets (Tx)	Packets (Rx)	Bytes (Tx)	Bytes (Rx)
Total	2,672 | 100%	4,065 | 100%	227,420 | 100%	366,581 | 100%
Mngt	950 | 36%		187,952 | 83%	
Probe Resp	183 | 7%		35,319 | 16%	
Beacon	767 | 29%		152,633 | 67%	
Ctrl	1,722 | 64%	2,628 | 65%	39,468 | 17%	47,688 | 13%
Block Ack	993 | 37%	847 | 21%	27,804 | 12%	23,716 | 6%
RTS	729 | 27%	1,027 | 25%	11,664 | 5%	16,432 | 4%
CTS		720 | 18%		7,200 | 2%
ACK		34 | 1%		340 | 0%
Data		1,437 | 35%		318,893 | 87%
Null		132 | 3%		3,168 | 1%
QoS Data		1,305 | 32%		315,725 | 86%
Retry	120 | 4%	2 | 0%	23,160 | 10%	126 | 0%
Encrypted		1,305 | 32%		315,725 | 86%
Broadcasts	767 | 29%		152,633 | 67%	
Unicasts	1,905 | 71%	4,065 | 100%	74,787 | 33%	366,581 | 100%

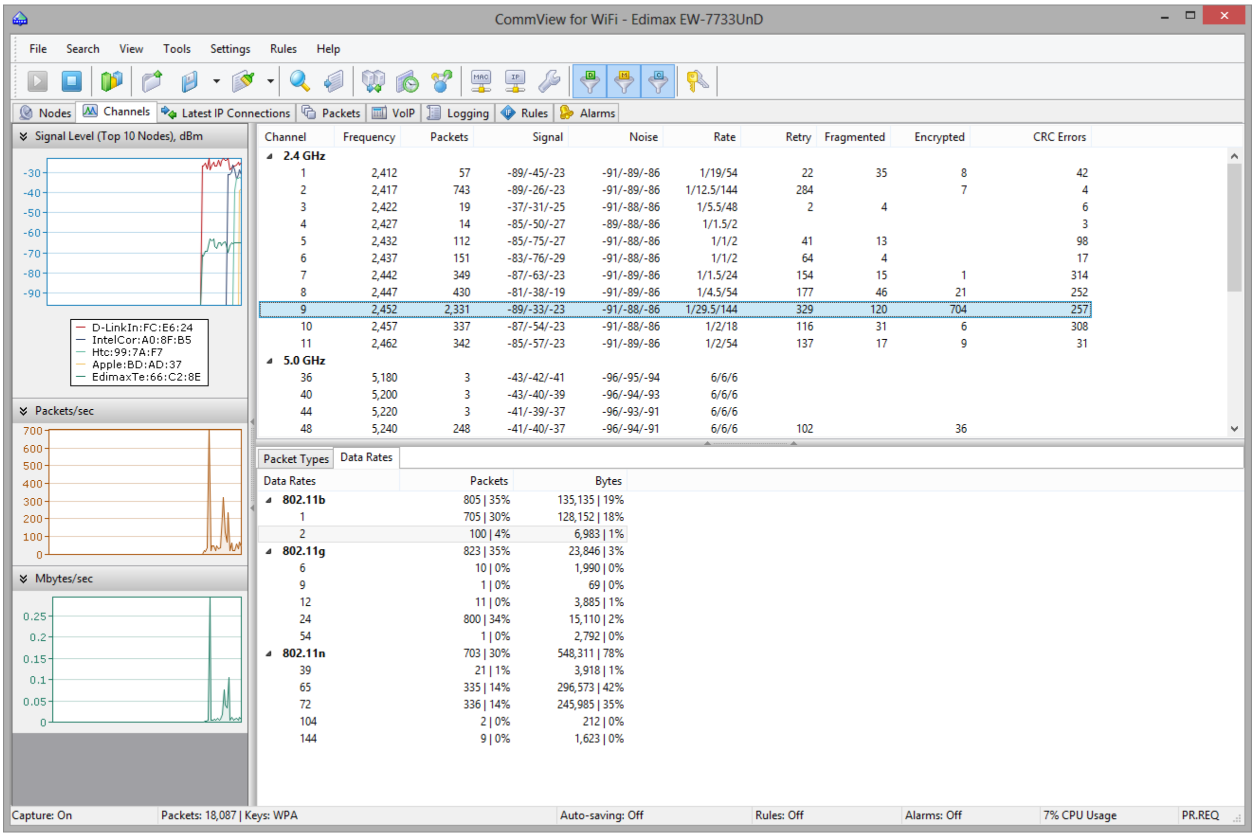
The top pane displays the type, MAC address, and SSID of the selected node, followed by other key details, such as channel, first seen and last seen times, etc. This pane uses the same color that is used to display the selected AP on the **Channels and Spectrum** pane of the main application window.

On the bottom pane, you can see **Packet Types** and **Data Rates** tables. These tables display detailed statistics for the selected channel based on the packet types and subtypes and on the data rates.

On the left pane, you can see three charts: **Signal Level**, **Packets/sec**, and **Mbytes/sec**. The **Signal Level** chart displays the signal level for the given node. The **Packets/sec** and **Mbytes/sec** charts show the number of packets and Mbytes per second sent to/from the given node. Note that these charts are updated only when the application actually captures data on the channel on which the given node is working. This means that if, for example, you are capturing data on channel 5 and the selected AP is also working on channel 5, then the charts will be constantly updated. However, if you are using the **Scanner Mode**, the charts will be updated every time the application sweeps through the channel on which the given AP is working.

Channels

This tab displays per-channel statistics for all the channels that have been or are being monitored. The number of channels shown in this table depends on the way you use CommView for WiFi. Normally, when you monitor only one channel used by your WLAN, the table will solely contain data on the selected channel, because the radio used in a wireless adapter can receive data on only one channel at a time. Once you have selected a different channel for monitoring, another channel will be added to the table. If you select the **Scanner mode** on the **Nodes** tab, the table will contain data on all the scanned channels for which at least one packet has been captured.



Channel	Frequency	Packets	Signal	Noise	Rate	Retry	Fragmented	Encrypted	CRC Errors
2.4 GHz									
1	2,412	57	-89/-45/-23	-91/-89/-86	1/19/54	22	35	8	42
2	2,417	743	-89/-26/-23	-91/-89/-86	1/12.5/144	284		7	4
3	2,422	19	-37/-31/-25	-91/-88/-86	1/5.5/48	2	4		6
4	2,427	14	-85/-50/-27	-89/-88/-86	1/1.5/2				3
5	2,432	112	-85/-75/-27	-91/-88/-86	1/1/2	41	13		98
6	2,437	151	-83/-76/-29	-91/-88/-86	1/1/2	64	4		17
7	2,442	349	-87/-63/-23	-91/-89/-86	1/1.5/24	154	15	1	314
8	2,447	430	-81/-38/-19	-91/-89/-86	1/4.5/54	177	46	21	252
9	2,452	2,331	-89/-33/-23	-91/-88/-86	1/29.5/144	329	120	704	257
10	2,457	337	-87/-54/-23	-91/-88/-86	1/2/18	116	31	6	308
11	2,462	342	-85/-57/-23	-91/-89/-86	1/2/54	137	17	9	31
5.0 GHz									
36	5,180	3	-43/-42/-41	-96/-95/-94	6/6/6				
40	5,200	3	-43/-40/-39	-96/-94/-93	6/6/6				
44	5,220	3	-41/-39/-37	-96/-93/-91	6/6/6				
48	5,240	248	-41/-40/-37	-96/-94/-91	6/6/6	102		36	

Data Rates	Packets	Bytes
802.11b	805 | 35%	135,135 | 19%
1	705 | 30%	128,152 | 18%
2	100 | 4%	6,983 | 1%
802.11g	823 | 35%	23,846 | 3%
6	10 | 0%	1,990 | 0%
9	1 | 0%	69 | 0%
12	11 | 0%	3,885 | 1%
24	800 | 34%	15,110 | 2%
54	1 | 0%	2,792 | 0%
802.11n	703 | 30%	548,311 | 78%
39	21 | 1%	3,918 | 1%
65	335 | 14%	296,573 | 42%
72	336 | 14%	245,985 | 35%
104	2 | 0%	212 | 0%
144	9 | 0%	1,623 | 0%

Because the 802.11 standard uses overlapping channel frequencies in the 2.4 GHz band, you might notice that even if your WLAN is configured to use only one channel, e.g. 6, you will still see non-zero values for the adjacent channels. Unlike 2.4 GHz channels, 5 GHz channels do not overlap.

On the bottom pane, you can see **Packet Types** and **Data Rates** tables. These tables display detailed statistics for the selected channel based on the packet types and subtypes and on the data rates.

On the left pane, you can see three charts: **Signal Level**, **Packets/sec**, and **Mbytes/sec**. The **Signal Level** chart displays the signal level for the top ten nodes found on the selected channel. The **Packets/sec** and **Mbytes/sec** charts show the number of packets and Mbytes per second captured on the selected channel. When working with information provided on these charts, please note the following:

- The charts display data for the selected channel only.
- The charts are updated only when the application actually captures data on the select channel. This means that if, for example, you are capturing data on channel 2 and select channel 2 from the channel list, the charts will be constantly updated. If you select channel 3, the charts will be "frozen." If you work In **Scanner**

Mode and select any channel, the charts will be updated every time the application sweeps through the selected channel.

The meaning of the channels table columns is explained below:

Channel – channel number.
Frequency – channel frequency in MHz.
Packets – the total number of captured packets.
Signal – signal level in the min/average/max format. The average value is calculated since the data in this table was last reset. Please refer to the Understanding Signal Strength chapter for more information.
Noise – noise level in the min/average/max format. The average value is calculated since the data in this table was last reset. Noise information may not be available from all adapters. If your adapter does not support it, this column will not be visible.
Rate – data transfer rate in the min/average/max format. The average value is calculated since the data in this table was last reset.
Retry – the number of packets where the Retry flag was set.
Fragmented – the number of packets for which the Fragmented flag was set.
Encrypted – the number of Data packets for which the Encrypted flag was set.
CRC Errors – the number of packets with CRC errors. See Understanding CRC and ICV Errors for a detailed explanation.

You can show or hide individual columns by right-clicking on list header or using the **View** => **Channels Columns** menu. The column order can be changed by dragging the column header to a new location. Right-clicking on the channel list brings up a menu with the following commands:

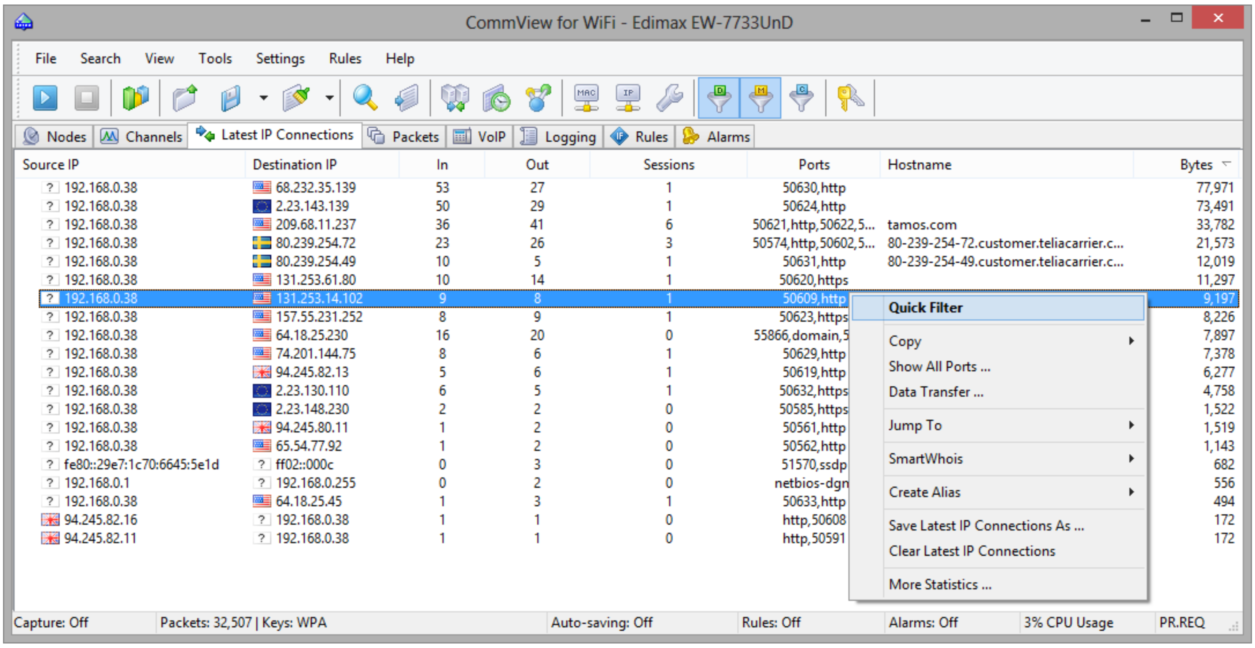
Quick Filter – finds the packets sent on the selected channel and displays them in a new window.
Save Channels As – allows you to save the contents of the Channels tab as an HTML report.
Clear Channels – clears the table.
More Statistics – shows a window with data transfer and protocol distribution statistics.

Right-clicking on the **Packet Types** and **Data Rates** tables brings up a menu with the following command:

Quick Filter – finds the packets with the selected packet type or data rate and displays them in a new window.

Latest IP Connections

This tab is used for displaying detailed information about WLAN connections (IP and IPv6 protocols only). To start capturing packets, select **File = > Start Capture** in the menu, or click on the corresponding button on the toolbar. Please note that this tab will **not** be populated unless the program is capable of decrypting WEP/WPA-encrypted WLAN traffic. If your WLAN uses WEP or WPA encryption, all the data packets being sent are encrypted, and it is impossible to obtain information about their IP address unless you have entered the correct decryption key by clicking **Settings => WEP/WPA Keys** in the menu. Additional steps are required in case of WPA decryption; see Understanding WPA Decryption.



Source IP	Destination IP	In	Out	Sessions	Ports	Hostname	Bytes
? 192.168.0.38	68.232.35.139	53	27	1	50630,http		77,971
? 192.168.0.38	2.23.143.139	50	29	1	50624,http		73,491
? 192.168.0.38	209.68.11.237	36	41	6	50621,http,50622,5...	tamos.com	33,782
? 192.168.0.38	80.239.254.72	23	26	3	50574,http,50602,5...	80-239-254-72.customer.teliacarrier.c...	21,573
? 192.168.0.38	80.239.254.49	10	5	1	50631,http	80-239-254-49.customer.teliacarrier.c...	12,019
? 192.168.0.38	131.253.61.80	10	14	1	50620,https		11,297
? 192.168.0.38	131.253.14.102	9	8	1	50609,http		9,197
? 192.168.0.38	157.55.231.252	8	9	1	50623,https		8,226
? 192.168.0.38	64.18.25.230	16	20	0	55866,domain,5		7,897
? 192.168.0.38	74.201.144.75	8	6	1	50629,http		7,378
? 192.168.0.38	94.245.82.13	5	6	1	50619,http		6,277
? 192.168.0.38	2.23.130.110	6	5	1	50632,https		4,758
? 192.168.0.38	2.23.148.230	2	2	0	50585,https		1,522
? 192.168.0.38	94.245.80.11	1	2	0	50561,http		1,519
? 192.168.0.38	65.54.77.92	1	2	0	50562,http		1,143
? fe80::29e7:1c70:6645:5e1d	? ff02::000c	0	3	0	51570,ssdp		682
? 192.168.0.1	? 192.168.0.255	0	2	0	netbios-dgn		556
? 192.168.0.38	64.18.25.45	1	3	1	50633,http		494
94.245.82.16	? 192.168.0.38	1	1	0	http,50608		172
94.245.82.11	? 192.168.0.38	1	1	0	http,50591		172

Capture: Off | Packets: 32,507 | Keys: WPA | Auto-saving: Off | Rules: Off | Alarms: Off | 3% CPU Usage | PR.REQ

The meaning of the table columns is explained below:

Source IP, Destination IP – shows the pair of IP addresses between which the packets are being sent. The program automatically determines the location of any IP address, and depending on your geolocation settings, may show the country name or flag next to the IP address. For more information, see Setting Options.
In – shows the number of packets received.
Out – shows the number of packets sent.
Sessions – shows the number of established TCP/IP sessions. If no TCP connections were established (connections failed, or the protocol is UDP/IP or ICMP/IP), this value is zero.
Ports – lists the remote computer's ports used during the TCP/IP connection or connection attempt. This list can be empty if the protocol is not TCP/IP. Ports can be displayed either as numeric values or as the corresponding service names. For more information, see Setting Options.
Hostname – shows the remote computer's hostname. If the hostname cannot be resolved, this column is empty.
Bytes – shows the number of bytes transmitted during the session.
Last packet – shows the time of the last packet sent/received during the session.

You can show or hide individual columns by right-clicking on list header or using the **View** => **Latest IP Connections Columns** menu. The column order can be changed by dragging the column header to a new location. Right-clicking on the Latest IP Connections list brings up a menu with the following commands:

Quick Filter – finds the packets sent between the selected IP addresses and displays them in a new window. The same action is performed when you double-click on this window.

Copy – copies the local IP address, remote IP address, or hostname to the clipboard.

Show All Ports – displays a window with the complete list of ports used in communicating between the selected pair of IP addresses. This is useful when many ports were used, and they do not fit into the corresponding column.

Data Transfer – displays a window with information on the data transfer volume between the selected pair of IP addresses and the time of the last packet.

Jump To – allows you to jump to the first/last packet with the selected source/destination IP address; the program will display the Packets tab and set the mouse cursor to the packet that matches the criterion.

SmartWhois – sends the selected source or destination IP address to SmartWhois, if it is installed on your system. SmartWhois is a stand-alone application developed by our company, capable of obtaining information about any IP address or hostname in the world. It automatically provides information associated with an IP address, such as domain, network name, country, state or province, city. The program can be downloaded from our site.

Create Alias – brings up a window where you can assign an easy-to-remember alias to the selected IP address.

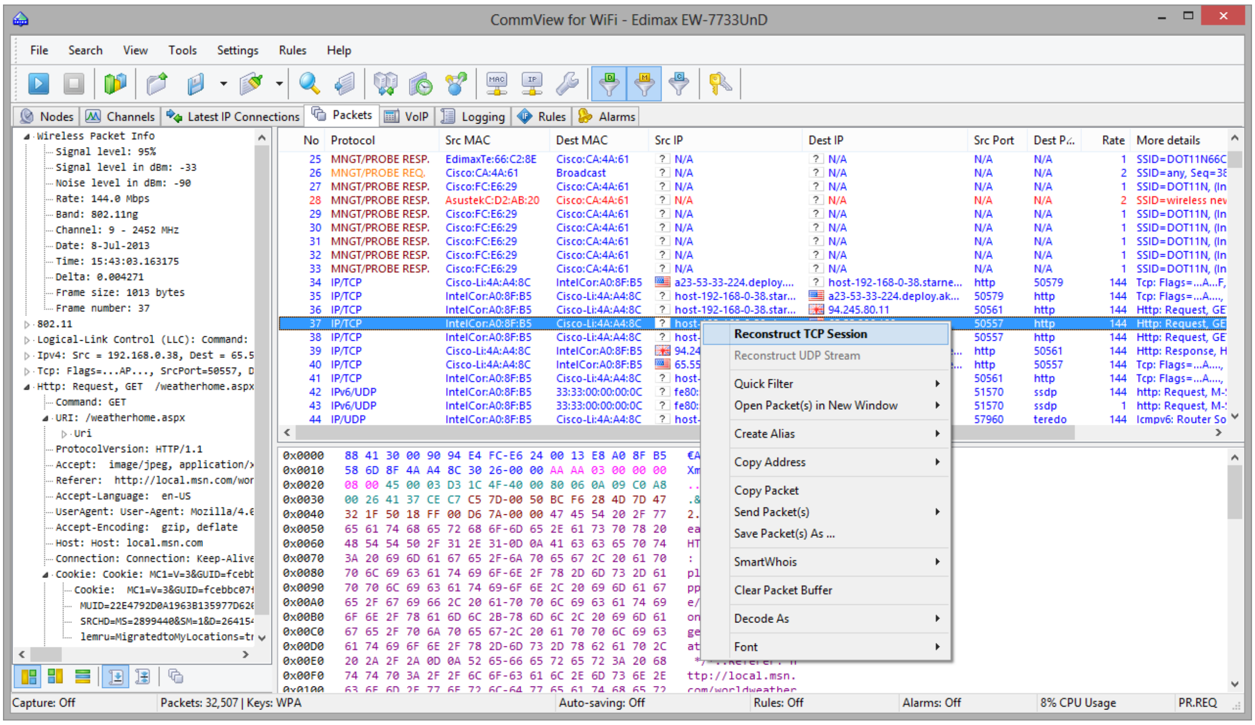
Save Latest IP Connections As – allows you to save the contents of the Latest IP Connections tab as an HTML report.

Clear Latest IP Connections – clears the table.

More Statistics – shows a window with data transfer and protocol distribution statistics.

Packets

This tab is used for listing all captured network packets and displaying detailed information about a selected packet.



```
Wireless Packet Info
    Signal level: 95%
    Signal level in dBm: -33
    Noise level in dBm: -90
    Rate: 144.0 Mbps
    Band: 802.11ng
    Channel: 9 - 2452 MHz
    Date: 8-Jul-2013
    Time: 15:43:03.163175
    Delta: 0.004271
    Frame size: 1013 bytes
    Frame number: 37
802.11
Logical-Link Control (LLC): Command:
Ipv4: Src = 192.168.0.38, Dest = 65.5
Tcp: Flags=...AP..., SrcPort=50557, D
Http: Request, GET  /weatherhome.aspx
    Command: GET
    URI: /weatherhome.aspx
        Uri
    ProtocolVersion: HTTP/1.1
    Accept:  image/jpeg, application/x
    Referer:  http://local.msn.com/wor
    Accept-Language:  en-US
    UserAgent: User-Agent: Mozilla/4.0
    Accept-Encoding:  gzip, deflate
    Host: Host: local.msn.com
    Connection: Connection: Keep-Alive
    Cookie: Cookie: MC1=V=3&GUID=fcebb
        Cookie:  MC1=V=3&GUID=fcebbc07f
        MUID=22E4792D0A1963B135977D62
        SRCHD=MS=2899440&SM=1&D=264154
        lemru=MigratedtoMyLocations=tr
```

No	Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest P...	Rate	More details
25	MNGT/PROBE RESP.	EdimaxTe:66:C2:8E	Cisco:CA:4A:61	? N/A	? N/A	N/A	N/A	1	SSID=DOT11N66C
26	MNGT/PROBE REQ.	Cisco:CA:4A:61	Broadcast	? N/A	? N/A	N/A	N/A	2	SSID=any, Seq=38
27	MNGT/PROBE RESP.	Cisco:FC:E6:29	Cisco:CA:4A:61	? N/A	? N/A	N/A	N/A	1	SSID=DOT11N, (In
28	MNGT/PROBE RESP.	AsustekC:D2:AB:20	Cisco:CA:4A:61	? N/A	? N/A	N/A	N/A	2	SSID=wireless nev
29	MNGT/PROBE RESP.	Cisco:FC:E6:29	Cisco:CA:4A:61	? N/A	? N/A	N/A	N/A	1	SSID=DOT11N, (In
30	MNGT/PROBE RESP.	Cisco:FC:E6:29	Cisco:CA:4A:61	? N/A	? N/A	N/A	N/A	1	SSID=DOT11N, (In
31	MNGT/PROBE RESP.	Cisco:FC:E6:29	Cisco:CA:4A:61	? N/A	? N/A	N/A	N/A	1	SSID=DOT11N, (In
32	MNGT/PROBE RESP.	Cisco:FC:E6:29	Cisco:CA:4A:61	? N/A	? N/A	N/A	N/A	1	SSID=DOT11N, (In
33	MNGT/PROBE RESP.	Cisco:FC:E6:29	Cisco:CA:4A:61	? N/A	? N/A	N/A	N/A	1	SSID=DOT11N, (In
34	IP/TCP	Cisco-Li:4A:A4:8C	IntelCor:A0:8F:B5	a23-53-33-224.deploy....	? host-192-168-0-38.starne...	http	50579	144	Tcp: Flags=...A...F,
35	IP/TCP	IntelCor:A0:8F:B5	Cisco-Li:4A:A4:8C	? host-192-168-0-38.star...	a23-53-33-224.deploy.ak...	50579	http	144	Tcp: Flags=...A....,
36	IP/TCP	IntelCor:A0:8F:B5	Cisco-Li:4A:A4:8C	? host-192-168-0-38.star...	94.245.80.11	50561	http	144	Http: Request, GE
37	IP/TCP	IntelCor:A0:8F:B5	Cisco-Li:4A:A4:8C	? host-		50557	http	144	Http: Request, GE
38	IP/TCP	IntelCor:A0:8F:B5	Cisco-Li:4A:A4:8C	? host-		50557	http	144	Http: Request, GE
39	IP/TCP	Cisco-Li:4A:A4:8C	IntelCor:A0:8F:B5	94.24	...	http	50561	144	Http: Response, H
40	IP/TCP	Cisco-Li:4A:A4:8C	IntelCor:A0:8F:B5	65.55	...	http	50557	144	Tcp: Flags=...A....,
41	IP/TCP	IntelCor:A0:8F:B5	Cisco-Li:4A:A4:8C	? host-		50561	http	144	Tcp: Flags=...A....,
42	IPv6/UDP	IntelCor:A0:8F:B5	33:33:00:00:00:0C	? fe80:		51570	ssdp	144	http: Request, M-!
43	IPv6/UDP	IntelCor:A0:8F:B5	33:33:00:00:00:0C	? fe80:		51570	ssdp	1	http: Request, M-!
44	IP/UDP	IntelCor:A0:8F:B5	Cisco-Li:4A:A4:8C	? host-		57960	teredo	144	Icmpv6: Router So

```
0x0000   88 41 30 00 90 94 E4 FC-E6 24 00 13 E8 A0 8F B5   €A
0x0010   58 6D 8F 4A A4 8C 30 26-00 00 AA AA 03 00 00 00   Xm
0x0020   08 00 45 00 03 D3 1C 4F-40 00 80 06 0A 09 C0 A8   ..
0x0030   00 26 41 37 CE C7 C5 7D-00 50 BC F6 28 4D 7D 47   .&
0x0040   32 1F 50 18 FF 00 D6 7A-00 00 47 45 54 20 2F 77   2.
0x0050   65 61 74 68 65 72 68 6F-6D 65 2E 61 73 70 78 20   ea
0x0060   48 54 54 50 2F 31 2E 31-0D 0A 41 63 63 65 70 74   HT
0x0070   3A 20 69 6D 61 67 65 2F-6A 70 65 67 2C 20 61 70   :
0x0080   70 6C 69 63 61 74 69 6F-6E 2F 78 2D 6D 73 2D 61   pl
0x0090   70 70 6C 69 63 61 74 69-6F 6E 2C 20 69 6D 61 67   pp
0x00A0   65 2F 67 69 66 2C 20 61-70 70 6C 69 63 61 74 69   e/
0x00B0   6F 6E 2F 78 61 6D 6C 2B-78 6D 6C 2C 20 69 6D 61   on
0x00C0   67 65 2F 70 6A 70 65 67-2C 20 61 70 70 6C 69 63   ge
0x00D0   61 74 69 6F 6E 2F 78 2D-6D 73 2D 78 62 61 70 2C   at
0x00E0   20 2A 2F 2A 0D 0A 52 65-66 65 72 65 72 3A 20 68    */*..Referer: h
0x00F0   74 74 70 3A 2F 2F 6C 6F-63 61 6C 2E 6D 73 6E 2E   ttp://local.msn.
```

Capture: Off | Packets: 32,507 | Keys: WPA | Auto-saving: Off | Rules: Off | Alarms: Off | 8% CPU Usage | PR.REQ

The **top table** displays the list of captured packets. Use this list for selecting a packet that you want to have displayed and analyzed. When you select a packet by clicking on it, other panes show information about the selected packet.

The meaning of the table columns is explained below:

No – a unique packet number.
Protocol – shows the packet's protocol.
Src MAC, Dest MAC – shows the source and destination MAC addresses.
BSSID – shows the AP's MAC addresses (where applicable).
Src IP, Dest IP – shows the source and destination IP addresses (where applicable).
Src Port, Dest Port – shows the source and destination ports (where applicable). Ports can be displayed either as numeric values or as the corresponding service names. For more information, see Setting Options.
Time / Delta – shows the packet's absolute or delta time. Delta time is the difference between the absolute times of the last two packets. You can switch from absolute to delta time by clicking **View** =>**Packets Columns** =>**Show Time As**.
Size – shows packet size in bytes. This column is not visible by default.
Signal – shows signal strength in percentile or dBm format. Please refer to the Understanding Signal Strength chapter for more information.
Rate – shows data transfer rate in Megabits per second.
More Details – shows a brief packet summary.
Errors – shows information of the errors. See Understanding CRC and ICV Errors for a detailed explanation. This column is not visible by default.
RA IP – if you use Remote Agent(s) to collect data, displays the IP address of the Remote Agent that captured the corresponding packet.

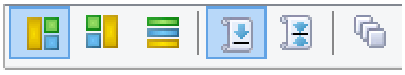
You can show or hide individual columns by right-clicking on list header or using the **View** => **Packets Columns** menu. The column order can be changed by dragging the column header to a new location.

The packet output can be suspended by clicking **File** =>**Suspend Packet Output**. In the Suspended mode, the packets are being captured, but not displayed, on the **Packets** tab. This mode is useful when you are interested only in the statistics rather than individual packets. To resume real-time packets display, click **File** =>**Resume Packet Output**.

The **middle pane** displays the raw contents of the packet, both in hexadecimal notation and as plain text. In the plain text, non-printable characters are replaced with dots. When multiple packets are selected in the **top table**, the **middle pane** displays the total number of selected packets, the total size, and the time span between the first and the last packet.

The **bottom pane** displays decoded packet information for the selected packet. This information includes vital data that can be used by network professionals. Right-clicking on the pane invokes the context menu that allows you to collapse/expand all the nodes or to copy the selected or all nodes.

The packets tab also includes a small toolbar shown below:



You can change the position of the decoder window by clicking on one of the three buttons on this toolbar (you can have a bottom-, left-, or right-aligned decoder window). The fourth button makes the packet list auto-scroll to the last packet received. The fifth button keeps the packet you selected in the list visible (i.e. it will not leave the visible area as new packets arrive). The sixth button allows you to open the contents of the current packet buffer in a new window. This functionality is very useful under a heavy network load, when the packet list is rapidly scrolling and it is difficult to examine packets before they move out of the visible area. Clicking on this button creates a snapshot of the buffer so you can comfortably examine it in a separate window. You can make as many snapshots as you wish.

Right-clicking on the packet list brings up a menu with the following commands:

Reconstruct TCP Session – allows you to reconstruct a TCP session starting from the selected packet; it opens a window that displays the entire conversation between two hosts. The same action is performed when you double-click on this window.
Reconstruct UDP Stream – allows you to reconstruct a UDP stream starting from the selected packet; it opens a window that displays the entire conversation between two hosts.
Quick Filter – finds the packets sent between the selected MAC addresses, IP addresses, or ports and displays them in a new window.
Open Packet(s) in New Window – allows you to open one or several selected packets in a new window for comfortable examination.
Create Alias – brings up a window where you can assign an easy-to-remember alias to the selected MAC or IP address.
Copy Address – copies the source MAC address, destination MAC address, source IP address, or destination IP address to the clipboard.
Copy Packet – copies the raw data of the selected packet to the clipboard.
Save Packet(s) As – saves the contents of the selected packet(s) to a file. The Save As dialog allows you to select the format to be used when saving data from the drop-down list.

SmartWhois – sends the source or destination IP address from the selected packet to SmartWhois if it is installed on your system. SmartWhois is a stand-alone application developed by our company capable of obtaining information about any IP address or hostname in the world. It automatically provides information associated with an IP address, such as domain, network name, country, state or province, and city. The program can be downloaded from our site. This option is disabled for non-IP packets.

Clear Packet Buffer – clears the contents of the program's buffer. The packet list will be cleared, and you will not be able to view the packets previously captured by the program.

Decode As – for TCP and UDP packets, allows you to decode supported protocols that use non-standard ports. For example, if your SOCKS server runs on port 333 rather than 1080, you can select a packet that belongs to the SOCKS session and use this menu command to make CommView for WiFi decode all packets on port 333 as SOCKS packets. Such protocol-port reassignments are not permanent and will last only until the program is closed. Note that you cannot override standard protocol-port pairs, e.g. you cannot make CommView for WiFi decode packets on port 80 as TELNET packets.

Font – allows you to increase or decrease the font size used to display packets without affecting the font size of all other interface elements.

You can also drag-and-drop selected packet(s) to the desktop.

Logging

This tab is used for saving captured packets to a file on the disk. CommView for WiFi saves packets in its own format with the .NCFX extension. You can open and view these files at any time using Log Viewer, or you can simply double-click on any NCFX file to have it loaded and decoded. NCFX is an open format; please refer to CommView Log Files Format chapter for detailed NCFX format description.

Save and Manage

Use this frame to save the captured packets manually to a file and to concatenate/split capture files. It is possible either to save all packets currently stored in the buffer or save only a part of them within a given range. The **To** and **From** fields allow you to set the necessary range based on the packet numbers as shown on the Packets tab. Click **Save As …** to select a file name. To concatenate manually multiple NCFX files into a single, larger file, click on the **Concatenate Logs** button. To split NCFX files that are too large into smaller chunks, click on the **Split Logs** button. Then the program will guide you through the process, and you will be able to enter the desired size of the output files.

Auto-saving

Check this box to have the program automatically save captured packets as they arrive. Use the **Maximum directory size** field to limit the total size of the capture files stored in the **Log Directory**. If the total size of the capture files exceeds the limit, the program automatically deletes the oldest files in the directory. The **Average Log File Size** field allows you to specify the approximate desired size of each log file. When the log file reaches the specified size, a new file is automatically created. To change the default **Log Directory**, click on the **Save files to** box and select a different folder.

> IMPORTANT: If you want to have an important capture file stored for a long time, do not keep it in the default Log Directory: there is a chance it will be automatically deleted as new files are being saved. Move the file to a different folder to preserve it.

Please note that the program does not save each packet individually immediately upon arrival. It means that if you view the log file in real time, it may not contain the latest packets. To make the program immediately dump the buffer to the log file, either click **Stop Capture** or uncheck the **Auto-saving** box.

WWW Access Logging

Check this box to enable logging of HTTP sessions. Use the **Maximum file size** field to limit the size of the log file. If the log file size exceeds the limit, the program automatically deletes the oldest records in the file. To change the default file name and path, click on the **Save files to** box and select a different file name. Log files can be generated in **HTML** or **TXT** formats. Click **Configure** to change the default logging options. You can change the port number that is used for HTTP access (the default value of 80 might not work for you if you are behind a proxy server), and exclude certain data types (usually logging anything other than HTML pages is quite useless; therefore it is a good idea to exclude URLs of pictures from the log file).

Viewing Logs

Log Viewer is a tool for viewing and exploring capture files created by CommView for WiFi and several other packet analyzers. It has the functionality of the **Packets** tab of the main program window, but unlike the **Packets** tab, Log Viewer displays packets loaded from the files on the disk rather than the packets captured in real time.

To open Log Viewer, click **File => Log Viewer** in the program's main menu, or just double-click on any CommView for WiFi capture file that you have previously saved. You can open as many Log Viewer windows as you wish, and each of them can be used for exploring one or several capture files.

Log Viewer can be used for exploring capture files created by other packet analyzers and personal firewalls. The current version can import files in the Network Instruments Observer®, Network General Sniffer® for DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ and AiroPeek™, Wireshark/Tcpdump, and Wireshark/pcapng formats. These formats are also used by a number of 3rd-party applications. Log Viewer is capable of exporting packet data by creating files in the Network Instruments Observer®, Network General Sniffer® for DOS/Windows, Microsoft® NetMon, WildPackets EtherPeek™ and AiroPeek™, Wireshark/Tcpdump, and Wireshark/pcapng formats, as well as the native CommView format.

Using Log Viewer is similar to using the **Packets** tab of the main window; please refer to the Packets chapter if you need detailed information.

Log Viewer Menu

File

Load CommView Logs – opens and loads one or several CommView for WiFi capture files.
Import Logs – allows you to import capture files created by other packet analyzers.
Export Logs – allows you to export the displayed packets to capture files in several formats.
Clear Window – clears the packet list.
Generate Statistics – makes CommView for WiFi generate statistics on the packets loaded in Log Viewer. Optionally, it is possible to reset previously collected statistical data displayed in the **Statistics** window. Please note that this function will not show packet distribution along the timeline. It is limited to displaying totals, protocol charts, and LAN hosts tables.
Send to VoIP Analyzer – sends all packets from the current Log Viewer window to a new VoIP Log Viewer window for VoIP-specific analysis.
Close Window – closes the window.

Search

Find Packet – shows a dialog that allows you to find packets matching a specific text.
Go to Packet Number - shows a dialog that allows you to jump to a packet with the specified number.

Rules

Apply – applies your current rule set to the packets displayed in Log Viewer. As a result, when you use this command the program will delete the packets that do not match the current rule set. Note that this will not modify the file on the disk.

From File … - does the same as the **Apply** command, but allows you to use a rule set from a previously saved .RLS file rather than the current rule set.

Rules

CommView for WiFi allows you to set two types of rules:

1. The first type (**wireless rules**) allows you to filter packets based on the wireless packet type: **Data**, **Management**, and **Control** packets. To turn capturing of these packet types on or off, use the **Rules** command of the program's menu, or the corresponding toolbar buttons. Additionally, the **Ignore Beacons** menu command allows you to switch capturing of beacon packets on and off.
2. The second type (**conventional rules**) allows you to filter packets based on many criteria, such as port number or MAC address. To use this type of rule, switch to the **Rules** tab of the program's main window. If one or more rules are set, the program filters packets based on the set rules and displays only the packets that comply with these rules. If a rule is set, the name of the corresponding page is displayed in bold font.

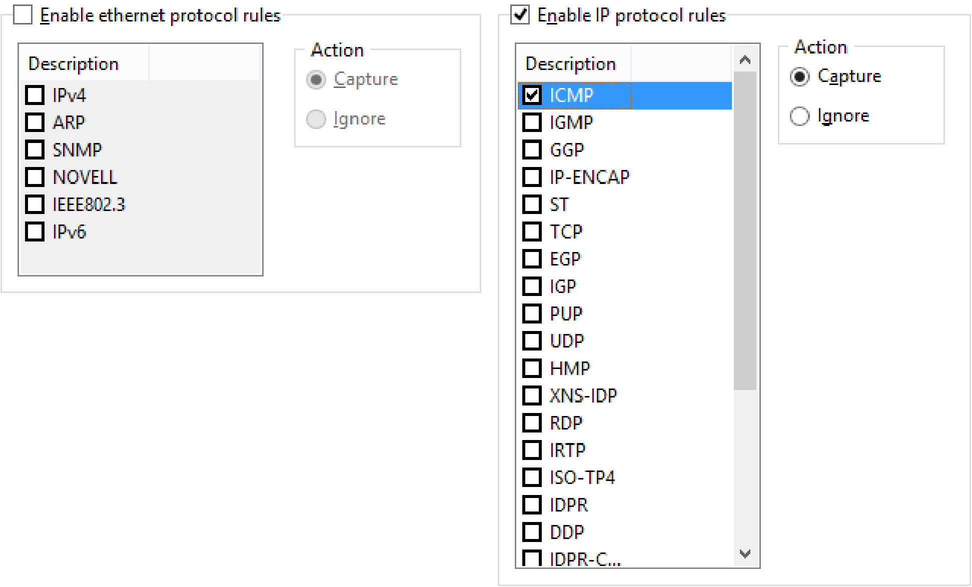
The program's status bar shows the number of conventional rules that are currently active. Note that it does **not** show the number of active wireless rules, as the state of the toolbar buttons (up or down) clearly indicate if any of the wireless rules are on or off. Also, note that wireless rules have precedence over conventional rules. Any captured packet must first pass the wireless rules before any further processing takes place. If, for example, none of the three wireless rules toolbar buttons is pressed, the program will not display any packets.

You can save your rules configuration(s) to a file and load them by using the **Rules** command of the program's menu.

Since WLAN traffic can often generate a high number of packets, it is recommended that you use rules to filter out unnecessary packets. This can considerably reduce the amount of system resources consumed by the program. If you want to enable/disable a rule, select the appropriate branch on the left side of the window (e.g. **IP Addresses** or **Ports**), and check or uncheck the box describing the rule (**Enable IP Address rules** or **Enable port rules**). Available types of rules are overviewed below.

Protocols

Allows you to ignore or capture packets based on Ethernet (Layer 2) and IP (Layer 3) protocols.



□ Enable ethernet protocol rules

Description
□ IPv4
□ ARP
□ SNMP
□ NOVELL
□ IEEE802.3
□ IPv6

Action
● Capture
○ Ignore

☑ Enable IP protocol rules

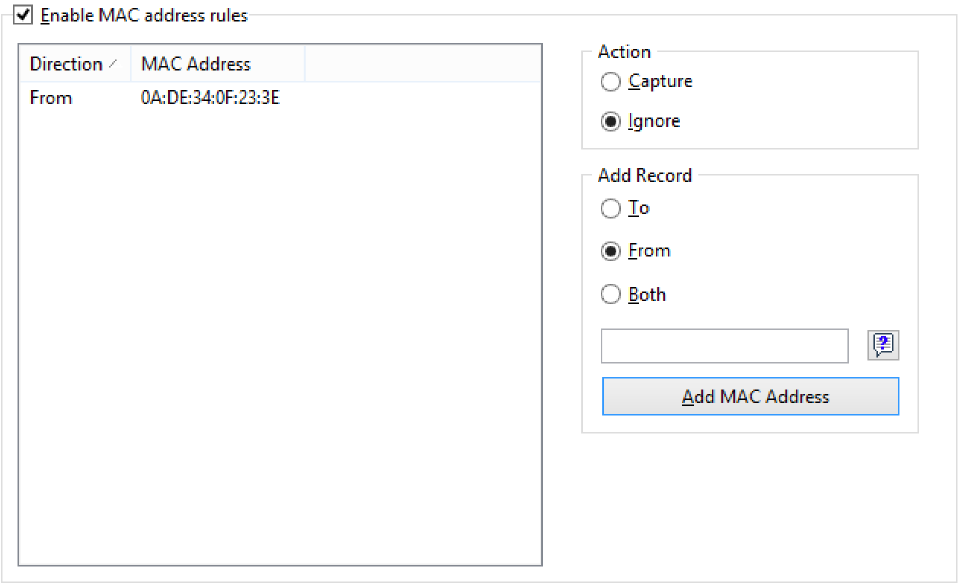
Description
☑ ICMP
□ IGMP
□ GGP
□ IP-ENCAP
□ ST
□ TCP
□ EGP
□ IGP
□ PUP
□ UDP
□ HMP
□ XNS-IDP
□ RDP
□ IRTP
□ ISO-TP4
□ IDPR
□ DDP
□ IDPR-C...

Action
● Capture
○ Ignore

This example shows how to make the program capture only ICMP and UDP packets. All other packets in the IP family will be ignored.

MAC Addresses

Allows you to ignore or capture packets based on MAC (hardware) addresses. Enter a MAC address in the **Add Record** frame, select the direction (**From, To,** or **Both**), and click **Add MAC Address**. The new rule will be displayed. Now you can select the action to be taken when a new packet is processed: the packet can be either captured or ignored. You can also click on the MAC Aliases button to get the list of aliases; double-click on the alias you would like to add, and the corresponding MAC address will appear in the input box.



☑ Enable MAC address rules

Direction	MAC Address
From	0A:DE:34:0F:23:3E

Action

○ Capture

● Ignore

Add Record

○ To

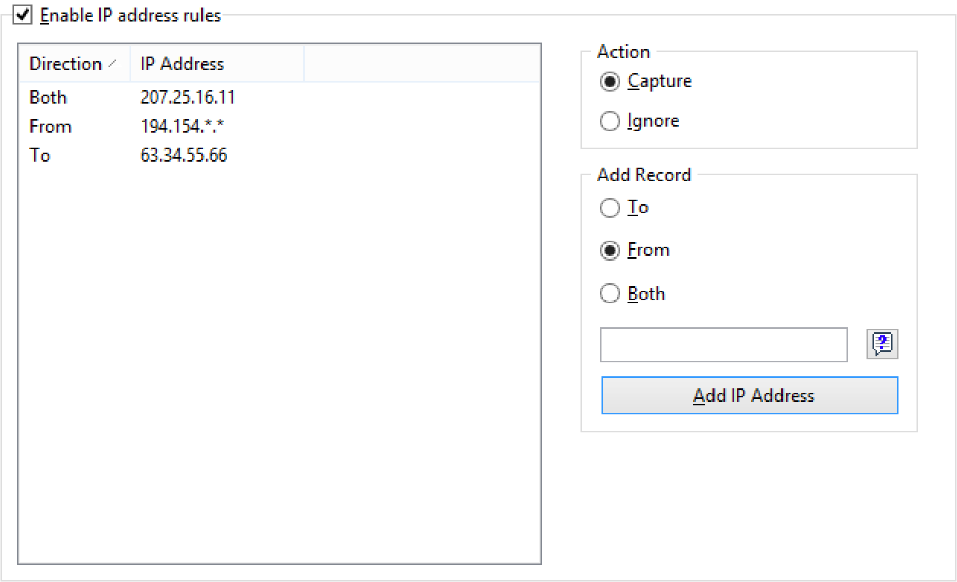
● From

○ Both

This example shows how to make the program ignore packets that come from 0A:DE:34:0F:23:3E. All packets that come from other MAC addresses will be captured.

IP Addresses

Allows you to ignore or capture packets based on IP addresses. Enter an IP or IPv6 address in the **Add Record** frame, select the direction (**From, To,** or **Both**), and click **Add IP Address**. You can use wildcards to specify blocks of IP addresses. The new rule will be displayed. Now you can select the action to be taken when a new packet is processed: the packet can be either captured or ignored. You can also click on the IP Aliases button to access the list of aliases; double-click on the alias you would like to add, and the corresponding IP address will appear in the input box.



☑ Enable IP address rules

Direction	IP Address
Both	207.25.16.11
From	194.154.*.*
To	63.34.55.66

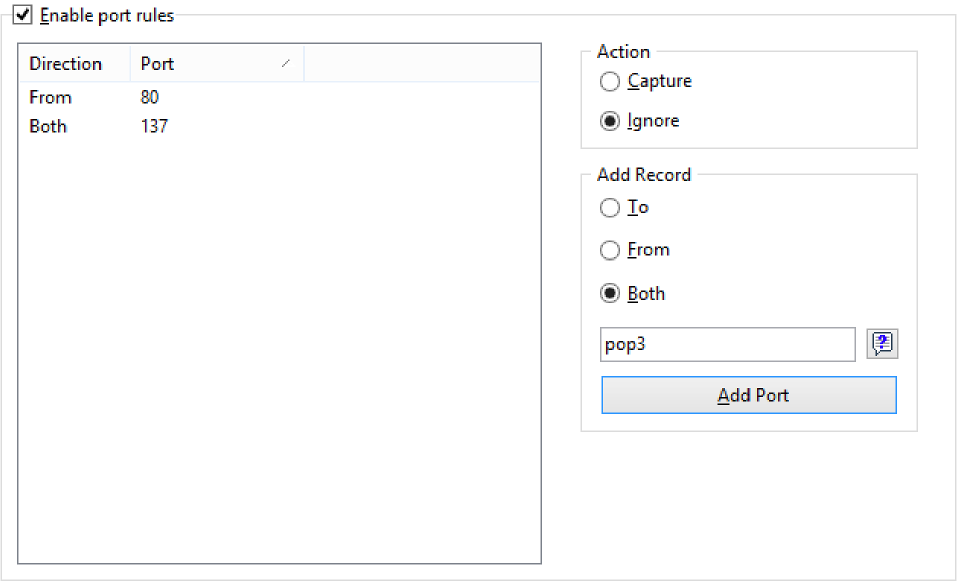
Action: ● Capture ○ Ignore

Add Record: ○ To ● From ○ Both

This example shows how to make the program capture the packets that go to 63.34.55.66, go to and come from 207.25.16.11 and come from all addresses between 194.154.0.0 and 194.154.255.255. All packets that come from other addresses or go to other addresses will be ignored. Since IP addresses are used in the IP protocol, such configuration will automatically make the program ignore all non-IP packets. Usage of IPv6 addresses requires Windows XP or higher and that the IPv6 stack be installed.

Ports

Allows you to ignore or capture packets based on ports. Enter a port number in the **Add Record** frame, select the direction (**From, To,** or **Both**), and click **Add Port**. The new rule will be displayed. Now you can select the action to be taken when a new packet is processed: the packet can be either captured or ignored. You can also press the Port Reference button to get a list of all known ports; double-click on the port you would like to add and its number will appear in the input box. You can also click on the Port Reference button to get a list of all known ports; double-click on the port you would like to add and its number will appear in the input box. Ports can also be entered as text; for example, you can type in *http* or *pop3*, and the program will convert the port name to the numeric value.



☑ Enable port rules

Direction	Port
From	80
Both	137

Action
○ Capture
● Ignore

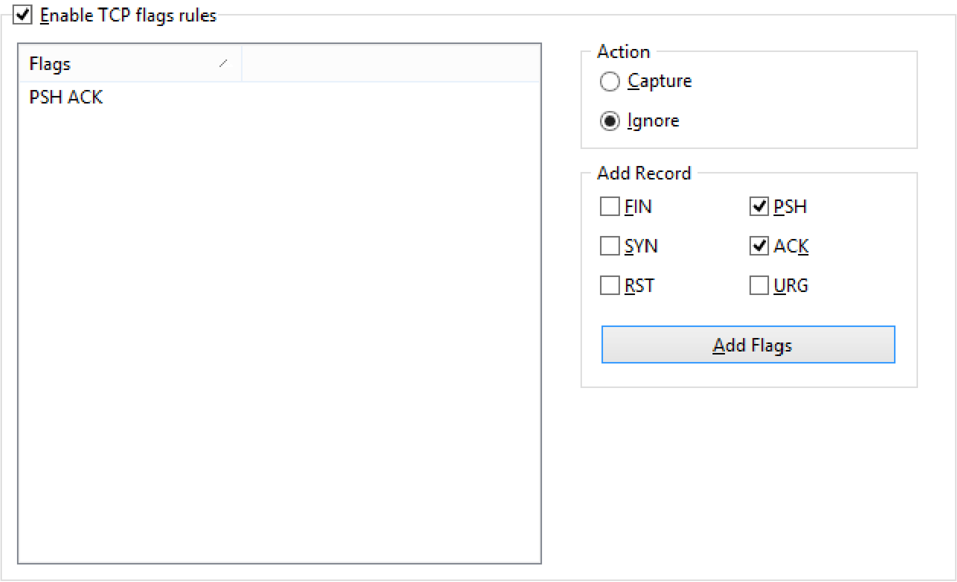
Add Record
○ To
○ From
● Both

pop3

This example shows how to make the program ignore packets that come from port 80 and go to and come from port 137. This rule will prevent CommView for WiFi from displaying inbound HTTP traffic, as well as inbound and outbound NetBIOS Name Service traffic. All packets coming to and from other ports will be captured.

TCP Flags

Allows you to ignore or capture packets based on TCP flags. Check a flag or a combination of flags in the **Add Record** frame, and click **Add Flags**. The new rule will be displayed. Now you can select the action to be taken when a new packet with the entered TCP flag is processed: the packet can be either captured or ignored.



☑ Enable TCP flags rules

Flags
PSH ACK

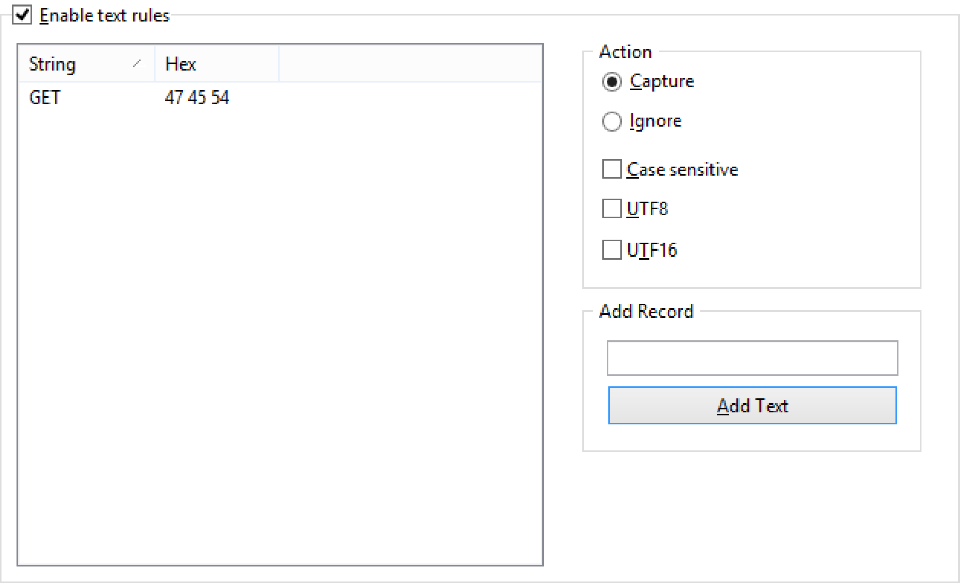
Action: ○ Capture ● Ignore

Add Record: □ FIN ☑ PSH □ SYN ☑ ACK □ RST □ URG

This example shows how to make the program ignore TCP packets with the PSH ACK flag. All packets with other TCP flags will be captured.

Text

Allows you to capture packets that contain certain text. Enter a text string in the **Add Record** frame and click **Add Text**. The new rule will be displayed. Now you can select the action to be taken when a new packet is processed: the packet can be either captured or ignored.



☑ Enable text rules

String	Hex
GET	47 45 54

Action: ● Capture ○ Ignore

□ Case sensitive
□ UTF8
□ UTF16

Add Record

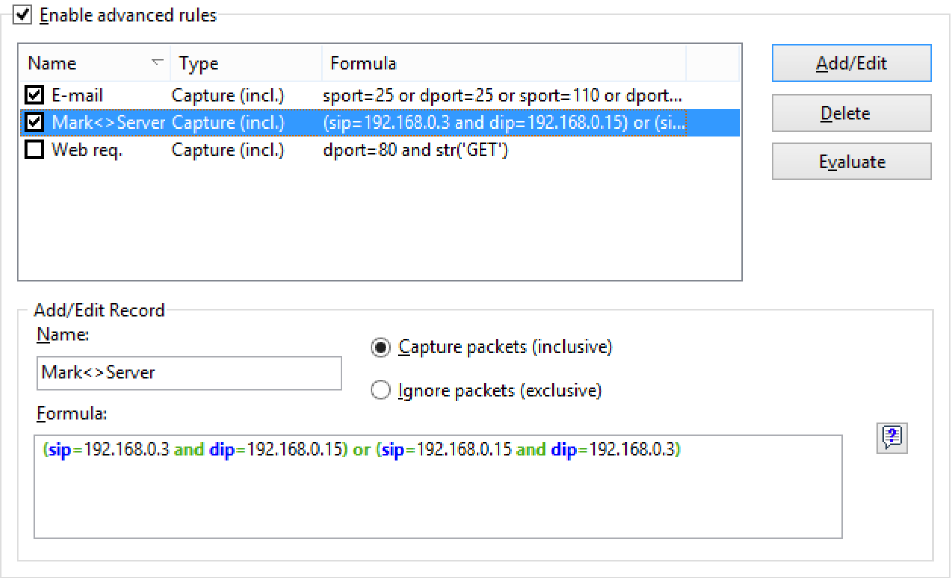
This example shows how to make the program capture only the packets that contain "GET". Check the **Case sensitive** box if you want the rules to be case sensitive. Check the **UTF8** or **UTF16** box if you want the rule to match the text encoded using the respective encodings. All other packets that do not contain the text mentioned above will be ignored. If you would like to create a rule based on hex byte sequences, when the text is not printable (e.g. 0x010203), use the Advanced Rules.

Advanced

Advanced rules are the most powerful and flexible rules that allow you to create complex filters using Boolean logic. For the detailed help on using advanced rules, please refer to the Advanced Rules chapter.

Advanced Rules

Advanced rules are the most powerful and flexible rules that allow you to create complex filters using Boolean logic. Using advanced rules requires a basic understanding of mathematics and logic, but the rules syntax is rather easy to understand.



☑ Enable advanced rules

Name	Type	Formula
☑ E-mail	Capture (incl.)	sport=25 or dport=25 or sport=110 or dport...
☑ Mark<>Server	Capture (incl.)	(sip=192.168.0.3 and dip=192.168.0.15) or (si...
□ Web req.	Capture (incl.)	dport=80 and str('GET')

Add/Edit Record

Name: Mark<>Server

● Capture packets (inclusive)

○ Ignore packets (exclusive)

Formula: (sip=192.168.0.3 and dip=192.168.0.15) or (sip=192.168.0.15 and dip=192.168.0.3)

Overview

To add a new rule, you should enter an arbitrary name in the **Name** field, select the action (**Capture/Ignore**), enter a **Formula** using the syntax described below, and click **Add/Edit**. Your new rule will be added to the list and become active immediately. You can add as many rules as you wish, but only those rules that have a checked box next to the rule name are active currently. You can activate/deactivate rules by checking/unchecking the corresponding boxes or completely delete selected rules using the **Delete** button. If more than one rule is active, you can evaluate the resulting combined rule by clicking **Evaluate**. Please note that multiple positive ("Capture") active rules are combined using the logical OR operator, e.g. if you have three active rules, RULE1, RULE2, and RULE3, the resulting rule is RULE1 OR RULE2 OR RULE3. If you also use negative ("Ignore") rules, those will be added to the final expression using the logical AND operator, because combining a negative rule as "OR" would be make no sense.

You can use advanced rules in conjunction with the basic rules described in the previous chapter. However, if you feel comfortable with Boolean logic, it is a good idea to use advanced rules only, as they offer much more flexibility. Basic rules are combined with advanced rules using the logical AND operator.

Syntax Description

dir – packet direction. Possible values are *in* (inbound), *out* (outbound), and *pass* (pass-through). This keyword is for compatibility with the standard, non-wireless edition of CommView only. In CommView for WiFi, there are no inbound or outbound packets, because your adapter does not participate in data exchange and only passively monitors pass-through packets.

etherproto – Ethernet protocol, the 13th and 14th bytes of the packet. Acceptable values are numbers (e.g. *etherproto=0x0800* for IP) or common aliases (e.g. *etherproto=ARP*, which is equivalent to 0x0806).

ipproto – IP protocol. Acceptable values are numbers (e.g. *ipproto!=0x06* for TCP) or commonly used aliases (e.g. *ipproto=UDP*, which is equivalent to 0x11).
smac – source MAC address. Acceptable values are MAC addresses in hex notation (e.g. *smac=00:00:21:0A:13:0F*) or user-defined aliases.

dmac – destination MAC address.

sip – source IP or IPv6 address. Acceptable values are IP addresses in dotted notation (e.g. *sip=192.168.0.1*), IP addresses with wildcards (e.g. *sip!=*.*.*.255,* except for IPv6 addresses), network addresses with subnet masks (e.g. *sip=192.168.0.4/255.255.255.240* or *sip=192.168.0.5/28*), IP ranges (e.g. *sip from 192.168.0.15 to 192.168.0.18* or *sip in 192.168.0.15 .. 192.168.0.18*), or user-defined aliases. Use of IPv6 addresses requires Windows XP or higher and that the IPv6 stack be installed.

dip – destination IP address.

sport – source port for TCP and UDP packets. Acceptable values are numbers (e.g. *sport=80* for HTTP), ranges (e.g. *sport from 20 to 50* or *sport in 20..50* for any port number between 20 and 50) or the aliases defined by your operating system (e.g. *sport=ftp*, which is equivalent to 21). For the list of aliases supported by your OS click **View => Port Reference**.

dport – destination port for TCP and UDP packets.

flag – TCP flag. Acceptable values are numbers (e.g. *0x18* for PSH ACK) or one or several of the following characters: *F* (FIN), *S* (SYN), *R* (RST), *P* (PSH), *A* (ACK), and *U* (URG), or the *has* keyword, which means that the flag contains a certain value. Usage examples: *flag=0x18*, *flag=SA*, *flag has F*.

size – packet size. Acceptable values are numbers (e.g. *size=1514*) or ranges (e.g. *size from 64 to 84* or *size in 64..84* for any size between 64 and 84).

str – packet contents. Use this function to indicate that the packet must contain a certain string. This function has three arguments: string, position, and case sensitivity. The first argument is a string, e.g. *'GET'*. The second argument is a number that indicates the string position (offset) in the packet. The offset is zero-based, i.e. if you are looking for the first byte in the packet, the offset value must be *0*. If the offset is not important, use *–1*. The third argument indicates the case-sensitivity and can be either *false* (case-insensitive) or *true* (case-sensitive). The second and third arguments are optional; if omitted, the offset defaults to *–1* and the case-sensitivity defaults to *false*. Usage examples: *str('GET',-1,false), str('GET',-1), str ('GET').*

hex – packet contents. Use this function to indicate that the packet must contain a certain hexadecimal byte pattern. This function has two arguments: hex pattern and position. The first argument is a hex value, e.g. *0x4500*. The second argument is a number that indicates the pattern position (offset) in the packet. The offset is zero-based, i.e. if you are looking for the first byte in the packet, the offset value must be *0*. If the offset is not important, use *–1*. The second argument is optional; if omitted, the offset defaults to *–1*. Usage examples: *hex(0x04500, 14)* , *hex(0x4500, 0x0E), hex (0x010101).*

bit - Packet contents. Use this function to determine if the specified bit at the specified offset is set to 1, in which case the function returns *true*. If the specified bit is set to 0 or the specified byte is beyond the packet boundary, the function returns *false*. This function has two arguments: bit index and byte position. The first argument is the bit index in the byte; the allowed values are 0-7. The index is zero-based, i.e. if you are looking for the eighth bit in the byte, the index value must be *7.* The second argument is a number that indicates the byte position (offset) in the packet. The offset is zero-based, i.e. if you are looking for the first byte in the packet, the offset value must be *0*. Both arguments are mandatory. Usage examples: *bit(0, 14)* , *bit(5, 1)*.

ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP, Order, Ftype, FsubType, Duration, FragNum, SeqNum - allow you to use 802.11 packet header fields in advanced rules. The names of the operators fully correspond to the packet header fields as described in the 802.11 standard specification. The acceptable values for ToDS, FromDS, MoreFrag, Retry, Power, MoreData, WEP, and Order are 0 or 1. For Ftype, FsubType, Duration, FragNum, and SeqNum operators other numeric values are acceptable.

Please refer to the 802.11 standard specification for the detailed information about 802.11 packet headers fields and their acceptable values.

The keywords described above can be used with the following operators:

and - Boolean conjunction.
or - Boolean disjunction.
not - Boolean negation.
= - arithmetic equality.
!= - arithmetic inequality.
<> - same as above.
> - arithmetic greater-than.
< - arithmetic less-than.
( ) – parenthesis, control operator precedence rules.

All numbers can be in decimal or hexadecimal notation. If you want to use the hexadecimal notation, the number must be preceded by *0x*, i.e. you can use either *15* or *0x0F*.

Examples

Below you will find a number of examples illustrating the rules syntax. Each rule is followed by our comments about what the rule does. The comments are separated from the actual rule by two slashes.

- **(smac=00:00:21:0A:13:0E or smac=00:00:21:0A:13:0F) and etherproto=arp** // Captures ARP packets sent by two computers, 00:00:21:0A:13:0E and 00:00:21:0A:13:0F.
- **ipproto=udp and dport=137** // Captures UDP/IP packets sent to the port number 137.
- **dport=25 and str('RCPT TO:', -1, true)** // Captures TCP/IP or UDP/IP packets that contain "'RCPT TO:" and where the destination port is 25.
- **not (sport>110)** // Captures everything except the packets where the source port is greater than 110.
- **(sip=192.168.0.3 and dip=192.168.0.15) or (sip=192.168.0.15 and dip=192.168.0.3)** // Captures only the IP packets being sent between two machines, 192.168.0.3 and 192.168.0.15. All other packets are discarded.
- **((sip from 192.168.0.3 to 192.168.0.7) and (dip = 192.168.1.0/28)) and (flag=PA) and (size in 200..600)** // Captures TCP packets the size of which is between 200 and 600 bytes coming form the IP addresses in the

192.168.0.3 - 192.168.0.7 range, where destination IP address is in the 192.168.1.0/255.255.255.240 segment, and where the TCP flag is PSH ACK.

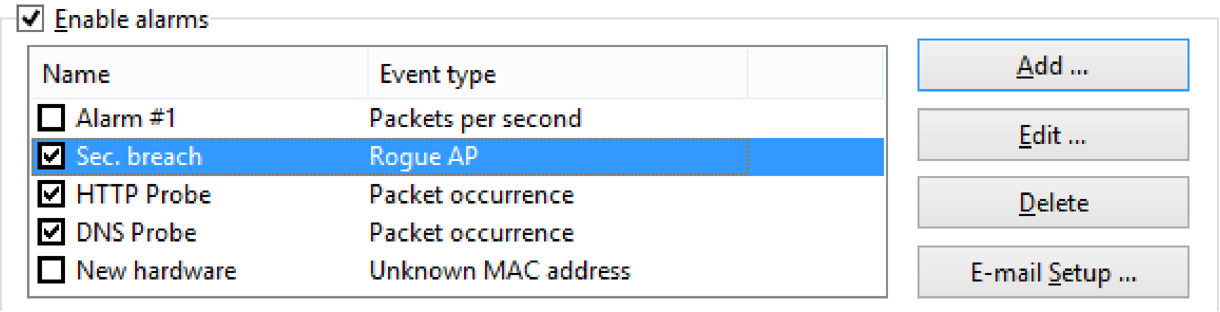
- **Hex(0x0203, 89) and (dir<>in)** // Captures the packets that contain 0x0203 at the offset 89, where the packet direction is not inbound.
- **not(ftype=0 and fsubtype=8)** // Ignore management packets of the beacon type
- **ftype=2 and wep=1** // Capture encrypted data packets
- **MoreFrag=0 and FragNum=0** // Capture unfragmented packets

Alarms

This tab allows you to create alarms that can notify you about important events, such as suspicious packets, high bandwidth utilization, unknown addresses, etc. Alarms are very useful in a situation where you need to watch the network for some suspicious events, for example distinctive byte patterns in captured packets, port scans, or unexpected hardware device connections.

> IMPORTANT: Alarms can be triggered only by those packets that have passed the program's filters. If, for example, you configured the program to filter out UDP packets by creating the corresponding rule, while one of your alarms is supposed to be triggered by a UDP packet, such an alarm will never be triggered.

Alarms are managed using the alarm list shown below:

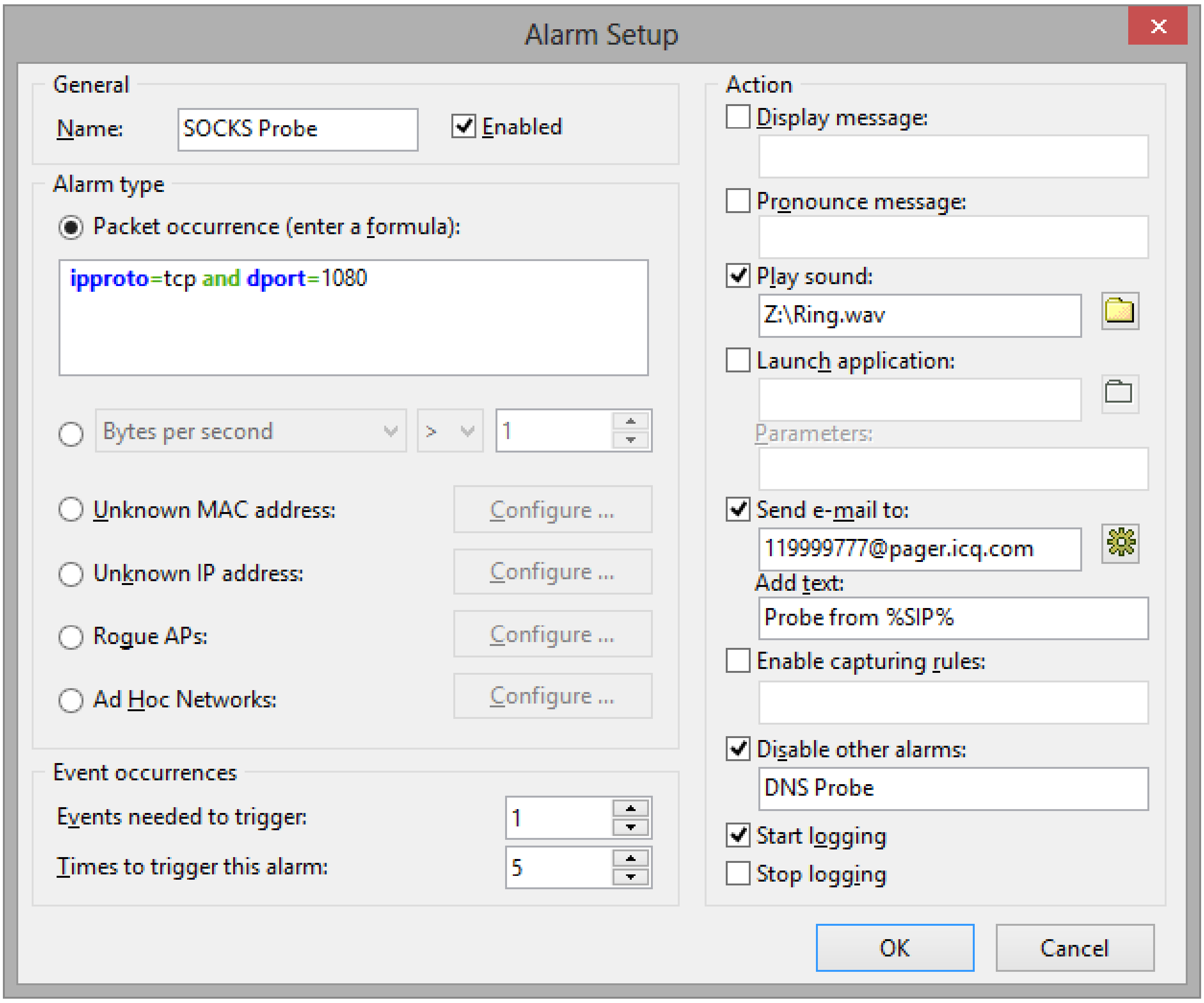


☑ Enable alarms

Name	Event type
☐ Alarm #1	Packets per second
☑ Sec. breach	Rogue AP
☑ HTTP Probe	Packet occurrence
☑ DNS Probe	Packet occurrence
☐ New hardware	Unknown MAC address

Each line represents a separate alarm, and the check box next to the alarm name indicates if the alarm is currently active. When an alarm is triggered, the check mark disappears. To reactivate a deactivated alarm, check the box next to its name. To disable all alarms, uncheck the **Enable alarms** box. To add a new alarm or edit or delete an existing one, use the buttons to the right of the alarm list. The **E-mail Setup** button should be used for entering information about your SMTP server if you plan to use e-mail notification options (see below).

The alarm setup window is shown below:



Alarm Setup

General

Name: SOCKS Probe ☑ Enabled

Alarm type

● Packet occurrence (enter a formula):

```
ipproto=tcp and dport=1080
```

○ Bytes per second > 1

○ Unknown MAC address: Configure ...

○ Unknown IP address: Configure ...

○ Rogue APs: Configure ...

○ Ad Hoc Networks: Configure ...

Event occurrences

Events needed to trigger: 1

Times to trigger this alarm: 5

Action

□ Display message:

□ Pronounce message:

☑ Play sound: Z:\Ring.wav

□ Launch application:

Parameters:

☑ Send e-mail to: 119999777@pager.icq.com

Add text: Probe from %SIP%

□ Enable capturing rules:

☑ Disable other alarms: DNS Probe

☑ Start logging

□ Stop logging

The **Name** field should be used for describing the alarm function. Check the **Enabled** box if you want the alarm that you are adding/editing to be activated once you have finished its setup. This check box is equivalent to the one shown in the alarms list. The **Alarm Type** frame allows you to select one of the ten alarm types:

- **Packet occurrence** – The alarm will be triggered once CommView for WiFi has captured a packet that matches the given formula. The formula syntax is the same as the syntax used in Advanced Rules and is described in the Advanced Rules chapter in detail.
- **Bytes per second** – The alarm will be triggered once the number of bytes per second has exceeded (or fallen below) the specified value. Note that you should enter the value in bytes, so if you would like to have the alarm triggered when the data transfer rate exceeds 1Mbyte per second, the value you should enter is 1000000.
- **Packets per second** – The alarm will be triggered once the number of packets bytes per second has exceeded (or fallen below) the specified value.
- **Broadcasts per second** - The alarm will be triggered once the number of broadcast packets has exceeded (or fallen below) the specified value.
- **Multicasts per second** - The alarm will be triggered once the number of multicast packets has exceeded (or fallen below) the specified value.

- **CRC errors per second** - The alarm will be triggered once the number of CRC errors per second has exceeded (or fallen below) the specified value.
- **Retries per second** - The alarm will be triggered once the number of retries per second has exceeded (or fallen below) the specified value.
- **Unknown MAC address** – The alarm will be triggered once CommView for WiFi has captured a packet with an unknown source or destination MAC address. Use the **Configure** button to enter known MAC addresses. This alarm type is useful for detecting new, unauthorized hardware devices connected to your WLAN.
- **Unknown IP address** – The alarm will be triggered once CommView for WiFi has captured a packet with an unknown source or destination IP or IPv6 address. Use the **Configure** button to enter known IP addresses. This alarm type is useful for detecting unauthorized IP connections behind a corporate firewall. Use of IPv6 addresses requires Windows XP or higher and that the IPv6 stack be installed.
- **Rogue APs** – The alarm will be triggered once CommView for WiFi has captured a beacon packet from an unknown access point. Use the **Configure** button to enter the MAC addresses of known access points. This alarm type is useful for detecting unauthorized access points.
- **Ad Hoc Networks –** The alarm will be triggered once CommView for WiFi has captured a beacon packet from an unknown Ad Hoc station. Use the **Configure** button to enter the MAC addresses of known Ad Hoc stations, if any. This alarm type is useful for detecting unauthorized usage of Ad Hoc networks.

The **Events needed to trigger** field allows you to specify the number of times the expected event must occur before the alarm is triggered. For example, if you specify the value of 3, the alarm will not be triggered until the event occurs three times. If you edit an existing alarm, the internal event counter will be reset.

The **Times to trigger this alarm** field allows you to specify the number of times your alarm may be triggered before deactivation. By default, this value equals 1, so the alarm will be disabled after the first event occurrence. By increasing this value, you will make CommView for WiFi trigger the alarm multiple times. If you edit an existing alarm, the internal trigger counter will be reset.

The **Action** frame allows you to select the actions to be performed when the alarm event occurs. The following actions are available:

- **Display message**: Shows a non-modal message box with the specified text. This action allows use of variables that are to be replaced by the corresponding parameters of the packet that has triggered the alarm. These variables are listed below:

  %SMAC% -- source MAC address.
  %DMAC% -- destination MAC address.
  %SIP% -- source IP address.
  %DIP% -- destination IP address.
  %SPORT% -- source port.
  %DPORT% -- destination port.
  %ETHERPROTO% -- Ethernet protocol.
  %IPPROTO% -- IP protocol.
  %SIZE% -- packet size.
  %FILE% -- the path to a temporary file that contains the captured packet.

  For example, if your message is "SYN packet received from %SIP%," in the actual pop-up window text %SIP% will be replaced by the source IP address of the packet that triggered the alarm. If you use the %FILE%

variable, a .NCFX file will be created in the temporary folder. It is your responsibility to delete the file after it has been processed; CommView for WiFi makes no attempt to delete it. You should not use variables if the alarm is triggered by **Bytes per second** or **Packets per second** values, as these alarm types are not triggered by individual packets.

- **Pronounce message:** Makes Windows speak the specified text using the text-to-speech engine. This box is disabled if your Windows version does not have the text-to-speech engine. By default, Windows only comes with English computer voices, so Windows may not be able to pronounce messages correctly if the text is entered in a language other than English. You can use the variables described in the **Display message** section in the message text.
- **Play sound –** plays the specified WAV file.
- **Launch application –** runs the specified EXE or COM file. Use the optional **Parameters** field to enter command line parameters. You can use the variables described in the **Display message** section above as the command line parameters if you want your application to receive and process information about the packet that triggered the alarm.
- **Send e-mail to –** sends e-mail to the specified e-mail address. You MUST configure CommView for WiFi to use your SMTP server prior to sending e-mail. Use the **E-mail Setup** button next to the alarm list to enter your SMTP server settings and send a test e-mail message. Usually, an e-mail message can also be used to send alerts to your instant messaging application, cell phone, or pager. For example, to send a message to an ICQ user, you should enter the e-mail address as ICQ_USER_UIN@pager.icq.com, where ICQ_USER_UIN is the user's unique ICQ identification number, and allow EmailExpress messages in the ICQ options. Please refer to your instant messenger documentation or cell phone operator for more information. The **Add text** field can be used to add an arbitrary message to the e-mail notification. You can use the variables described in the **Display message** section in the message text.
- **Enable capturing rules –** enables Advanced Rules; you should enter the rule name(s). If multiple rules must be enabled, separate them with a comma or semicolon.
- **Disable other alarms –** disables other alarms; you should enter the alarm name(s). If multiple alarms must be enabled, separate them with a comma or semicolon.
- **Start logging –** turns on auto-saving (see the Logging chapter); CommView for WiFi will start dumping packets to the hard drive.
- **Stop logging –** turns off auto-saving.

Click **OK** to save the settings and close the alarm setup dialog.

All the events and actions related to the alarms will be listed in the **Event Log** window below the alarm list.

WEP/WPA Keys

The **WEP/WPA Keys** window allows WEP, WPA, or WPA2 keys to be entered for the decryption of captured packets. Without these keys, the program will not be able to decrypt data packets being transmitted on your WLAN. Since some WLANs use mixed mode encryption, where both WEP- and WPA-enabled clients can authenticate, you can use a WEP key and WPA passphrase simultaneously.

WEP

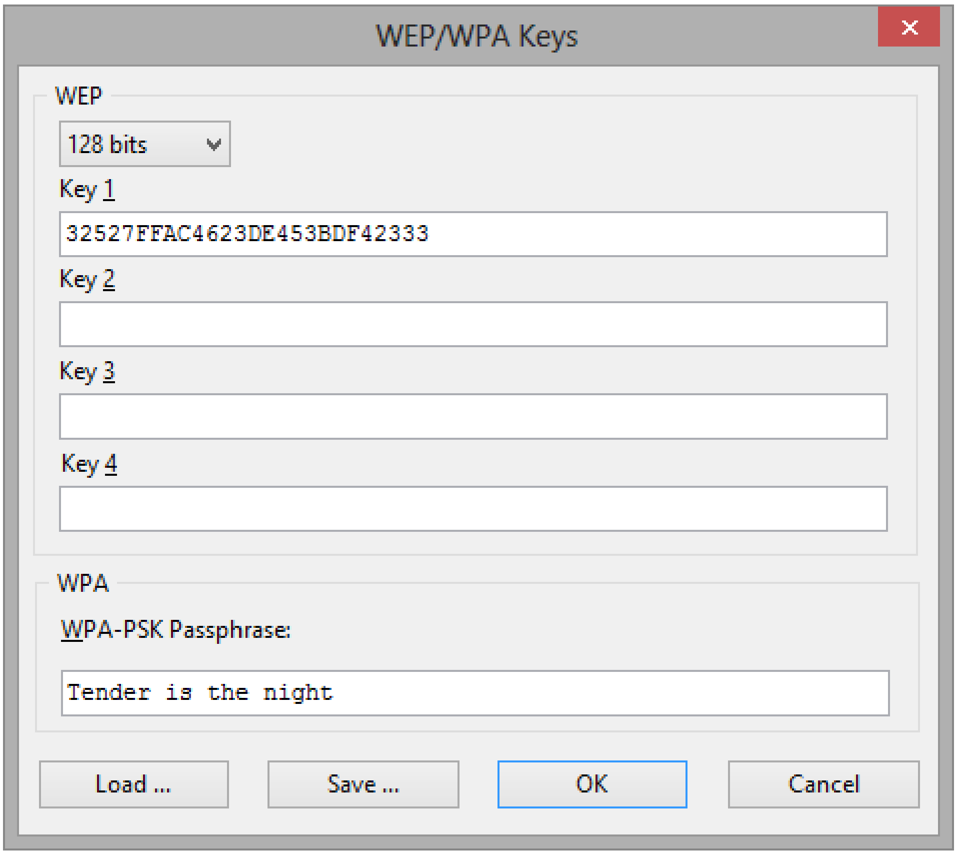
The standard allows you to use up to four WEP keys, so you can specify one, two, three, or four keys. The key length drop-down list allows you to select the key length. Supported lengths are 64, 128, 152, and 256 bits, and you should enter a hexadecimal string that is 10, 26, 32, or 58 characters long correspondingly.

WPA

The Wi-Fi Protected Access (WPA) standard defines a number of authentication and encryption modes. Not all of them are supported by CommView for WiFi due to the restrictions of the underlying security model. CommView for WiFi supports decryption of WPA or WPA2 in Pre-Shared Key (PSK) mode using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard/Counter CBC-MAC Protocol (AES/CCMP) data encryption. You can enter either a passphrase or a hexadecimal key that is 64 characters long.

> IMPORTANT: Please note that **packet traffic encrypted with WPA3 cannot be decrypted**. WPA3 uses the passphrase only for authentication; decryption is impossible.

> IMPORTANT: Please refer to the Understanding WPA Decryption chapter for detailed information about the way CommView for WiFi processes WPA-encrypted traffic. You may also want to use the Node Reassociation tool once you have entered a new WPA passphrase.



WEP: 128 bits

Key 1: 32527FFAC4623DE453BDF42333

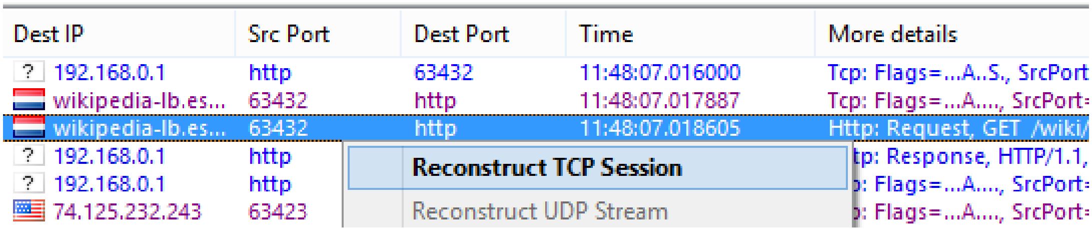
WPA-PSK Passphrase: Tender is the night

To save the current key set, click **Save** .... To load a previously saved key set, click **Load...** .

The key set that you can enter or load using this dialog will be applied to packets captured in real-time, as well as to any NCFX capture files that might have been saved previously. When captured packets are saved to a NCFX capture file, those packets that were decrypted successfully will be saved in decrypted form, while those packets that could not be decrypted will be saved in the original, unmodified form.

Reconstructing TCP Sessions

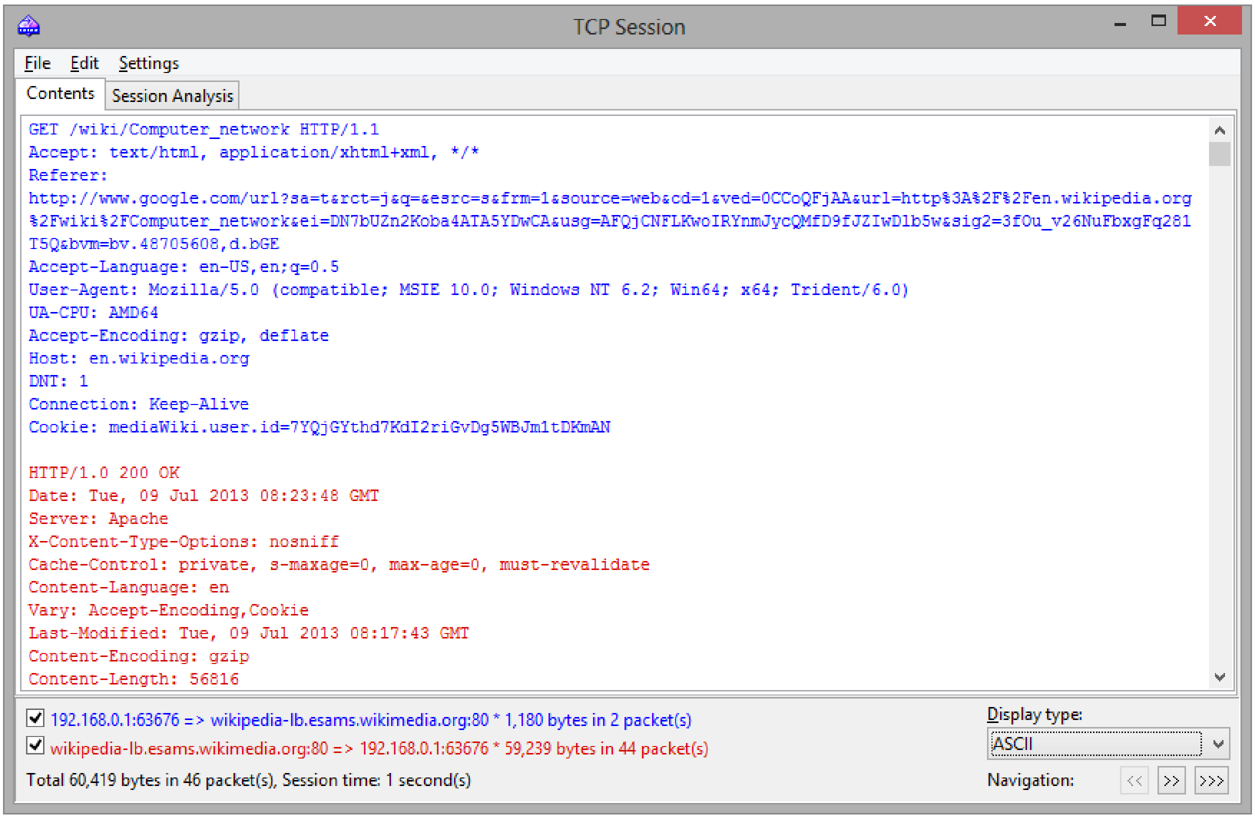
This tool allows you to view the TCP conversation between two hosts. To reconstruct a TCP session, you should first select a TCP packet on the **Packets** tab. Depending on the settings (the **Search for the session start when reconstructing TCP sessions** box in **Settings** => **Options => Decoding)**, the session will be reconstructed from the selected packet that may be in the middle of the "conversation" or from the session start. After you locate and select the packet, right-click on it and select **Reconstruct TCP Session** from the pop-up menu as shown below:



Dest IP	Src Port	Dest Port	Time	More details
? 192.168.0.1	http	63432	11:48:07.016000	Tcp: Flags=...A..S., SrcPort
wikipedia-lb.es...	63432	http	11:48:07.017887	Tcp: Flags=...A...., SrcPort=
wikipedia-lb.es...	63432	http	11:48:07.018605	Http: Request, GET /wiki/
? 192.168.0.1	http			tp: Response, HTTP/1.1,
? 192.168.0.1	http			p: Flags=...A...., SrcPort=
74.125.232.243	63423			p: Flags=...A...., SrcPort=

Reconstructing sessions works best for text-based protocols, such as POP3, Telnet, or HTTP. Of course, you can also reconstruct a download of a large zipped file, but it can take CommView for WiFi a long time to reconstruct several megabytes of data, and the obtained information would be useless in most of the cases. The **Contents** tab displays the actual session data, while the **Session Analysis** tab graphically displays the flow of the reconstructed TCP session.

A sample HTTP session that contains HTML data displayed in ASCII and HTML modes is shown below:



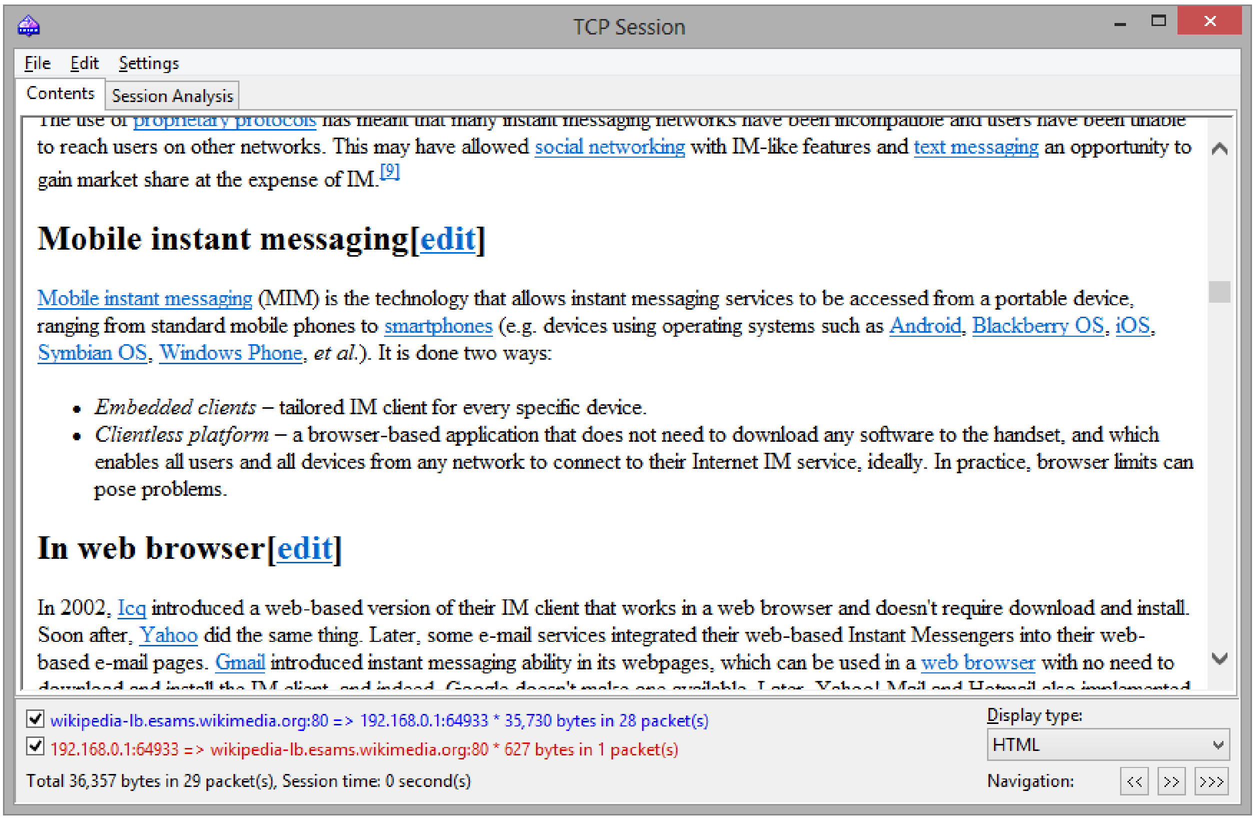
```
GET /wiki/Computer_network HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer:
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fen.wikipedia.org
%2Fwiki%2FComputer_network&ei=DN7bUZn2Koba4ATA5YDwCA&usg=AFQjCNFLKwoIRYnmJycQMfD9fJZIwDlb5w&sig2=3f0u_v26NuFbxgFq281
T5Q&bvm=bv.48705608,d.bGE
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Win64; x64; Trident/6.0)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: en.wikipedia.org
DNT: 1
Connection: Keep-Alive
Cookie: mediaWiki.user.id=7YQjGYthd7KdI2riGvDg5WBJm1tDKmAN

HTTP/1.0 200 OK
Date: Tue, 09 Jul 2013 08:23:48 GMT
Server: Apache
X-Content-Type-Options: nosniff
Cache-Control: private, s-maxage=0, max-age=0, must-revalidate
Content-Language: en
Vary: Accept-Encoding,Cookie
Last-Modified: Tue, 09 Jul 2013 08:17:43 GMT
Content-Encoding: gzip
Content-Length: 56816
```

☑ 192.168.0.1:63676 => wikipedia-lb.esams.wikimedia.org:80 * 1,180 bytes in 2 packet(s)

☑ wikipedia-lb.esams.wikimedia.org:80 => 192.168.0.1:63676 * 59,239 bytes in 44 packet(s)

Total 60,419 bytes in 46 packet(s), Session time: 1 second(s)

Display type: ASCII



The use of proprietary protocols has meant that many instant messaging networks have been incompatible and users have been unable to reach users on other networks. This may have allowed social networking with IM-like features and text messaging an opportunity to gain market share at the expense of IM.[9]

Mobile instant messaging[edit]

Mobile instant messaging (MIM) is the technology that allows instant messaging services to be accessed from a portable device, ranging from standard mobile phones to smartphones (e.g. devices using operating systems such as Android, Blackberry OS, iOS, Symbian OS, Windows Phone, *et al.*). It is done two ways:

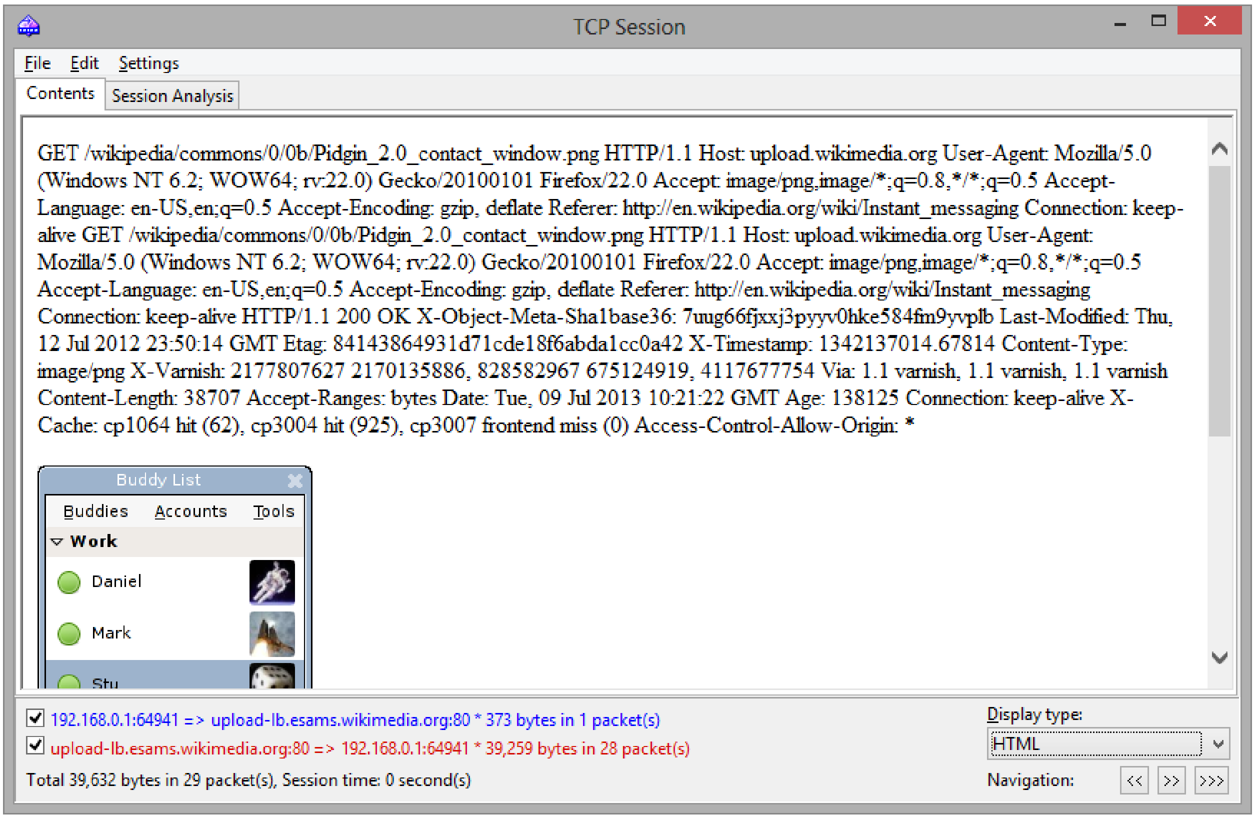
- *Embedded clients* – tailored IM client for every specific device.
- *Clientless platform* – a browser-based application that does not need to download any software to the handset, and which enables all users and all devices from any network to connect to their Internet IM service, ideally. In practice, browser limits can pose problems.

In web browser[edit]

In 2002, Icq introduced a web-based version of their IM client that works in a web browser and doesn't require download and install. Soon after, Yahoo did the same thing. Later, some e-mail services integrated their web-based Instant Messengers into their web-based e-mail pages. Gmail introduced instant messaging ability in its webpages, which can be used in a web browser with no need to download and install the IM client, and indeed, Google doesn't make one available. Later, Yahoo! Mail and Hotmail also implemented

☑ wikipedia-lb.esams.wikimedia.org:80 => 192.168.0.1:64933 * 35,730 bytes in 28 packet(s)
☑ 192.168.0.1:64933 => wikipedia-lb.esams.wikimedia.org:80 * 627 bytes in 1 packet(s)
Total 36,357 bytes in 29 packet(s), Session time: 0 second(s)

In HTML display mode, HTML pages typically do not include inline graphics, because in HTTP protocol images are transferred separately from HTML data. To view the images, it is usually necessary to navigate to the next TCP session. A sample HTTP session that contains image data displayed in HTML mode is shown below:



GET /wikipedia/commons/0/0b/Pidgin_2.0_contact_window.png HTTP/1.1 Host: upload.wikimedia.org User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0 Accept: image/png,image/*;q=0.8,*/*;q=0.5 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://en.wikipedia.org/wiki/Instant_messaging Connection: keep-alive GET /wikipedia/commons/0/0b/Pidgin_2.0_contact_window.png HTTP/1.1 Host: upload.wikimedia.org User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0 Accept: image/png,image/*;q=0.8,*/*;q=0.5 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://en.wikipedia.org/wiki/Instant_messaging Connection: keep-alive HTTP/1.1 200 OK X-Object-Meta-Sha1base36: 7uug66fjxxj3pyyv0hke584fm9yvplb Last-Modified: Thu, 12 Jul 2012 23:50:14 GMT Etag: 84143864931d71cde18f6abda1cc0a42 X-Timestamp: 1342137014.67814 Content-Type: image/png X-Varnish: 2177807627 2170135886, 828582967 675124919, 4117677754 Via: 1.1 varnish, 1.1 varnish, 1.1 varnish Content-Length: 38707 Accept-Ranges: bytes Date: Tue, 09 Jul 2013 10:21:22 GMT Age: 138125 Connection: keep-alive X-Cache: cp1064 hit (62), cp3004 hit (925), cp3007 frontend miss (0) Access-Control-Allow-Origin: *

☑ 192.168.0.1:64941 => upload-lb.esams.wikimedia.org:80 * 373 bytes in 1 packet(s)
☑ upload-lb.esams.wikimedia.org:80 => 192.168.0.1:64941 * 39,259 bytes in 28 packet(s)
Total 39,632 bytes in 29 packet(s), Session time: 0 second(s)

By default, CommView for WiFi attempts to decompress GZIP'd web content and reconstruct images from binary streams. If you want to turn off this functionality, use the **Decoding** tab of the program's **Options** dialog.

You can filter out the data that came from one of the directions by unchecking one of the check boxes on the bottom pane. Incoming and outgoing data are marked with different colors for your convenience. If you want to change one of the colors, click **Settings** =>**Colors** and pick a different color. You can enable or disable word wrapping using the **Word Wrap** item in the **Settings** menu.

The **Display type** drop-down list allows you to view data in the **ASCII** (plain-text data), **HEX** (hexadecimal data), **HTML** (web pages and images), **EBCDIC** (IBM mainframes' data encoding), and **UTF-8** (Unicode data) formats. Please note that viewing data as HTML does not necessarily produce exactly the same results as the one you can see in the web browser (e.g. you will not be able to see inline graphics); however, it should give you a good idea of what the original page looked like.

You can choose the default display type for TCP Session Reconstruction window in the **Decoding** tab of the program's **Options** dialog.

The **Navigation** buttons allow you to search the buffer for the next or previous TCP session. The first forward button (>>) will search for the next session between those two hosts that were involved in the first reconstructed session. The second forward button (>>>) will search for the next session between any two hosts. If you have multiple TCP sessions between the two hosts in the buffer and you'd like to see them all one by one, it is recommended to start the reconstruction from the first session, as the back button (**<<**) cannot navigate beyond the TCP session that was reconstructed first.

The obtained data can be saved as binary data, HTML, text, or rich text file by clicking **File** =>**Save As**… . When saving in text format, the resulting file is a Unicode UTF-16 file. When saving in HTML format, the encoding of the resulting file depends on the currently selected **Display type**. If HTML is currently selected, the resulting file is an ANSI text file; for all other display types, the resulting file is a Unicode UTF-16 file. Note that if you are saving an HTTP session with images, the images in the saved HTML file are stored in the temporary location on your hard drive, so if you want to preserve them, open the saved file in your browser and re-save the file in a format that includes images, such as MHT, before closing CommView for WiFi.

You can search for a string in the session by clicking **Edit => Find**… .

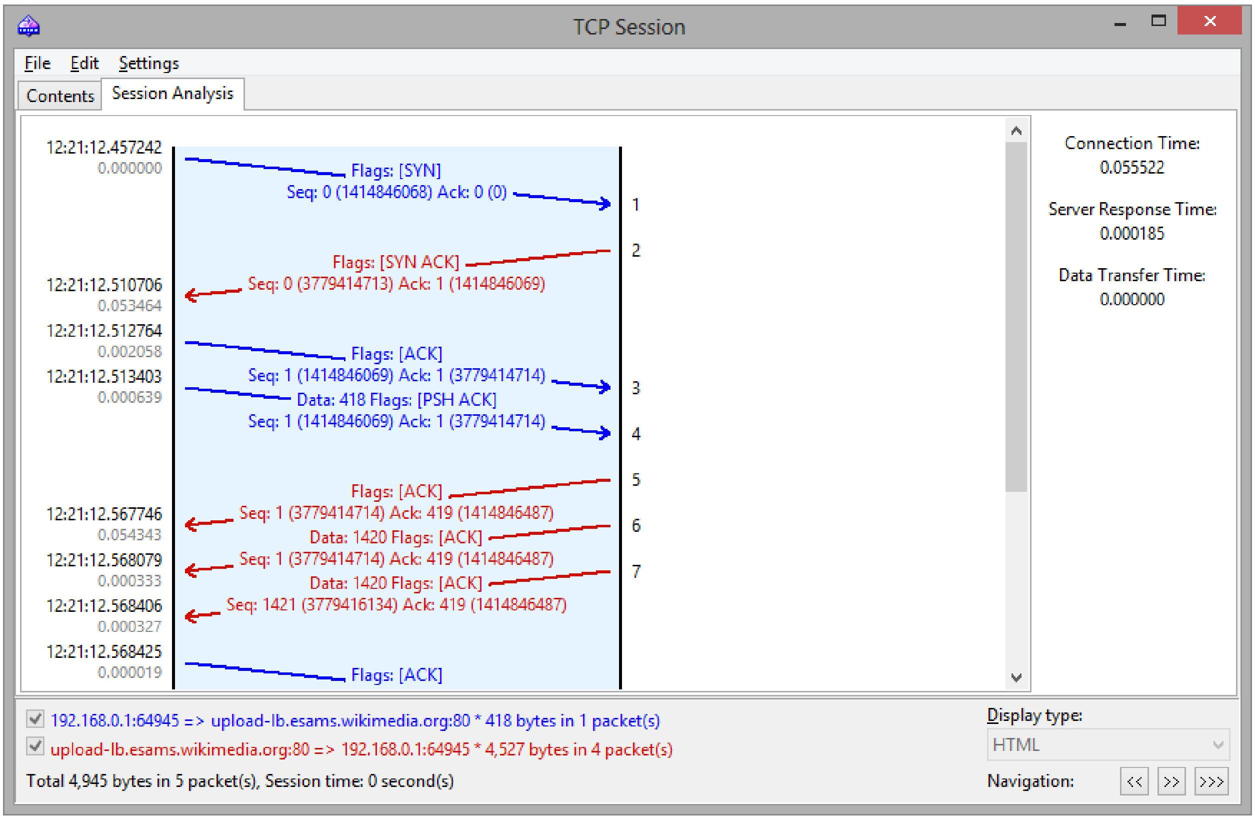
Session Analysis

The Session Analysis tab of the TCP Session window graphically displays the reconstructed TCP session. You can see the session data flow, errors, delays, and retransmissions of lost data.

The following data is displayed for every session packet:

- TCP flags.
- Absolute and relative SEQ and ACK values.
- Packet arrival time.
- Delta time between the current and previous packet.
- Packet number in the reconstructed session.

If a packet contains errors, the nature of the error is explained. It appears as a text description along the right edge of the graph. When you move the mouse over a packet, its contents are displayed in a hint window if the packet contains any data. Note that the **Display type** field affects the way the data is decoded in the hint window. A sample session analysis window is shown below:



12:21:12.457242
0.000000
Flags: [SYN]
Seq: 0 (1414846068) Ack: 0 (0)
1

2
Flags: [SYN ACK]
Seq: 0 (3779414713) Ack: 1 (1414846069)
12:21:12.510706
0.053464

12:21:12.512764
0.002058
Flags: [ACK]
Seq: 1 (1414846069) Ack: 1 (3779414714)
3

12:21:12.513403
0.000639
Data: 418 Flags: [PSH ACK]
Seq: 1 (1414846069) Ack: 1 (3779414714)
4

5
Flags: [ACK]
Seq: 1 (3779414714) Ack: 419 (1414846487)
12:21:12.567746
0.054343

6
Data: 1420 Flags: [ACK]
Seq: 1 (3779414714) Ack: 419 (1414846487)
12:21:12.568079
0.000333

7
Data: 1420 Flags: [ACK]
Seq: 1421 (3779416134) Ack: 419 (1414846487)
12:21:12.568406
0.000327

12:21:12.568425
0.000019
Flags: [ACK]

Connection Time:
0.055522

Server Response Time:
0.000185

Data Transfer Time:
0.000000

☑ 192.168.0.1:64945 => upload-lb.esams.wikimedia.org:80 * 418 bytes in 1 packet(s)

☑ upload-lb.esams.wikimedia.org:80 => 192.168.0.1:64945 * 4,527 bytes in 4 packet(s)

Total 4,945 bytes in 5 packet(s), Session time: 0 second(s)

Display type: HTML

The right pane shows some basic statistics for the given session:

Connection Time - the time it took to establish the TCP connection. In other words, it's the three-way TCP handshake time (SYN => SYN ACK => ACK).

Server Response Time - the time elapsed between the initial client request and the server's first data response.

Data Transfer Time - the time between the server's first and final data responses (0 if there was only one server response).

You can save the graphic layout of the reconstructed TCP session as a BMP, GIF, or PNG file by right clicking on the layout and selecting the **Save Image As...** menu item of the context menu. Sessions with a large number of packets will be split into multiple files.

Reconstructing UDP Streams

This tool is very similar to the TCP session reconstruction tool described in the previous chapter; please refer to it for more information. However, because unlike TCP, UDP is a connectionless protocol, the following distinctions exist between TCP session reconstruction and UDP stream reconstruction:

- There is no **Session Analysis** tab, as there are no sessions, SEQs or ACKs in UDP.
- Because there are no SYNs or FINs in UDP, all packets between the given pairs of IP addresses and ports are considered to belong to the same stream.

Searching Packets

To find packets matching a specific text or address, use the Find dialog (**Search => Find Packet**). Enter a search string, select the type of entered information (**String** or **Hex**), and then click **Find Next**. The program will search for packets that match the search criterion and display them on the **Packets** tab.

You can enter text as a string, hexadecimal value, MAC or IP address. Text string search will be performed in ASCII and Unicode (UTF-8 and UTF-16) formats. A hex string should be used when you want to enter non-printable characters: just type in the hexadecimal string, e.g. AD0A027804. Use of IPv6 addresses requires Windows XP or higher and that the IPv6 stack be installed.

Check **Match Case** for case-sensitive search. Check **At offset** to search for a string that begins at a certain offset. Note that the offset indicator is hexadecimal and zero-based (i.e. if you are looking for the first byte in the packet, the offset value is 0). You can also select a search direction, **Up** or **Down**.

Statistics and Reports

This window (**View => Statistics**) displays vital network statistics of your WLAN segment, such as packets per second rate, bytes per second rate, Ethernet protocols, and IP protocols and sub-protocols distribution graphs. You can copy any of the graphs to the clipboard by double-clicking on the graph. Ethernet protocols, IP protocols and sub-protocols "pie" graphs can be rotated using the small buttons in the lower right corner for better visibility of the slices.

The data displayed on each page can be saved as a bitmap or comma-delimited text file using the context menu or drag-and-drop. The **Report** page allows you to have CommView for WiFi automatically generate customizable reports in HTML or comma-delimited text formats.

Network statistics can be collected either by using all the data that passes through your network adapter or by using the rules that are currently set. If you want the statistics counters to process only the data (packets) that match the current rule set and ignore all other data, you should check the **Apply current rules** box.

General

Displays Packets per second and Bytes/Bits per second histograms, a bandwidth utilization gauge (traffic per second divided by the wireless adapter speed), as well as the overall packet and byte counters. Double-clicking on the gauge brings up a dialog window that allows you to manually configure the adapter speed to be used in the bandwidth utilization calculations.

Protocols

Displays the distribution of the Ethernet protocols, such as ARP, IP, SNAP, SPX, etc. Use the **Chart by** drop-down list to select one of the two available calculation methods: by number of packets or by number of bytes. If your WLAN uses WEP or WPA encryption, you must configure the WEP or WPA keys correctly to be able to decrypt network traffic; otherwise, this chart will be empty.

IP Protocols

Displays the distribution of the IP protocols. TCP, UDP, and ICMP. Use the **Chart by** drop-down list to select one of the two available calculation methods: by number of packets or by number of bytes. If your WLAN uses WEP or WPA encryption, you must configure the WEP or WPA keys correctly to be able to decrypt network traffic; otherwise, this chart will be empty.

IP Sub-protocols

Displays the distribution of the main IP application-level sub-protocols: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS, and DNS. To add more protocols, click on the **Customize** button. This dialog allows you to define up to 8 custom protocols. You should enter a protocol name, select the IP protocol type (TCP/UDP), and port number. Use the **Chart by** drop-down list to select one of the two available calculation methods: by number of packets or by number of bytes. If your WLAN uses WEP or WPA encryption, you must configure the WEP or WPA keys correctly to be able to decrypt network traffic; otherwise, this chart will be empty.

Sizes

Displays the packet size distribution chart.

Hosts by MAC

Lists active WLAN hosts by MAC address and displays data transfer statistics. You can assign aliases to MAC addresses. If you have too many multicast packets on your network and the Hosts by MAC table is overpopulated, you may want to group multicast addresses to one line that will be named GroupedMulticast. You can enable this function by checking the **Group multicast addresses** box. Please note that only the packets that arrived after this option has been set will be grouped accordingly, the previously received packets will not be affected by this option.

Hosts by IP

Lists active WLAN hosts by IP address and displays data transfer statistics. Since IP packets captured by the program can be originated from an unlimited number of IP addresses (both internal to your WLAN and external), by default this tab does not display any statistics. To have the statistics displayed, you should first set the range of IP addresses to be monitored by clicking **Add/Set Ranges**. Normally, these ranges should belong to your WLAN, and configuring the program to monitor a certain range of IP addresses allows you to have the usage statistics. You can enter any number of ranges, but the total number of IP addresses being monitored cannot exceed 1,000. To delete a range, right-click on the list of ranges and select the appropriate menu command. You can assign aliases to IP addresses. Additionally, you can check the **All** box to have the program list all IP addresses; however, this option is not recommended for RAM and CPU utilization reasons. If your WLAN uses WEP or WPA encryption, you must configure the WEP or WPA keys correctly to be able to decrypt network traffic; otherwise, this chart will be empty.

Matrix by MAC

This page displays the graphical conversation matrix between hosts based on their MAC addresses. The hosts represented by their MAC addresses are placed on the circle, and the sessions between them are shown as lines that connect the hosts. Moving the mouse over a host highlights all connections that this host makes with other hosts. You can change the number of the most active host pairs that are displayed in the matrix by changing the value in the **Most active pairs** field. To change the number of the latest address pairs examined by the program, modify the value in the **Latest pairs to count** field. If your network segment has many broadcast or multicast packets that overpopulate the matrix, you can ignore such packets by checking the **Ignore broadcasts** and **Ignore multicasts** boxes.

Matrix by IP

This page displays the graphical conversation matrix between hosts based on their IP addresses. The hosts represented by their IP addresses are placed on the circle, and the sessions between them are shown as lines that connect the hosts. Moving the mouse over a host highlights all connections that this host makes with other hosts. You can change the number of the most active host pairs that are displayed in the matrix by changing the value in the **Most active pairs** field. To change the number of latest address pairs examined by the program, modify the value in the **Latest pairs to count** field. If your network segment has many broadcast or multicast packets that overpopulate the matrix, you can ignore such packets by checking the **Ignore broadcasts** and **Ignore multicasts** boxes. If your WLAN uses WEP or WPA encryption, you must configure the WEP or WPA keys correctly to be able to decrypt network traffic; otherwise, this chart will be empty.

Report

This tab allows you to have CommView for WiFi automatically generate customizable reports in HTML (including images of charts and graphs) or comma -delimited text formats.

It is possible to have the program generate statistics on pre-captured data in addition to real-time statistics. To do that, load a capture file in Log Viewer and click **File => Generate Statistic**. You can optionally reset previously collected statistics displayed in the **Statistics** window. Please note that this function will not show packet distribution along the timeline. It is limited to displaying totals, protocol charts, and LAN host tables.

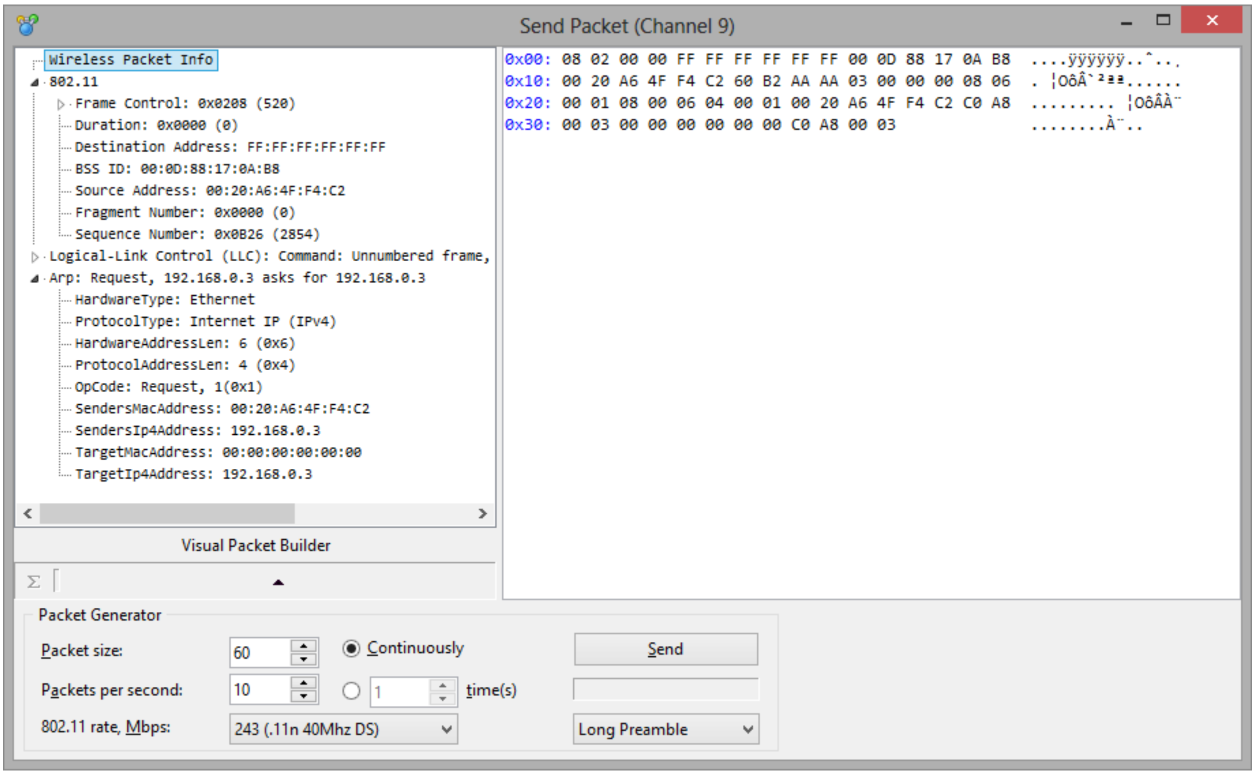
Using Aliases

Aliases are easy-to-remember human-readable names that CommView for WiFi will substitute for a MAC or IP address when showing the packets on the **Packets** and **Statistics** tabs. This can make packets easier to recognize and analyze. For example, 00:00:19:2D:0D:35 becomes GATEWAY2, and ns1.earthlink.com becomes MyDNS.

To add a MAC alias right-click on a packet and select **Create Alias Using Source MAC** or **Using Destination MAC** from the pop-up menu. A window will pop up where the MAC address field is already filled out, and you will only need to type in an alias. Alternatively, you can click **Settings** => **MAC Aliases**… and fill out the MAC address and Alias fields manually. To delete an alias or clear the entire aliases list, right-click on the Aliases window and select **Delete Record** or **Clear All**. The same applies to creating IP aliases. When a new IP alias is created by right-clicking on a packet, the alias field is pre-filled with the corresponding hostname (if available) which can then be edited by the user.

Packet Generator

This tool allows you to edit and send packets via your wireless network adapter. To open the Packet Generator, click **Tools => Packet Generator**, or select a packet from the **Packets** tab, right-click on it, and select the **Send Packet** command.



Send Packet (Channel 9)

```
Wireless Packet Info
802.11
  Frame Control: 0x0208 (520)
  Duration: 0x0000 (0)
  Destination Address: FF:FF:FF:FF:FF:FF
  BSS ID: 00:0D:88:17:0A:B8
  Source Address: 00:20:A6:4F:F4:C2
  Fragment Number: 0x0000 (0)
  Sequence Number: 0x0B26 (2854)
Logical-Link Control (LLC): Command: Unnumbered frame,
Arp: Request, 192.168.0.3 asks for 192.168.0.3
  HardwareType: Ethernet
  ProtocolType: Internet IP (IPv4)
  HardwareAddressLen: 6 (0x6)
  ProtocolAddressLen: 4 (0x4)
  OpCode: Request, 1(0x1)
  SendersMacAddress: 00:20:A6:4F:F4:C2
  SendersIp4Address: 192.168.0.3
  TargetMacAddress: 00:00:00:00:00:00
  TargetIp4Address: 192.168.0.3
```

```
0x00: 08 02 00 00 FF FF FF FF FF FF 00 0D 88 17 0A B8   ....ÿÿÿÿÿÿ..ˆ...
0x10: 00 20 A6 4F F4 C2 60 B2 AA AA 03 00 00 00 08 06   . ¦OôÂ`²ªª......
0x20: 00 01 08 00 06 04 00 01 00 20 A6 4F F4 C2 C0 A8   ......... ¦OôÂÀ¨
0x30: 00 03 00 00 00 00 00 00 C0 A8 00 03               ........À¨..
```

Packet Generator

Packet size: 60

Packets per second: 10

802.11 rate, Mbps: 243 (.11n 40Mhz DS)

● Continuously

○ 1 time(s)

Long Preamble

Please read the following important information about the limitations and peculiarities of using in the Packet Generator with wireless adapters:

- Do not use the Packet Generator unless you know exactly what effect you want to achieve. Sending packets may produce unpredictable results, and we strongly recommend refraining from using this tool unless you are an experienced network administrator.
- Your adapter firmware may fail to send certain packets, or it may send certain packets multiple times. This behavior is fully controlled by the firmware and is beyond our control.
- Your adapter firmware may disallow you to send packets at an arbitrary rate. It is quite possible that when you select the rate of 1000 packets per second, the firmware will actually send the packets at a much slower rate.

Please note that the Packet Generator cannot and should not be used for sending application-layer TCP streams, i.e. it cannot take care of incrementing SEQ or ACK values automatically, adjusting checksums and packet sizes and so forth. If you need to send a TCP stream, you should use a Winsock-based application specifically designed for that purpose. The Packet Generator is a tool for replaying pre-captured data, testing firewalls and intrusion detection systems, as well as for performing other specific tasks that require manual packet crafting.

The Packet Generator allows you to change the packet contents and have the packet decode displayed in the left window as you edit it. You can create packets of any kind; you have full control over the packet contents. For IP, TCP, UDP, and ICMP packets, you can automatically correct the checksum(s) by clicking on the **Sigma** button. To assist you with packet editing, the Visual Packet Builder tool is also available; click on the corresponding button to invoke it.

You can also click on the button with an arrow on it to display the list of available packet templates. The program comes with **TCP**, **UDP**, and **ICMP** packet templates; using them is often faster than typing hex codes in the editor window. These templates contain typical TCP, UDP, and ICMP packets, but you would most probably want to edit many packet fields and use meaningful values that suit your needs, such as real MAC and IP addresses, port numbers, SEQ and ACK numbers, etc. You can use your own templates rather than the built-in ones. You can drag-and-drop a packet from the CommView Packets tab to the Templates section in the Packet Generator window. If you drop several packets into the Templates section, only the first packet will be used as a template. An entry named New Template will appear in the list of templates. You can rename a template by right-clicking on it in the list and selecting **Rename**. If you need to delete a template, right-click on it and select **Delete** from the pop-up menu. Selecting a template in the list will load the packet that it contains in the editor window where it can be edited prior to sending.

You can also place NCFX files with the templates of your choice to the TEMPLATES subfolder in the application folder. If CommView for WiFi finds NCFX files (or just one of them) in the TEMPLATES subfolder, it will list them among the available templates in the drop-down list. These NCFX files should contain only one packet per file, but if you use a file that contains many packets, CommView for WiFi will load only the first one.

Once you have edited a packet, use the controls below to send it:

Packet Size – modifies the packet size.
Packets Per Second – controls the speed at which packets will be sent.
Continuously – select this option if you want the Packet Generator to send packets continuously until you click Stop.
Time(s) – select this option if you want the Packet Generator to send packet a given number of times.
802.11 rate – modifies the 802.11 rate to be used for sending packets. Depending on the currently selected band and channel, not all rates may be used. For example, 802.11a packets cannot be sent at the rate of 2 Mbps.
Long/Short Preamble – sets the preamble type for 802.11b and 802.11g packets. Not applicable to 802.11a.
Send/Stop – click this button when you are ready to send packets or to stop sending them.

Working with multiple packets

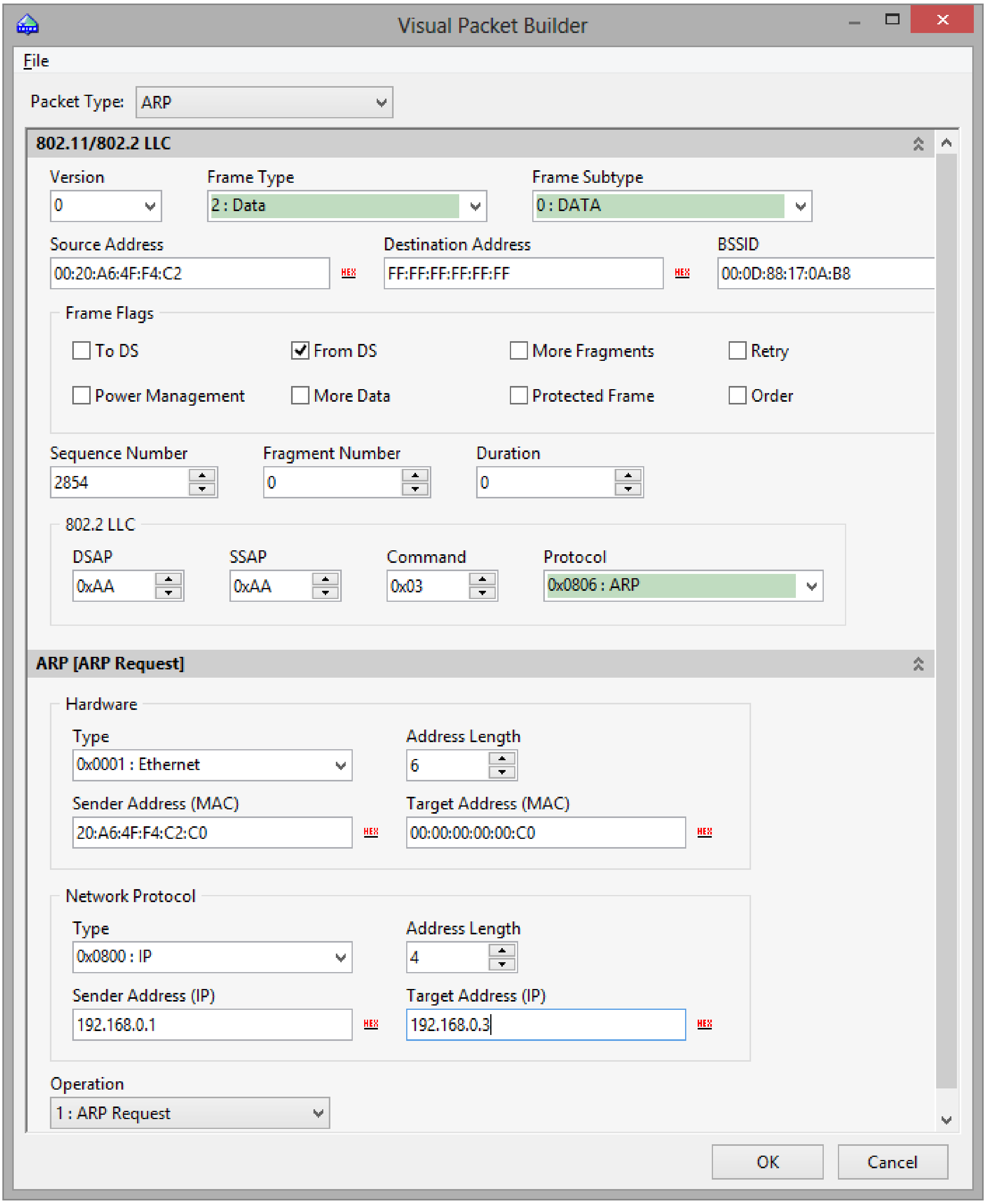
You can use the Packet Generator to send multiple packets at once. To do that, just select the packets you want to send in the list and invoke the Packet Generator using the right-click menu, or drag and drop the selected packets to the Packet Generator window. Alternatively, you can drag and drop capture files in all supported formats directly to the Packet Generator window. When multiple packets are being sent, the packer editor and decoder tree become invisible.

Saving edited packets

If you edited a packet and would like to save it, just drag the decoder tree to the desktop or any folder, and a new file in NCFX format containing the packet will be created. The file name is always PACKET.NCFX. You can also drag the packet to the templates window. If you need to edit and send multiple packets, edit them one by one, each time dragging a new packet to the desktop and renaming it. After that, open a new Log Viewer window, drag-n-drop the edited packets from the desktop to Log Viewer, select them using the Shift button, and invoke the Packet Generator using the context menu.

Visual Packet Builder

Visual Packet Builder is a tool designed for facilitating packet editing and generation in the Packet Generator. This tool allows you to quickly and correctly create a new packet or modify an existing one using ready-made templates. Once created or edited, a packet can be injected into the network using the Packet Generator.



Visual Packet Builder

Packet Type: ARP

802.11/802.2 LLC

Version: 0

Frame Type: 2 : Data

Frame Subtype: 0 : DATA

Source Address: 00:20:A6:4F:F4:C2

Destination Address: FF:FF:FF:FF:FF:FF

BSSID: 00:0D:88:17:0A:B8

Frame Flags

☐ To DS ☑ From DS ☐ More Fragments ☐ Retry

☐ Power Management ☐ More Data ☐ Protected Frame ☐ Order

Sequence Number: 2854

Fragment Number: 0

Duration: 0

802.2 LLC

DSAP: 0xAA

SSAP: 0xAA

Command: 0x03

Protocol: 0x0806 : ARP

ARP [ARP Request]

Hardware

Type: 0x0001 : Ethernet

Address Length: 6

Sender Address (MAC): 20:A6:4F:F4:C2:C0

Target Address (MAC): 00:00:00:00:00:C0

Network Protocol

Type: 0x0800 : IP

Address Length: 4

Sender Address (IP): 192.168.0.1

Target Address (IP): 192.168.0.3

Operation: 1 : ARP Request

Standard TCP, UDP, and ICMP (based on the 4th and 6th versions of IP protocol), and ARP packet generation is supported. To create a packet, select its type from the **Packet Type** drop-down list. The default values of the packet fields will be automatically filled in, but can be changed afterwards.

ICMP, TCP, UDP, and ARP packets consist of several encapsulated layers, and the interface of Visual Packet Builder is arranged the same way. Options that correspond to the same layer are located on a separate panel. For example, a TCP packet consists of 4 layers; the **Source MAC** and **Destination MAC** address fields are located on the **Ethernet II** panel (Data link layer), and **Src Port** and **Dst Port** values are located on the TCP panel (Transport layer). If you would like to hide a panel, click the **Expand/Collapse** button located in the right corner of the panel header.

Note that some "parental" layer values affect the packet type on lower layers; hence modifying upper layers may lead to rebuilding the lower layers of a packet. Therefore, if you change the **Protocol** type in the **Ethernet II** panel (Data link layer), it will lead to rebuilding the whole packet. Another peculiarity that you should keep in mind is that the values of some fields depend on the contents of other fields, as well as the data contents of the lower layers. Such fields are: checksums and header lengths, and/or data of lower layers. Visual Packet Builder calculates such values automatically. However, when creating non-standard packets, you may want to specify different values manually by checking the **Override default value** box and specifying the desired values.

IMPORTANT: Visual Builder helps you control the correctness of the packet being built by highlighting the headers and fields with incorrect or non-standard values in red.

Despite the fact that Visual Packet Builder has internal support for TCP, UDP, ICMP and ARP protocols only, you can still use it to edit packets that use other protocols. For such packets, you can use the hex editor to modify the data.

Once created, a packet can be saved and subsequently loaded to Visual Packet Builder again. Use the respective commands located in the **File** menu of Visual Packet Builder for loading/saving capture files. You can load any CommView for WiFi capture file (NCFX); however, if the file contains more than one packet, only the first one will be loaded.

NIC Vendor Identifier

The first 24 bits of a network card's MAC address uniquely identify the network card's vendor. This 24-bit number is called the OUI ("Organizationally Unique Identifier"). The NIC Vendor Identifier is a tool that allows you to look up a vendor name by MAC address. To look up a vendor name, click **Tools** =>**NIC Vendor Identifier**, enter a MAC address, and click **Find**. The vendor's name will be displayed. By default, CommView for WiFi replaces the first three octets of the MAC address by the adapter vendor name in the **Packets** tab. This behavior may be changed by unchecking the **Display vendor names in MAC addresses** checkbox in the **General** tab of the program **Options** dialog. The list of vendors is contained in the MACS.TXT file located in the CommView for WiFi application folder. You can manually edit this list to add/modify information.

Scheduler

You can use this tool to create and edit scheduled capturing tasks. This is useful when you want CommView for WiFi to start and/or stop capturing when you are not around, for example, at night or on weekends. To add a new task, click **Tools** => **Scheduler**, and then click on the **Add** button.

Use the **Start capturing** frame to specify the date and time when CommView for WiFi will start capturing. Use the **Channel** drop-down list to specify the WLAN channel that should be monitored. Use the **Stop capturing** frame to specify the date and time when CommView for WiFi will stop capturing. You do not necessarily have to check both **Start capturing** and **Stop capturing** boxes. If you check only the first box, capturing would go on until you manually stop it. If you check only the second box, you would have to start capturing manually, but then CommView for WiFi would automatically stop capturing at the specified time.

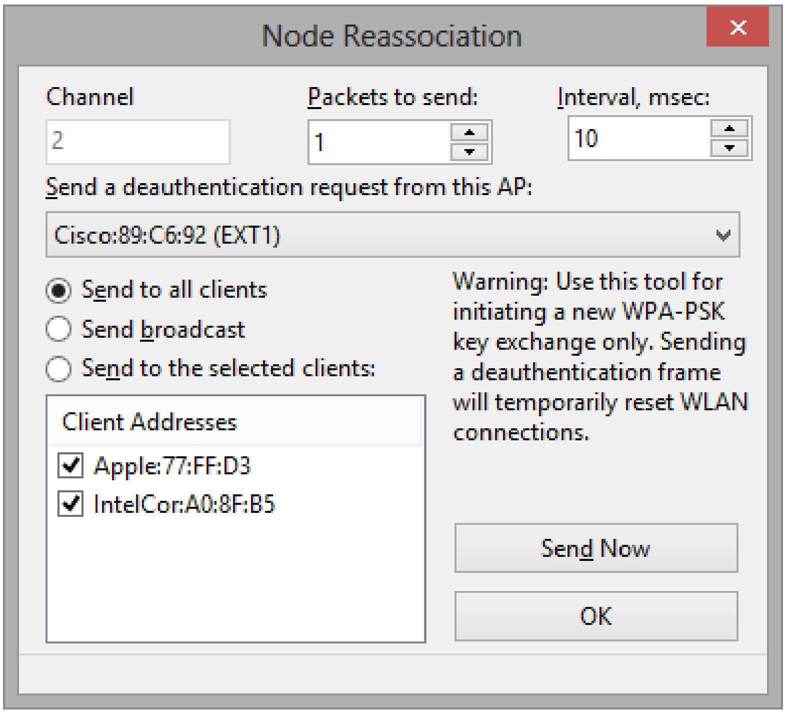
If CommView for WiFi is already capturing packets at the time when the scheduled task is due and if the adapter you specified is different from the adapter currently being monitored, CommView for WiFi will stop capturing, switch to the adapter you specified, and restart capturing.

It is important to understand that the scheduled tasks can be performed only when CommView for WiFi is running.

Node Reassociation

Given the dynamic nature of WPA encryption, knowing the WPA passphrase alone does not allow you to decrypt traffic immediately after entering the correct passphrase. To be able to decrypt WPA-encrypted traffic, CommView for WiFi must be running and capturing packets during the key exchange phase (key exchange is carried out using the EAPOL protocol). Please refer to the Understanding WPA Decryption chapter for detailed information.

The Node Reassociation tool can be used for initiating a new key exchange:



Node Reassociation

Channel: 2

Packets to send: 1

Interval, msec: 10

Send a deauthentication request from this AP: Cisco:89:C6:92 (EXT1)

● Send to all clients
○ Send broadcast
○ Send to the selected clients:

Client Addresses
☑ Apple:77:FF:D3
☑ IntelCor:A0:8F:B5

Warning: Use this tool for initiating a new WPA-PSK key exchange only. Sending a deauthentication frame will temporarily reset WLAN connections.

This tool simply sends a deauthentication request to the selected stations on behalf of the access point. This causes the stations to reassociate with the access point. The reassociation process usually takes a second and lets CommView for WiFi capture EAPOL packets necessary for WPA-PSK decryption. Do not use this tool unless you need to decrypt WPA-PSK traffic on your WLAN.

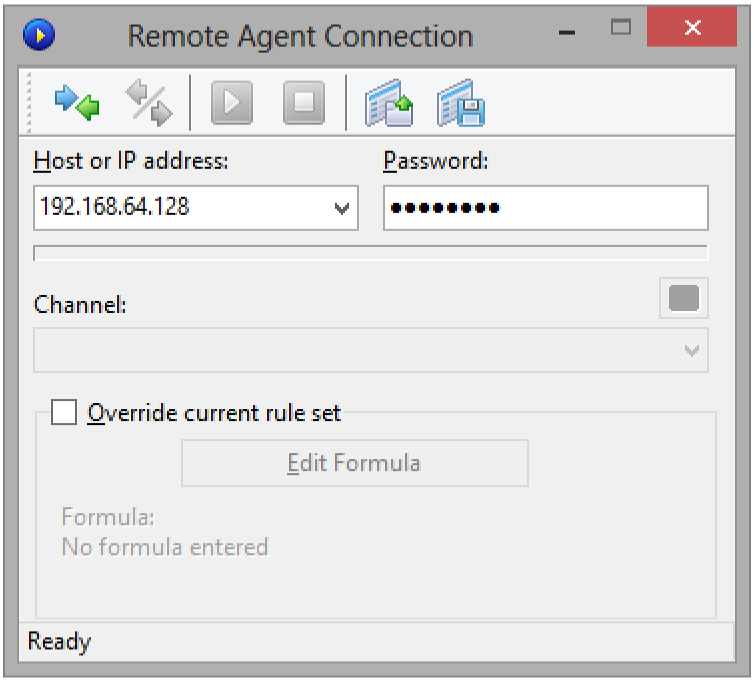
To initiate a reassociation, select an access point from the drop-down list, select the stations, and click **Send**. The **Send to all clients** and **Send to selected clients** options send unicast packets to all or selected clients. The **Send broadcast** option sends a broadcast packet to the FF:FF:FF:FF:FF:FF address. While this option covers even undetected stations, some stations may ignore broadcast deauthentication requests. You may want to send several packets using the **Packets to send** and **Interval** boxes.

Using Remote Agent for WiFi

CommView Remote Agent for WiFi is a companion product that can be used for monitoring network traffic remotely. All you have to do is to install Remote Agent for WiFi on the target computer, and then use CommView for WiFi to connect to Remote Agent. Once you are connected and authenticated, you can start monitoring as if you were there.

> IMPORTANT: This chapter describes how to use CommView for WiFi to connect to Remote Agent and capture traffic remotely. For detailed information on Remote Agent installation and configuration, please refer to the help file that comes with Remote Agent. It is highly recommended that you carefully read the Remote Agent documentation prior to using it. CommView Remote Agent for WiFi can be downloaded from our website.

To switch to remote monitoring mode, click **File** => **Remote Monitoring Mode**. An additional toolbar will appear in the CommView for WiFi main window next to the main toolbar. If you are behind a firewall or proxy server, or using a non-standard Remote Agent port, you may need to click on the **Advanced Network Settings** button to change the port number and/or enter SOCKS5 proxy server settings. The **Advanced Network Settings** dialog also allows you to define whether Remote Agent will apply the filtering rules locally, or send all the captured traffic to CommView for WiFi; this will be discussed in detail later in this chapter.



Host or IP address: 192.168.64.128

Password: ●●●●●●●●●

☐ Override current rule set

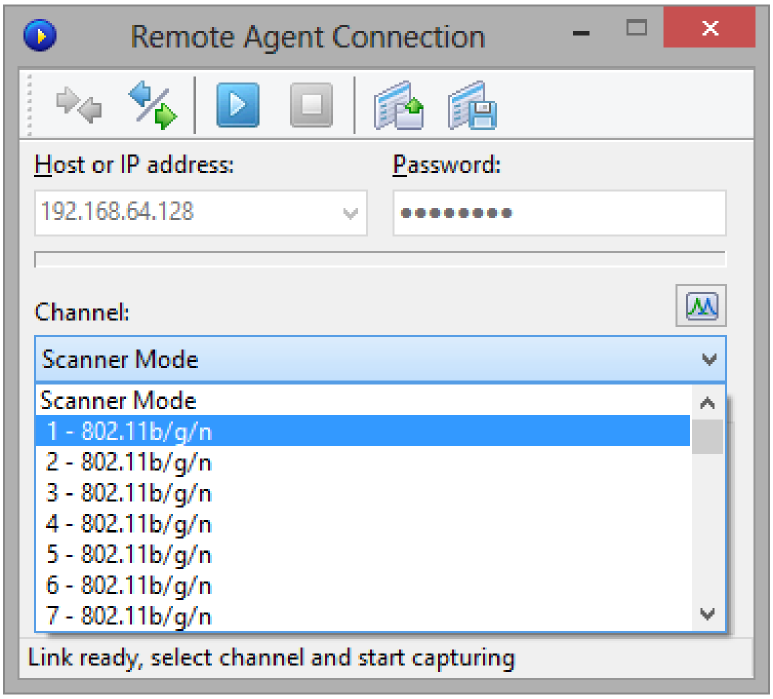
Formula:
No formula entered

Ready

Click on the **New Remote Agent Connection** button to establish a new connection, or click on the **Load Remote Agent Profile** toolbar button to load a previously saved Remote Agent connection profile. A previously saved profile may also be loaded from the New Remote Agent Connection window.

A Remote Agent Connection window will appear. Enter the IP address of the computer running CommView Remote Agent for WiFi into the IP address input area, enter the connection password and click on the **Connect** button. If the password is correct, a connection will be established. You will then see the *Link Ready* message in the status bar and the channel selection box will list the channels supported by the wireless adapter installed on the remote computer. In addition to the channel list, a special **Scanner Mode** item will be added as the first item on the list.

If you select **Scanner Mode**, the remote wireless adapter will cycle through the available channels, capturing data from each of them for several seconds. The small button located on the right side of the window, just above the channel selection box, allows you to adjust the scanner settings. Click on this button to select the channels to be monitored in Scanner Mode and set the interval, i.e. the number of seconds per channel.


Remote Agent Connection

Host or IP address: 192.168.64.128

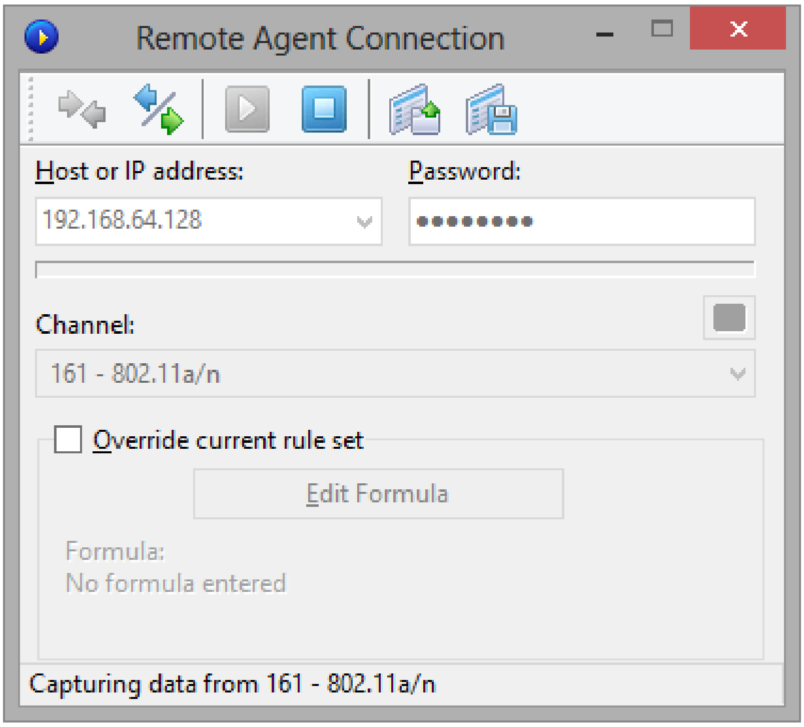
Password: ●●●●●●●●●

Channel: Scanner Mode

Scanner Mode
1 - 802.11b/g/n
2 - 802.11b/g/n
3 - 802.11b/g/n
4 - 802.11b/g/n
5 - 802.11b/g/n
6 - 802.11b/g/n
7 - 802.11b/g/n

Link ready, select channel and start capturing

Now is the best time to configure the capturing rules using the **Rules** tab in the CommView for WiFi main window. You can also apply a custom set of capturing rules to this connection and override the current rules defined in CommView for WiFi by checking the **Override current rule set** box, clicking on the **Edit Formula** button and entering the rules formula in the field below. The formula syntax is the same as the one used in Advanced Rules. Once you are ready to start monitoring, select the channel from the list and click the **Start Capture** toolbar button. CommView for WiFi allows you to save the Remote Agent Connection settings as a connection profile for quick and easy access in the future. Click on the **Save Remote Agent profile** toolbar button in the New Remote Agent Connection window and enter a name for the file.



Remote Agent Connection

Host or IP address: 192.168.64.128

Password: ●●●●●●●●●

Channel: 161 - 802.11a/n

□ Override current rule set

Edit Formula

Formula:
No formula entered

Capturing data from 161 - 802.11a/n

CommView for WiFi will start to capture the remote adapter's traffic as if it is your local network traffic; there is virtually no difference between using CommView for WiFi locally or remotely. When you are done with remote monitoring, just click on the **Stop Capture** toolbar button. You can then change the channel or disconnect from Remote Agent by clicking the **Disconnect** toolbar button. To return to the standard mode, click **File** => **Remote Monitoring Mode**, and the additional toolbar will disappear.

Please note that CommView for WiFi can work with multiple Remote Agents simultaneously. You can open several remote connections, each having its own settings and an independent set of rules and collect the traffic from remote WLANs in one CommView for WiFi instance.

How to Use CommView Remote Agent for WiFi Efficiently

Agent to CommView for WiFi. As mentioned before, Remote Agent should be installed on a computer that has a compatible wireless adapter (to be used for monitoring) and Ethernet adapter (to be used for the connection between Remote Agent and CommView for WiFi).

By default, Remote Agent sends all the collected packets back to CommView for WiFi, regardless of the capturing rules that may be configured in CommView for WiFi. This is done for providing correct statistical data and decryption, as well as the means for correct identification of wireless nodes. Since a fully loaded Wi-Fi network may have a bandwidth of about 1 Gbit/s, it's important that the wired link between Remote Agent and CommView for WiFi be capable of handling this bandwidth. In a modern office environment, where Gigabit networks are common, a single Gigabit adapter can easily receive data from a dozen Remote Agents.

There are situations where a fast connection is problematic. For example, a high bandwidth connection may not be available if you are monitoring a remote WLAN over the Internet. Even a T3 connection (4.5 Mbit/s) is insufficient to transfer all packets from a moderately loaded WLAN. In such situations, you can change the default setting and make Remote Agent filter the packets before they are transferred to CommView for WiFi. The Advanced Network Settings button on the additional remote monitoring toolbar in the main CommView for WiFi window allows you to enable the Minimize bandwidth option. When this option is enabled, the current CommView for WiFi rule set is periodically sent to Remote Agent. This rule set is then applied locally, so that only those packets that pass the rules are sent back to CommView for WiFi. In this mode, the Nodes may not display any nodes, and the Channels tab will not show full per-channel statistics, so use this mode only when you have limited bandwidth, but still need access to the packets from a remote WLAN.

For the same bandwidth reasons, it is highly recommended to NOT use a wireless connection for exchanging data between Remote Agent and CommView for WiFi. It is also a bad idea because the monitoring wireless adapter would pick up the packets sent by the wireless adapter being used for communicating with CommView for WiFi if they operate on the same or close channels. This will simply cause the snowball effect.

If CommView Remote Agent for WiFi captures more data than it can send to CommView for WiFi, it uses an internal buffer to store the packets that cannot be sent immediately. The buffer size is 5 Mbytes. The Buffer utilization indicator in the Remote Agent window shows the current status of the buffer. For example, if the program has buffered 2.5 Mbytes of data, the buffer utilization is 50%. If/when the buffer utilization reaches 100%, the program stops buffering data and discards captured packets until some buffer space is free.

Security

CommView Remote Agent for WiFi was made with security in mind. It can be accessed only by using a password that is never transmitted in plain text and that is ensured by using a challenge-response protocol with a secure hash function. If the authentication is successful, all transmitted traffic is compressed and then encrypted with the same password. Please take precautions to keep your password secret. Once it is revealed to an unauthorized person, that person will have broad capabilities to study your network and intercept network traffic on the remote computer.

Using RPCAP

IMPORTANT: This chapter describes experimental functionality that might or might not work as expected depending on the specific implementation in third party software and hardware. No technical support will be provided for this functionality.

In addition to the remote capture functionality provided by CommView Remote Agent, CommView for WiFi can also capture traffic from remote computers using the RPCAP (Remote Packet Capture) protocol. This protocol is supported by some hardware (e.g. Aerohive Access Points) and software (e.g. WinPcap).

To switch to remote monitoring mode, click **File** => **Remote Monitoring Mode**. An additional toolbar will appear in the CommView for WiFi main window next to the main toolbar. Click the **New RPCAP Connection** button to open a new connection window.

To connect to a remote device, enter its **hostname or IP address,** specify the **port** number (RPCAP uses port 2002 by default), check the **User Authentication** box and specify a **user name** and **password**, if authentication is required, and then check the **Promiscuous mode** box if that is the capture mode you wish to use. Click **Connect** to establish a connection. Once the connection has been established, the **Adapter** drop-down list will be populated by available network interfaces. Click **Capture** to start capturing.

Using Aruba Remote Capture

> IMPORTANT: This chapter describes experimental functionality that might or might not work as expected depending on the specific implementation in third party software and hardware. No technical support will be provided for this functionality.

In addition to the remote capture functionality provided by CommView Remote Agent, CommView for WiFi can also capture traffic from access points manufactured by Aruba.

To switch to remote monitoring mode, click **File** => **Remote Monitoring Mode**. An additional toolbar will appear in the CommView for WiFi main window next to the main toolbar. Click the **New Aruba Remote Capture** button to open a new connection window.

Remote packet capture must be initiated on the AP side using the command-line interface. Aruba remote capture uses the following syntax:

```
pcap start <interface-mac> <target-ipaddr> <target-port> 4 <maxlen>
```

Example:

```
pcap start 18:64:72:e3:6a:10 192.168.0.2 5000 4 2346
```

Once you have configured remote capture on the AP side, specify the **port** number that you have chosen and click **Connect** to begin receiving packets from your Aruba AP.

Port Reference

This window (**View => Port Reference**) displays a table of port numbers and corresponding service names. This reference is obtained from the SERVICES file installed by Windows. You can find it in the **C:\windows\system32\drivers\etc** folder. You can manually edit this file if you want to add more ports/service names. CommView for WiFi reads this file on start up, so your changes to the file will be displayed only after you restart the program.

Setting Options

You can configure some of the program's options by selecting **Settings => Options** in the menu.

General

Auto-start capturing – check this box if you want CommView for WiFi to start capturing packets immediately after launching the program. Please select the channel that you would like to monitor from the drop-down list.

Disable DNS resolving – check this box if you do not want CommView for WiFi to perform reverse DNS lookups of the IP addresses. If you check it, the **Hostname** column on the **Latest IP Connections** tab will be blank.

Convert numeric port values to service names – check this box if you want CommView for WiFi to display service names rather than numbers. For example, if this box is checked, port **21** is shown as **ftp**, and port **23** as **telnet**. The program converts numeric values to service names using the SERVICES file installed by Windows. You can find it in the **C:\Windows\system32\drivers\etc** folder. You can edit this file manually if you want to add more ports/service names.

Convert MAC addresses to aliases – substitute MAC addresses for aliases on the **Packets** tab. Aliases can be assigned to MAC addresses using the **Settings =>MAC Aliases** menu command.

Convert IP addresses to aliases – substitute IP addresses for aliases on the **Packets** and **Statistics** tabs. Aliases can be assigned to IP addresses using the **Settings =>IP Aliases** menu command.

Convert IP addresses to hostnames in the "Packets" tab – check this box if you want CommView for WiFi to show resolved hostnames rather than IP addresses in the **Packets** tab. If this box is checked, CommView for WiFi will first attempt to find an alias for the given IP address. If no alias is found or the previous box (**Convert IP addresses to aliases**) is not checked, CommView for WiFi will query the internal DNS cache for the hostname. If no hostname is found, the IP address will be displayed in numeric form.

Display vendor names in the MAC addresses – by default, CommView for WiFi replaces the first three octets of the MAC address by the adapter vendor name in the **Packets** tab. Uncheck this checkbox if you want to change this behavior.

Capture Damaged Packets – because of the distance, radio interference, and other physical phenomena, some packets received by your wireless adapter might be damaged, i.e. contain partly or fully invalid data. Check this box if you want the program to capture and display such packets. This option has both drawbacks and advantages. The advantage is that if you are located far away from WLAN stations and/or access points, a high percentage of packets might be broken, and enabling this option would allow you to see more data, even though the data might be partly damaged. However, the drawback is that you would see some packets with invalid data, e.g. you might see IP packets sent to non-existent IP addresses. Also, when this box is checked, the program will try to decrypt those WEP- or WPA-encrypted packets in which the Integrity Check Value is incorrect, but the headers appear to be valid.

Memory Usage

Display

Maximum packets in buffer – sets the maximum number of packets the program stores in the memory and can display in the packet list (2nd tab). For example, if you set this value to 3000, only the last 3000 packets will be stored in the memory and packet list. The higher this value is, the more computer resources the program consumes.

Note that if you want to have access to a high number of packets, it is recommended that you use the auto-saving features (see Logging for more information): it allows you to dump all the packets into a log file on the hard drive.

Maximum Latest IP Connections lines – sets the number of lines the program displays on the Latest IP Connections tab. When the number of connections exceeds the limit, the connections that have been idle for the longest period of time are removed from the list.

Driver Buffer – sets the driver buffer size. This setting affects the program's performance: the more memory allocated for the driver buffer, the fewer packets the program drops. For low traffic WLANs, the buffer size is not critical. For high traffic WLANs, you may want to increase the buffer size if the program drops packets. To check the number of dropped packets, use the **File => Performance Data** menu command while capturing is on.

Latest IP Connections

Display Logic – allows you to select the Latest IP Connections layout that best suits your needs. Selecting an item from the drop-down list will display the description of the selected logic. In most cases, it is recommended to use the default **Smart** logic.

Define Local IP Addresses – you should use this tool if you monitor WLAN traffic with many pass-through packets and a mixture of external and internal IP addresses. In such a situation, CommView for WiFi does not "know" which IP addresses should be treated as local and might reverse the IP addresses in the Source and Destination IP columns. This tool allows you to define the local network addresses and subnet masks to make sure the Latest IP Connections window works correctly. This will work only if you use the default **Smart** logic.

Colors

Packet color – sets the colors for displaying different kinds of packets (Normal, Bad CRC, Bad ICV) on the **Packets** tab.

Colorize Packet Headers – check this box if you want CommView for WiFi to colorize packet contents. If this box is checked, the program displays the first eight packet layers using different colors. To change a color, select the type of header for which you want to change the color and click on the colored rectangle.

Formula syntax highlighting – sets the colors for highlighting keywords in formulas in the Advanced Rules window.

Selected byte sequence color – sets the font and background color for displaying the byte sequence that was selected in the decoder tree. For example, when you select the "TCP" tree node, the corresponding part of the packet will be highlighted using these colors.

Management frame color – sets the colors for different types of Management frames. Color is used in the **Protocol** column of the **Packets** tab to show the corresponding frame types.

Decoding

Always fully expand all nodes in the decoder window – check this box if you would like to have all nodes in the decoder windows automatically expanded when you select a new packet in the packet list.

Expand the last nodes – check this box if you would like to have the last node(s) in the decoder window automatically expanded when you select a new packet in the packet list and set the number of nodes to be expanded. By default, the first node is expanded. This setting has no effect if the **Always fully expand all nodes in the decoder window** box is checked.

Expand level – set the number of levels to expand. This defines the "depth" of tree node expansion.

Decode up to the first level only in ASCII export – this option affects the decoding format used when you export a packet log or individual packet as an ASCII file with decoding. If this box is checked, only the top-level nodes will be saved. For example, if you save a TCP/IP packet when this option is disabled, all *Type of service* sub-nodes are saved. When this option is enabled, these sub-nodes are not saved. Checking this box makes the output ASCII file less detailed and more compact.

Ignore incorrect checksums when reconstructing TCP sessions – this option affects the way CommView for WiFi treats malformed TCP/IP packets when reconstructing TCP sessions. By default, this option is on, and packets with incorrect checksums are not discarded in the process of reconstruction. If you turn off this option, packets with incorrect checksums will be discarded and not displayed in the TCP reconstruction window.

Include packet numbers when reconstructing TCP sessions – check this box if you'd like the chunks of data shown in the TCP session reconstruction window to be prepended by the packet numbers that correspond to these chunks of data.

Search for the session start when reconstructing TCP sessions – if this box is checked, the program will attempt to find the beginning of the TCP session when you reconstruct it. If it is not checked, the session will be reconstructed only from the selected packet, i.e. earlier packets will be discarded.

Decompress GZIP content – check this box if you want CommView for WiFi to convert GZIP-compressed HTTP content into readable text in the TCP Session Reconstruction windows. GZIP content is decompressed only when the display type in the window is set to "ASCII."

Reconstruct images – check this box if you want CommView for WiFi to convert binary HTTP streams that represent images into viewable JPG, BMP, PNG, and GIF pictures in the TCP Session Reconstruction windows. Images are shown only when the display type in the window is set to "HTML." Images are never shown within the HTML pages to which they belong, as they are transferred by the server in a separate HTTP session.

Use IPv4-style endings in IPv6 addresses – if this box is not checked, IPv6 addresses are shown using hexadecimal symbols only, e.g. fe80::02c0:26ff:fe2d:edb5. If this box is checked, the last 4 bytes of IPv6 addresses are shown using the IPv4-style dotted notation, e.g. fe80::02c0:26ff:254.45.237.181.

Reassemble fragmented IP packets – check this box if you would like the program to reassemble IP packets that are fragmented. By default, fragmented IP packets are displayed as they were received from the wire, in their original form. If this option is turned on, the program will maintain an internal buffer of fragments and will attempt to "glue" them, displaying only the results of successful reassembly.

Display signal level in dBm – check this box if you would like the program to display signal strength in dBm rather than in percentile format. The availability of signal level in dBm depends on the wireless adapter model being used. Please refer to the Understanding Signal Strength chapter for more information.

Default display type – select the display type value from the drop-down list that you want to set as default for the TCP Session Reconstruction function. The available values are ASCII, HEX, HTML, and EBCDIC.

VoIP

> IMPORTANT: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

Disable VoIP analysis – disables capture and analysis of VoIP data. Check this box if you do not plan to work with VoIP and want to minimize the usage of computer resources by the application.

Maximum records in the list – limits the number of displayed and processed VoIP events. When the number of records exceed the specified limit, older records are deleted from the lists.

Ignore orphan RTP streams – when this box is checked, VoIP analyzer will ignore captured RTP data streams that do not have a parent signaling session. Orphan RTP streams typically appear if packet capturing was started in the middle of a call, or the signaling protocol is unknown to the application (i.e. not SIP and not H.323), or the signaling protocol was sent in a non-standard manner (e.g. encrypted or as part of some other session). Such streams are still available for analysis, and sometimes for playback. Please see the Call Playback chapter for more detailed information on playing VoIP calls. If you are not interested in such orphan streams and want to save on computer resources, please disable this option. Note that when orphan streams are not ignored, VoIP analyzer may mistakenly identify data transferred over UDP protocol as RTP streams. Generally, this is not an error, as RTP packets do not have a standard uniform signature, so such "false positives" are ok.

Ignore damaged packets in VoIP analyzer – when this box is checked, wireless packets with bad CRC will be discarded by the VoIP analysis module. This prevents the application from creating "ghost" signaling or media streams that may appear if packets with bad CRC are not dropped.

Geolocation

Geolocation is IP-to-country mapping for IP addresses. When this functionality is enabled, CommView for WiFi checks the internal database to provide information on the country any IP address belongs to. You can configure the program to show **ISO country code**, **Country name**, or **Country flag** next to any IP address. You can also disable geolocation. For some IP addresses, such as reserved ones (e.g. 192.168.*.* or 10.*.*.*) no information on the country can be provided. In such cases, the country name is not shown, or if you use the **Country flag** option, a flag with a question mark is displayed.

As IP allocation is constantly changing, it is important that you always have an up-to-date version of CommView for WiFi. A fresh, up-to-date database is included in every CommView for WiFi build. A fresh database has 98% accuracy. Without updates, the accuracy percentage falls by approximately 15% every year.

Miscellaneous

Hide from the taskbar on minimization – check this box if you do not want to see the program's button on the Windows taskbar when you minimize the program. If this box is checked, use the program's system tray icon to restore it after minimization.

Prompt for confirmation when exiting the application – check this box if you would like the program to ask you for a confirmation when you close it.

Auto-scroll packet data window – if this box is checked, the program scrolls the text of the packet data window automatically when you select a new packet from the packets list (but only if the text does not fit into the window). This is useful when you want to see the contents of a long packet without manually scrolling the window.

Auto-scroll packet list to the last packet – if this box is checked, the program automatically scrolls the packet list in the **Packets** tab down to the last received packet.

Auto-sort new records in Latest IP Connections – if this box is checked, the program auto-sorts new records on the Latest IP Connections tab based on the user-defined sorting criterion (e.g. ascending order of remote IP addresses).

Smart CPU utilization control – if this box is checked, the program tries to decrease CPU utilization when capturing high-volume traffic by decreasing the quality and frequency of the screen updates.

Run on Windows startup - if this box is checked, the program is launched automatically every time you start Windows. Under Windows Vista and higher, this box is disabled if UAC is enabled. This is a limitation of Windows Vista and newer Windows versions that prevents applications with elevated rights from loading on startup. If this feature is important, disable UAC.

Run minimized – if this box is checked, the program is launched minimized and the main window is not displayed until you click on the tray icon or taskbar button.

Show gridlines – makes the program draw gridlines in all packet, channel, and AP lists.

Enable automatic application updates – check this box to let the program connect to the TamoSoft Web site periodically and check for updates. Use the **Interval between checks** box to configure how often the checks should be made.

Plug-ins

This tab is used by 3rd party plug-ins for performing configuration tasks. Please see Custom Decoding for more information.

Frequently Asked Questions

In this chapter, you can find answers to some of the most frequently asked questions. The latest FAQ is always available at http://www.tamos.com/products/commwifi/faq.php

Q. I'm on a wireless network, and I want to monitor my own inbound and outbound packets. Which product do I need: the standard, non-wireless CommView edition, or CommView for WiFi?

A. You need the standard, non-wireless CommView edition. It will allow you to monitor your own traffic, but you will not be able to see the traffic of other WLAN stations. Unlike the standard CommView edition, CommView for WiFi allows you to monitor other wireless stations, capture management frames, view signal strength, etc.

Q. Do I need special hardware to use CommView for WiFi?

A. Yes, you need a compatible wireless adapter. The list of compatible adapters can be found at http://www.tamos.com/products/commwifi/. In order to enable the monitoring features of your wireless adapter, you will need to use the special drivers that come with this product. When CommView for WiFi is not running, your adapter will be able to communicate with other wireless hosts or access points, just like when you are using the original driver supplied by the adapter manufacturer. When CommView for WiFi is running, your adapter will be put in passive, promiscuous monitoring mode.

Q. My card is not on your list of supported hardware. What are my options?

A. Our hardware compatibility list includes only those cards that we have tested ourselves in our test lab. There are other cards that may be compatible with CommView for WiFi. The best way to find out if your card is compatible is downloading our Adapter Test Utility and running it on your computer. If a compatible adapter is installed, the utility will display its name. Before running our test utility, make sure that you use the latest driver supplied by your computer or adapter vendor. Visit their Web site to download and install the latest driver version. This is important, because the results of the test depend on the driver that is used. The newer the driver, the better the chances that it will work with CommView for WiFi. Finally, you may want to buy a compatible card, as they are not terribly expensive these days. Or simply order a boxed version from us; it comes with a compatible USB adapter.

Q. What adapter would you recommend for use with your application?

A. We suggest that you refer to the list of compatible hardware, which can be found at http://www.tamos.com/products/commwifi/adapterlist.php . By using this list, you choose the best adapter based on the form factor (USB, Integrated, etc.), sensitivity, supported Windows version, and supported 802.11 bands. Generally, the best choice would be an 802.11ac USB adapter.

Q. Which supported adapters have external antenna connectors?

A. Alfa Networks AWUS1900 and Alfa Networks AWUS036ACM.

Q. Can I capture data from multiple channels simultaneously?

A. Yes, if you use multiple supported USB adapters. Please refer to the Multi-Channel Capturing chapter for more information.

Q. I have installed the special driver for my adapter and now the adapter cannot connect to my wireless network after I close CommView for WiFi. What could be the problem?

A. When you replace the driver for your adapter, the configuration settings (including preferred networks and passwords) may be lost, so you may have to re-configure the adapter. If your adapter has been configured and still cannot connect, please disable and re-enable it in Device Manager, this will restore the connectivity.

Q. Some of the channels are not available in the channel selection controls. Is this normal? What if want to monitor these channels?

A. The answer depends on the adapter:

- Intel 7xxx, 8xxx, 9xxx, and AX2xx integrated adapters, recommended Realtek-, MediaTek-, and Ralink-based USB adapters, and Atheros-based USB adapters: All channels are always available when using them in CommView for WiFi.
- Atheros-based miniPCI and miniPCIe adapters: Depending on your country, your wireless adapter may not support all the channels shown in that window. The channels that are available for use in a particular country differ according to the regulations of that country. In the United States, for example, FCC regulations only allow channels 1 to 11 to be used in the 2.4 GHz band. The firmware of the wireless adapters being sold in the US is typically configured to disallow channels 12 and 13.
- Other adapters (e.g. Dell or Broadcom): enabling channels 12 and 13 may be possible. Open the CommView for WiFi application folder (usually C:\Program Files (x86)\CommViewWiFi). You will see the file named ch1213.exe there. Double-click on that file to execute it. Restart CommView and these channels will become available for selection. Note that the adapter's ability to capture packets on channels 12 and 13 depends on the regulatory domain set by the laptop vendor. If the vendor enabled them in your case, there won't be a problem. However, we've heard of many examples when laptop vendors did not enable channels 12 and 13 even in the laptops that were sold in a country where these channels were legal.

Q. When monitoring a WLAN, can I be sure that the program will capture every packet being sent or received?

A. No, and here is why. When a wireless station is connected and authenticated, the station and access point(s) employ a mechanism that allows them to resend the packets that were not received by the other party or damaged en route for some reason (e.g. radio interference). In case of CommView for WiFi, the wireless adapter is put into passive, monitoring mode. Therefore, the adapter cannot send "requests" to have packets resent, nor can it acknowledge successful receipt of packets. This results in loss of some packets. The percentage of lost packets may vary. Generally, the closer to other stations and access points you are, the fewer packets will be dropped.

Q. Can the program decrypt WPA- and WPA2-encrypted packets?

A. Yes, in WPA-PSK mode. Both TKIP (WPA) and AES/CCMP (WPA2) are supported. WPA3 cannot be decrypted. WPA3 uses the passphrase only for authentication; decryption is impossible.

Q. I'm on a WLAN with high traffic volume, and it's hard to examine individual packets when the application is receiving hundreds of thousands of packets per second, as the old packets are quickly removed from the circular buffer. Is there anything I can do about it?

A. Yes, you can use the **Open current buffer in new window** button on the small toolbar on the **Packets** tab. This will allow you to make snapshots of the current buffer as many times as you wish, at any intervals. You will then be able to explore the packets in these new windows at your leisure.

Q. I launched the program, selected the channel, started capturing, but no packets are displayed. Please help!

A. First, switch to the **Packets** tab. The **Latest IP Connections** tab might be empty if you did not enter correct WEP keys, and your WLAN uses WEP encryption. If the **Packets** tab is empty too, look at the program's status bar. If the packet counter is being incremented, then you have active rules that prevent the program from displaying packets. Click **Rules => Reset All**, and then press three toolbar buttons: **Capture Data Packets**, **Capture Management Packets**, and **Capture Control Packets.** If the packet counter on the status bar is not being incremented, then there are probably no active wireless stations or access points available/detected. If you are absolutely certain that there are wireless stations or access points, report this problem to us.

Q. Can CommView for WiFi read NCF log files generated by the standard, non-wireless CommView edition? How about vice versa?

A. Yes, CommView for WiFi can read NCF log files generated by the standard, non-wireless CommView edition. The standard, non-wireless CommView edition can read NCF log files generated by CommView for WiFi (and will soon be able to read the latest NCFX log format), but you will not be able to see wireless-specific columns, such as signal strength or channel number.

Q. Does CommView for WiFi run on multi-processor computers?

A. Yes, it does.

Q. It seems to be impossible to save more than 5,000 packets from the packet buffer. Is there a workaround?

A. Actually, there is no such limitation. The application uses a circular buffer for storing captured packets. By default, the buffer can contain up to 5,000 latest packets, but this value can be adjusted in the **Settings** window. The maximum buffer size is 20,000 packets (the buffer cannot be unlimited for an obvious reason: your computer’s RAM is not unlimited). You can save the contents of the buffer to a file using the **Logging** tab. However, by no means does this limit on the buffer size restrict your ability to save any number of packets. You simply need to enable automatic logging on the **Logging** tab. Such automatic logging will make the application dump all the captured packets to file(s) continuously, and you can set any limit on the total size of the captured data.

Q. My firewall software warns me that CommView for WiFi is "attempting to access the Internet." I am aware that some sites are able to track users by collecting the information sent by their programs via Internet. Why does CommView "attempt to access the Internet"?

A. Three activities may alert your firewall. First, it may be an attempt to resolve IP addresses to hostnames. Since CommView for WiFi has to contact your DNS servers to make a DNS query, it inevitably triggers the alarm. You can disable this feature (Settings => Options => Disable DNS resolving), but in this case, the Latest IP Connections tab will not be able to show you the hostnames. Second, you may have configured the program to check if updates or new versions are available. To do this, CommView for WiFi has to connect to www.tamos.com. You can disable this feature (Settings => Options => Misc. => Enable automatic application updates). Third, when you purchase the product, you need to activate it. If you select online activation, CommView for WiFi has to connect to www.tamos.com. You can avoid this by selecting manual activation. These are the only types of connections CommView for WiFi can potentially make. There are no other hidden activities. We do not sell spyware.

Q. I'm often logged on as a user without administrative privileges. Do I have to log off and then re-logon as the administrator to be able to run CommView for WiFi?

A. No, you can open CommView for WiFi folder, right-click on the CV.exe file while holding down the Shift key, and select "Run As" from the pop-up menu. Enter the administrative login and password in the window that pops up and click OK to run the program. Under Windows Vista and higher, CommView for WiFi is automatically launched with elevated rights.

Q. When reconstructing TCP sessions that contain HTML pages in Japanese or Chinese, I cannot see the original text.

A. To see text in East Asian languages, you should install East Asian fonts. Open Control Panel => Regional and Language Options, select the "Languages" tab, and check the "Install files for East Asian languages" box.

Q. I'm confused about the license types available for CommView for WiFi. Could you explain the difference between the license types?

A. Two license types are currently available for CommView for WiFi: Standard license and VoIP license. The more expensive VoIP license enables all the application features, including VoIP analyzer, whereas the standard license does not enable VoIP analyzer.

Additionally, the Standard License is also available as a One Year Subscription, which is a time-limited license valid for one year from the date of purchase only.

CommView for WiFi can also be purchased as a boxed product. Boxed versions include a compatible wireless adapter and a USB flash drive. The price includes UPS ground shipping.

Please refer to the End User License Agreement that comes with the product for other licensing terms and conditions.

Q. Can I save the audio from the VoIP analyzer to a standard .wav or .mp3 file?

A. Not directly, but there are many utilities on the market that offer a "virtual audio cable" that allows saving anything that is played back through your sound card to a file. Try, for example, Xilisoft Sound Recorder (use the "What you hear" mode).

VoIP Analysis

Introduction

NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

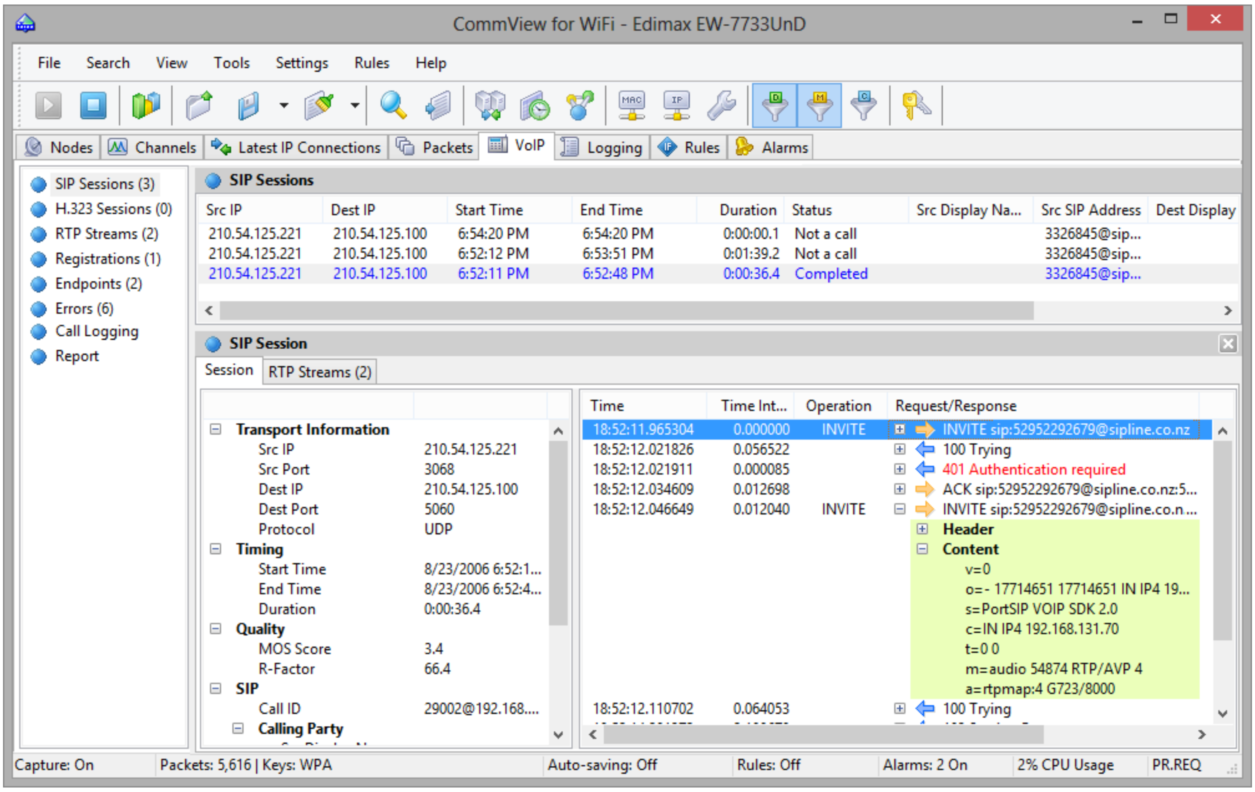
VoIP analyzer is a built-in CommView for WiFi module that is suited for real-time capturing and analyzing Internet telephony (VoIP) events, such as call flow, signaling sessions, registrations, media streams, errors, etc. By visualizing this data and assessing voice quality, this tool helps you boost productivity in debugging VoIP networks, software, and hardware. CommView's VoIP analyzer supports **SIP 2.0** and **H.323** signaling protocols and **RTP 2.0** media streams and many widespread codecs. In addition to real-time analysis, the analyzer can be used for post-capture import and analysis of capture logs in a number of formats (e.g. Tcpdump, EtherPeek, etc.)

If your WLAN uses WEP or WPA encryption, you must configure the WEP or WPA keys correctly to be able to decrypt network traffic; otherwise, VoIP analysis will not be available. Please see WEP/WPA Keys and Understanding WPA Decryption for more information.

Working with VoIP Analyzer

NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

VoIP analyzer can be accessed through the **VoIP** tab of the main application window, where real-time analysis of captured packets is performed, or through the VoIP Log Viewer window that should be used when you wish to perform post-capture analysis of log files. VoIP analyzer works concurrently with packet capture and displays results in real-time:



SIP Sessions

Src IP	Dest IP	Start Time	End Time	Duration	Status	Src Display Na...	Src SIP Address	Dest Display
210.54.125.221	210.54.125.100	6:54:20 PM	6:54:20 PM	0:00:00.1	Not a call		3326845@sip...	
210.54.125.221	210.54.125.100	6:52:12 PM	6:53:51 PM	0:01:39.2	Not a call		3326845@sip...	
210.54.125.221	210.54.125.100	6:52:11 PM	6:52:48 PM	0:00:36.4	Completed		3326845@sip...	

Transport Information	
Src IP	210.54.125.221
Src Port	3068
Dest IP	210.54.125.100
Dest Port	5060
Protocol	UDP
Timing	
Start Time	8/23/2006 6:52:1...
End Time	8/23/2006 6:52:4...
Duration	0:00:36.4
Quality	
MOS Score	3.4
R-Factor	66.4
SIP	
Call ID	29002@192.168....
Calling Party	

Time	Time Int...	Operation	Request/Response
18:52:11.965304	0.000000	INVITE	INVITE sip:52952292679@sipline.co.nz
18:52:12.021826	0.056522		100 Trying
18:52:12.021911	0.000085		401 Authentication required
18:52:12.034609	0.012698		ACK sip:52952292679@sipline.co.nz:5...
18:52:12.046649	0.012040	INVITE	INVITE sip:52952292679@sipline.co.n...
			Header
			Content
			v=0
			o=- 17714651 17714651 IN IP4 19...
			s=PortSIP VOIP SDK 2.0
			c=IN IP4 192.168.131.70
			t=0 0
			m=audio 54874 RTP/AVP 4
			a=rtpmap:4 G723/8000
18:52:12.110702	0.064053		100 Trying

Capture: On | Packets: 5,616 | Keys: WPA | Auto-saving: Off | Rules: Off | Alarms: 2 On | 2% CPU Usage | PR.REQ

The information in the VoIP analyzer window is organized by several categories. The category list is located on the pane and allows selection and viewing of detailed analysis data that is displayed in the right part of the window. The following categories are available:

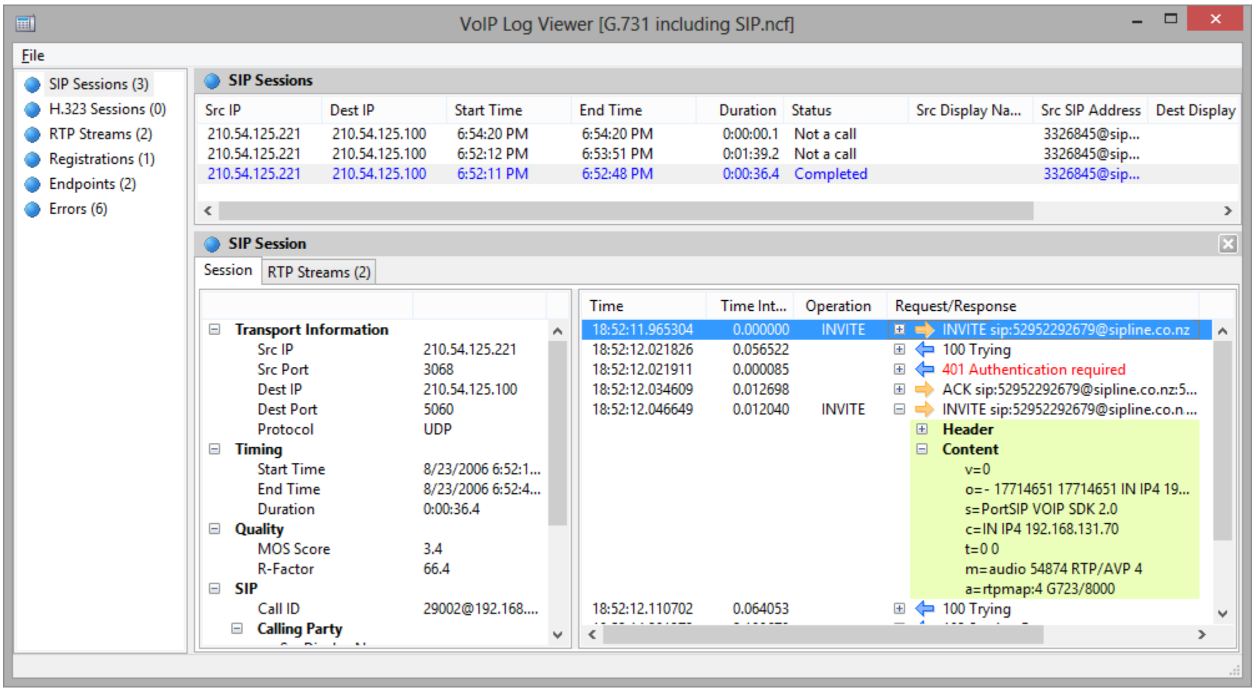
SIP Sessions – list of captured SIP 2.0 sessions.
H.323 Sessions – list of captured H.323 sessions.
RTP Streams – list of captured RTP streams.
Registrations – list of clients registered at the registration server and the clients' registration history.
Endpoints –list of workstations involved in VoIP data exchange.
Errors – list of errors registered during VoIP data exchange.
Call Logging – logging configuration for captured VoIP data.
Report – report generation configuration, including the automatic mode.

Please refer to Working with Lists in VoIP Analyzer for detailed information on how the data is arranged in VoIP analyzer.

SIP and H.323 Sessions

> NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

VoIP analyzer currently supports two types of VoIP signaling protocols, SIP and H.323. SIP and H.323 sessions are presented as two separate items on the left pane. Selecting one of the two items will display corresponding signaling sessions captured by the application and provide detailed information related to each session:



Src IP	Dest IP	Start Time	End Time	Duration	Status	Src Display Na...	Src SIP Address	Dest Display
210.54.125.221	210.54.125.100	6:54:20 PM	6:54:20 PM	0:00:00.1	Not a call		3326845@sip...	
210.54.125.221	210.54.125.100	6:52:12 PM	6:53:51 PM	0:01:39.2	Not a call		3326845@sip...	
210.54.125.221	210.54.125.100	6:52:11 PM	6:52:48 PM	0:00:36.4	Completed		3326845@sip...	

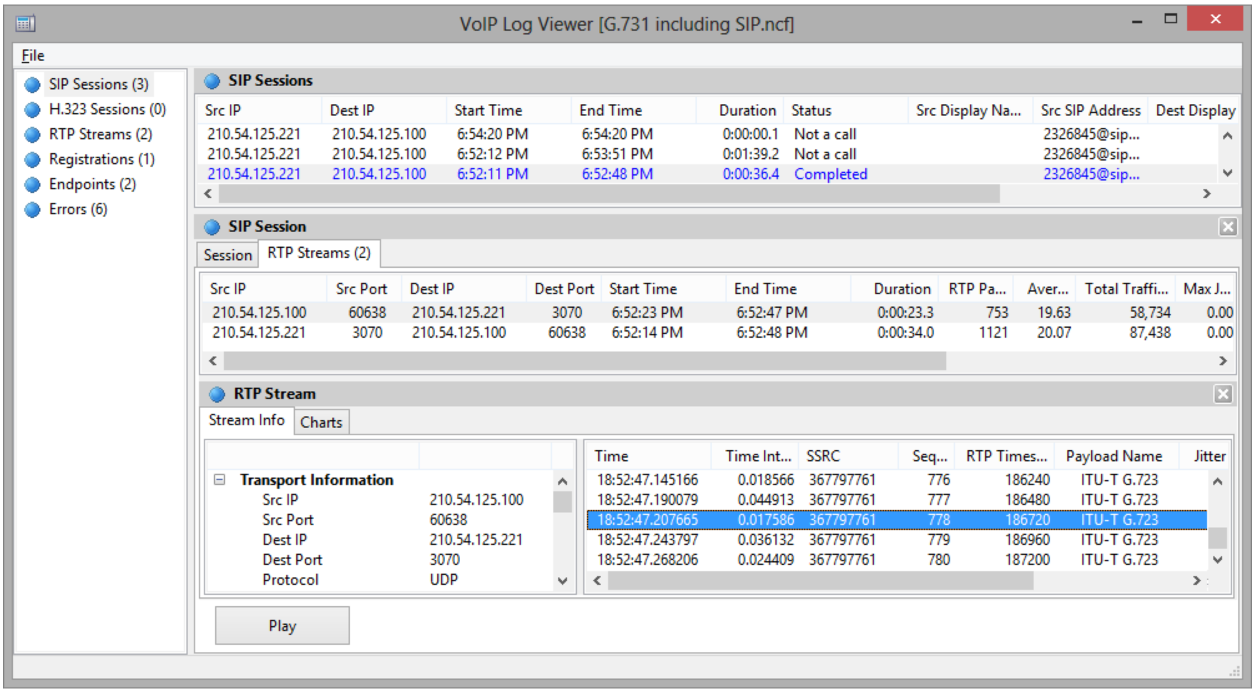
```
⊟ Transport Information
    Src IP          210.54.125.221
    Src Port        3068
    Dest IP         210.54.125.100
    Dest Port       5060
    Protocol        UDP
⊟ Timing
    Start Time      8/23/2006 6:52:1...
    End Time        8/23/2006 6:52:4...
    Duration        0:00:36.4
⊟ Quality
    MOS Score       3.4
    R-Factor        66.4
⊟ SIP
    Call ID         29002@192.168....
  ⊟ Calling Party
```

Time	Time Int...	Operation	Request/Response
18:52:11.965304	0.000000	INVITE	⊞ ⇨ INVITE sip:52952292679@sipline.co.nz
18:52:12.021826	0.056522		⊞ ⇦ 100 Trying
18:52:12.021911	0.000085		⊞ ⇦ 401 Authentication required
18:52:12.034609	0.012698		⊞ ⇨ ACK sip:52952292679@sipline.co.nz:5...

18:52:12.046649	0.012040	INVITE	⊟ ⇨ INVITE sip:52952292679@sipline.co.n ...
			⊞ Header
			⊟ Content
			v=0
			o=- 17714651 17714651 IN IP4 19...
			s=PortSIP VOIP SDK 2.0
			c=IN IP4 192.168.131.70
			t=0 0
			m=audio 54874 RTP/AVP 4
			a=rtpmap:4 G723/8000

18:52:12.110702	0.064053		⊞ ⇦ 100 Trying

The upper pane displays a complete list of captured SIP or H.323 sessions. When selecting a SIP/H.323 session from the list, the lower pane displays detailed information on the selected session, including a detailed session log, summarized and statistical data, as well as the RTP streams related to the selected session:



SIP Sessions

Src IP	Dest IP	Start Time	End Time	Duration	Status	Src Display Na...	Src SIP Address	Dest Display
210.54.125.221	210.54.125.100	6:54:20 PM	6:54:20 PM	0:00:00.1	Not a call		2326845@sip...	
210.54.125.221	210.54.125.100	6:52:12 PM	6:53:51 PM	0:01:39.2	Not a call		2326845@sip...	
210.54.125.221	210.54.125.100	6:52:11 PM	6:52:48 PM	0:00:36.4	Completed		2326845@sip...	

SIP Session – RTP Streams (2)

Src IP	Src Port	Dest IP	Dest Port	Start Time	End Time	Duration	RTP Pa...	Aver...	Total Traffi...	Max J...
210.54.125.100	60638	210.54.125.221	3070	6:52:23 PM	6:52:47 PM	0:00:23.3	753	19.63	58,734	0.00
210.54.125.221	3070	210.54.125.100	60638	6:52:14 PM	6:52:48 PM	0:00:34.0	1121	20.07	87,438	0.00

RTP Stream – Stream Info

Transport Information	
Src IP	210.54.125.100
Src Port	60638
Dest IP	210.54.125.221
Dest Port	3070
Protocol	UDP

Time	Time Int...	SSRC	Seq...	RTP Times...	Payload Name	Jitter
18:52:47.145166	0.018566	367797761	776	186240	ITU-T G.723	
18:52:47.190079	0.044913	367797761	777	186480	ITU-T G.723	
18:52:47.207665	0.017586	367797761	778	186720	ITU-T G.723	
18:52:47.243797	0.036132	367797761	779	186960	ITU-T G.723	
18:52:47.268206	0.024409	367797761	780	187200	ITU-T G.723	

If RTP streams are available for the selected signaling sessions, it is possible to play a call by clicking **Play**.

See also:

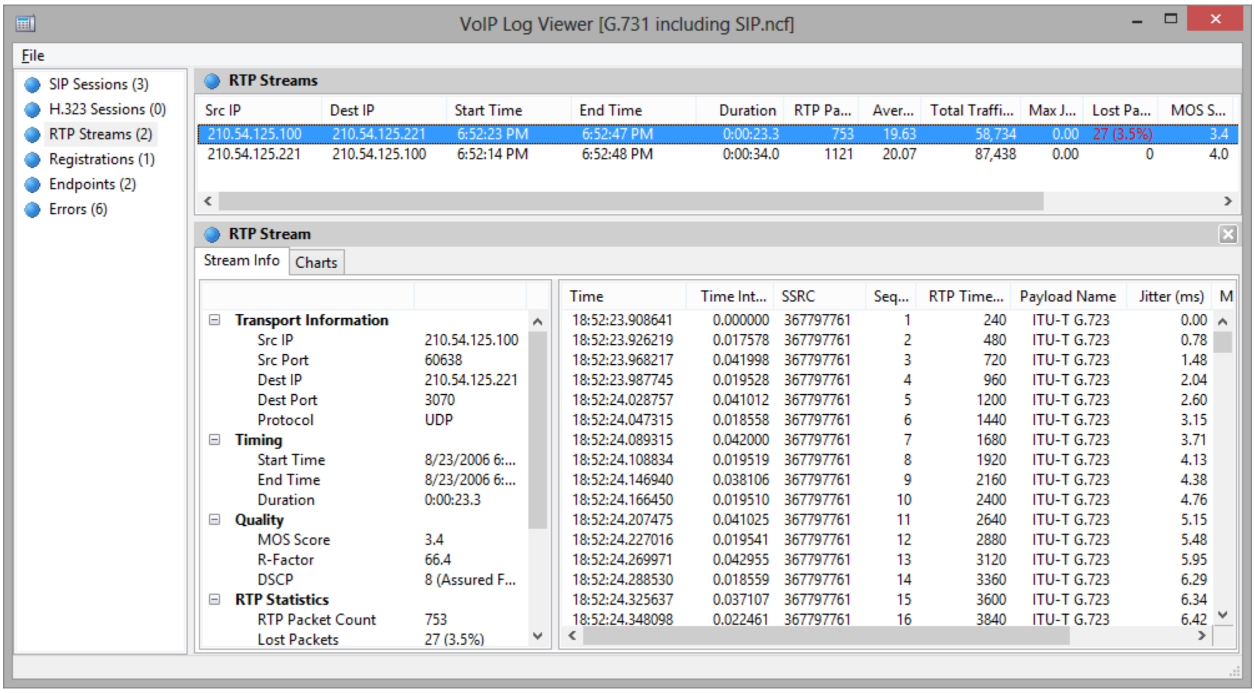
Working with Lists in VoIP Analyzer
Call Playback
NVF files

RTP Streams

NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

The Real-time Transport Protocol (or RTP) defines a standardized packet format for delivering audio and video over the Internet. While protocols like SIP or H.323 are used to control the call (e.g. setting up a connection, dialing, disconnecting, etc.), RTP is used for reliable transmission of data packets and maintaining Quality of Service. In other words, RTP streams carry the actual voice payload encoded utilizing one of a number of codecs, and analysis of RTP data provided invaluable information for assessing call quality and troubleshooting VoIP networks.

To view RTP streams captured by the application, select **RTP Streams** in the left pane of the VoIP analyzer window:

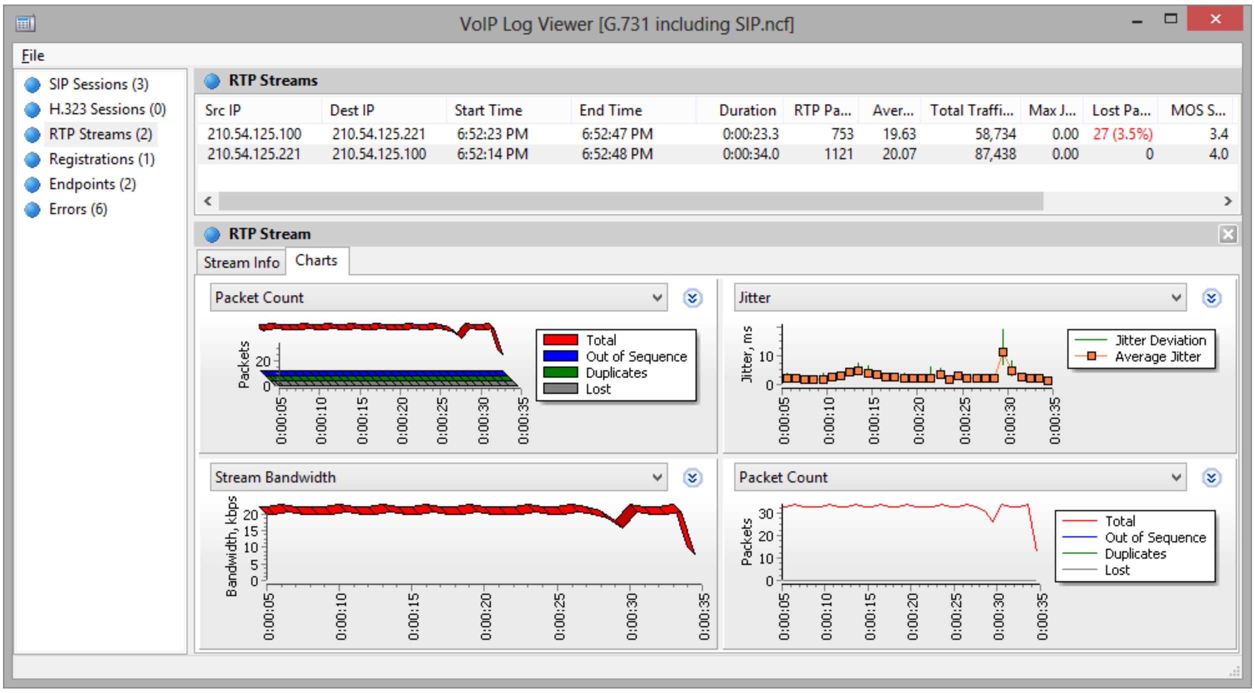


Src IP	Dest IP	Start Time	End Time	Duration	RTP Pa...	Aver...	Total Traffi...	Max J...	Lost Pa...	MOS S...
210.54.125.100	210.54.125.221	6:52:23 PM	6:52:47 PM	0:00:23.3	753	19.63	58,734	0.00	27 (3.5%)	3.4
210.54.125.221	210.54.125.100	6:52:14 PM	6:52:48 PM	0:00:34.0	1121	20.07	87,438	0.00	0	4.0

Transport Information	
Src IP	210.54.125.100
Src Port	60638
Dest IP	210.54.125.221
Dest Port	3070
Protocol	UDP
Timing	
Start Time	8/23/2006 6:...
End Time	8/23/2006 6:...
Duration	0:00:23.3
Quality	
MOS Score	3.4
R-Factor	66.4
DSCP	8 (Assured F...
RTP Statistics	
RTP Packet Count	753
Lost Packets	27 (3.5%)

Time	Time Int...	SSRC	Seq...	RTP Time...	Payload Name	Jitter (ms)	M
18:52:23.908641	0.000000	367797761	1	240	ITU-T G.723	0.00	
18:52:23.926219	0.017578	367797761	2	480	ITU-T G.723	0.78	
18:52:23.968217	0.041998	367797761	3	720	ITU-T G.723	1.48	
18:52:23.987745	0.019528	367797761	4	960	ITU-T G.723	2.04	
18:52:24.028757	0.041012	367797761	5	1200	ITU-T G.723	2.60	
18:52:24.047315	0.018558	367797761	6	1440	ITU-T G.723	3.15	
18:52:24.089315	0.042000	367797761	7	1680	ITU-T G.723	3.71	
18:52:24.108834	0.019519	367797761	8	1920	ITU-T G.723	4.13	
18:52:24.146940	0.038106	367797761	9	2160	ITU-T G.723	4.38	
18:52:24.166450	0.019510	367797761	10	2400	ITU-T G.723	4.76	
18:52:24.207475	0.041025	367797761	11	2640	ITU-T G.723	5.15	
18:52:24.227016	0.019541	367797761	12	2880	ITU-T G.723	5.48	
18:52:24.269971	0.042955	367797761	13	3120	ITU-T G.723	5.95	
18:52:24.288530	0.018559	367797761	14	3360	ITU-T G.723	6.29	
18:52:24.325637	0.037107	367797761	15	3600	ITU-T G.723	6.34	
18:52:24.348098	0.022461	367797761	16	3840	ITU-T G.723	6.42	

The upper part displays a complete list of all RTP streams. When selecting a RTP stream from the list, the lower pane displays detailed information on the selected stream, including the complete list of RTP packets, summarized and statistical data, as well as the charts:



Src IP	Dest IP	Start Time	End Time	Duration	RTP Pa...	Aver...	Total Traffi...	Max J...	Lost Pa...	MOS S...
210.54.125.100	210.54.125.221	6:52:23 PM	6:52:47 PM	0:00:23.3	753	19.63	58,734	0.00	27 (3.5%)	3.4
210.54.125.221	210.54.125.100	6:52:14 PM	6:52:48 PM	0:00:34.0	1121	20.07	87,438	0.00	0	4.0

Up to four different charts for the selected stream can be displayed simultaneously, with the window interval from 5 to 60 seconds. Note that right clicking and dragging the graph will scroll it to the left or right respectively. The following chart types are available:

Packet Count – number of RTP packets per second including duplicates, lost packets, and "out of order" packets.
Stream Bandwidth – stream speed in terms of kilobits per second.
Packet Sizes – average sizes of RTP packets broken down by network and RTP headers, and RTP payload.
Jitter – stream jitter.
R-Factor, MOS Score – stream quality estimation.
Packet Intervals – temporal allocation of RTP packets in a stream.

The RTP Streams list contains all captured RTP streams, both belonging to SIP or H.232 signaling sessions, and the ones for which signaling sessions were not identified (so called 'orphan' streams, i.e. the ones that do not belong to any parent session). Please refer to the Settings chapter for more detailed information on how to exclude RTP streams that do not have corresponding signaling sessions.

See also:

Working with Lists in VoIP Analyzer
Call Playback
NVF Files

Registrations, Endpoints, and Errors

> NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

To view the VoIP clients registered with the registration servers, select the **Registrations** item in the left pane of the VoIP analyzer window. The upper part of the right pane displays a complete list of all registrations, including current registration status of VoIP clients. When you select a registration record, the registration message log containing the messages of the VoIP client sent to/received from the registration server is displayed.

To view the list of workstations involved in the VoIP data exchange, including statistical data and top callers list, select the **Endpoints** item in the left pane of the VoIP analyzer window. The complete list of workstations is displayed in the upper part of the pane. When you select an end point, the lower part of the pane displays the calls initiated or received by the selected computer.

To view the list of recent errors registered during the data exchange between VoIP clients and servers, select the **Errors** item in the left pane of the VoIP analyzer window. The list of recent errors is displayed in the upper part of the pane. When you select a record, related call information is displayed in the lower part of the pane.

Call Logging and Reports

> NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

The **Call Logging** pane allows you to save all VoIP-related packets to CommView for WiFi capture files automatically. Enable the **Auto-saving** option and select the output data you want to be recorded in a log file. The **Data to include** frame lets you configure the specific packets that you want the application to log.

The **Report** pane is intended for automatic VoIP report generation. Checking the **Generate reports** box enables report generation. The **Data to include** frame lets you configure the specific information that you want to be included in the reports. You can also configure the report format (CSV or HTML) as well as the time intervals at which reports are generated. New reports can either replace old ones or be appended.

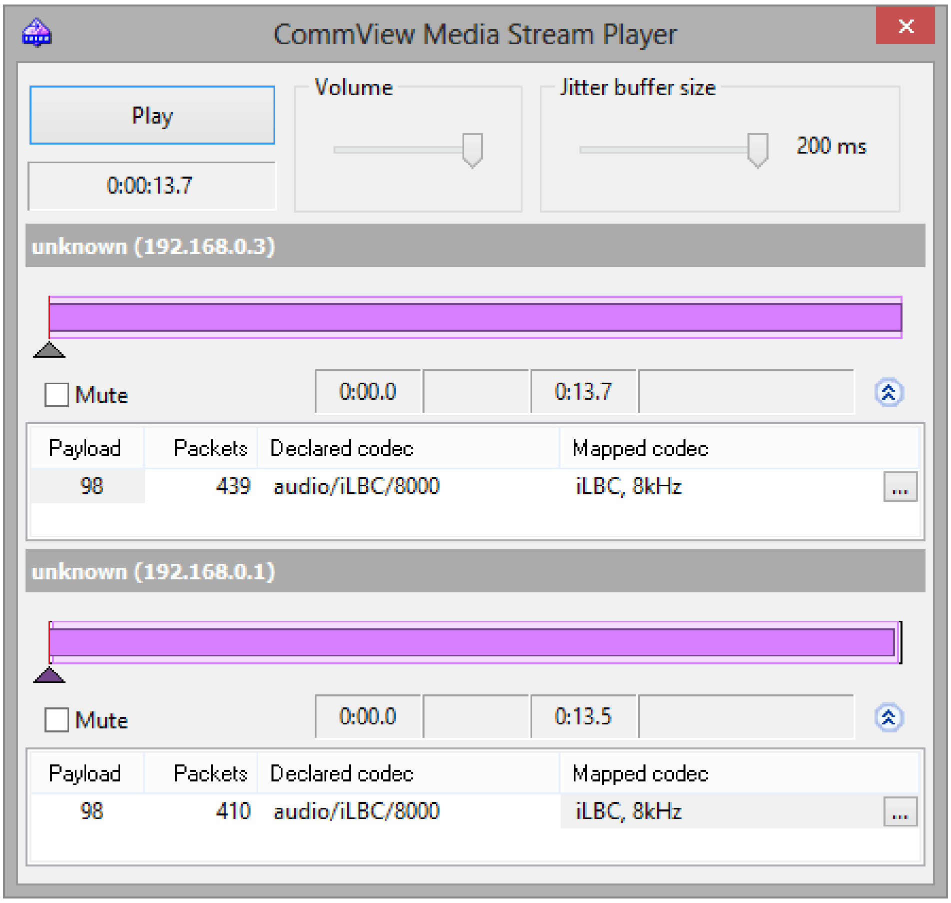
Call Playback

> NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

The call playback functionality can be used for assessing the audio quality experienced by the parties participating in a VoIP call. In most of the cases, VoIP analyzer allows you to play captured calls (this depends on the support of the specific codec(s) being used in the given VoIP call). To play a call, select the desired call record in the VoIP analyzer window, select the **RTP Streams** tab, and click on the **Play** button. Alternatively, you can select any item on the right pane containing the list of RTP streams (for example, the RTP Streams category), select one or several streams, right-click on them, and select the **Play Selected** menu item. That way, it is possible to interrelate and play back the streams for which the signaling session is either absent, or the signaling protocol is not supported (i.e. the protocol is not SIP or H.323).

> NOTE: Simultaneous playback of RTP streams that belong to **different calls** initiated at different times usually will not work. The main problem is the significant time discrepancy between the streams that belong to different VoIP calls, aside from the fact that it makes no sense to listen to unrelated audio that is part of unrelated calls. The functionality that allows selecting arbitrary RTP streams for subsequent playback is provided solely for manual recovery of a call from several streams in cases where parent SIP or H.323 sessions are not available.

After clicking on the **Play** button, the Media Stream Player window will be opened:



Jitter buffer size: 200 ms

0:00:13.7

unknown (192.168.0.3)

□ Mute 0:00.0 0:13.7

Payload	Packets	Declared codec	Mapped codec
98	439	audio/iLBC/8000	iLBC, 8kHz ...

unknown (192.168.0.1)

□ Mute 0:00.0 0:13.5

Payload	Packets	Declared codec	Mapped codec
98	410	audio/iLBC/8000	iLBC, 8kHz ...

Click on the double-arrow button to have the application display more detailed information about the audio stream(s) and access to manual codec mapping. For each of the RTP streams you can:

- Manually synchronize a stream by time, i.e. set the starting time of playback in relationship to other streams. To do that, move the small triangle to the left or to the right.
- Select the correct sound codec for each of the payload types in the RTP stream. In most cases, Media Stream Player will automatically select the correct codec. However, when working with "orphan" RTP streams that lack parent SIP or H.323 sessions, and, therefore, information on the codecs being used, you will have to manually select the correct codec from the drop-down list. If you find it difficult to pick the correct codec, try clicking on the **Try to Guess** button and Media Stream Player will try to select the codec by itself.

Note that it is sometimes impossible to play back audio from RTP streams, as these streams may be encrypted or use proprietary codecs or codecs not supported by CommView for WiFi.

The **Volume** control allows you to adjust the sound volume. The **Jitter buffer size** control allows you to simulate the jitter buffer used in real world VoIP end nodes. A typical jitter buffer is 30 ms to 50 ms in size. Increasing the buffer size improves the voice quality but increases the delay.

Viewing VoIP Logs

> NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

VoIP Log Viewer is a tool for viewing and analyzing capture files created by CommView for WiFi and some other third party network analyzers. It has very similar functionality to the VoIP analyzer that is part of the main application window; however, its purpose is post-capture analysis, i.e. working with files rather than packets captured in real time. Please refer to the Working with VoIP Analyzer chapter for detailed information on how to work with this tool.

Click **File => VoIP Log Viewer** to launch VoIP Log Viewer. You can open as many VoIP Log Viewer windows as you wish, and each window can be used for analysis of one or several capture files.

VoIP Log Viewer can be used for loading CommView for WiFi capture files in NCFX format and other ones created by third party network analyzers. Additionally, it is possible to load CommView VoIP Files (NVF) into VoIP Log Viewer.

VoIP Log Viewer Menu

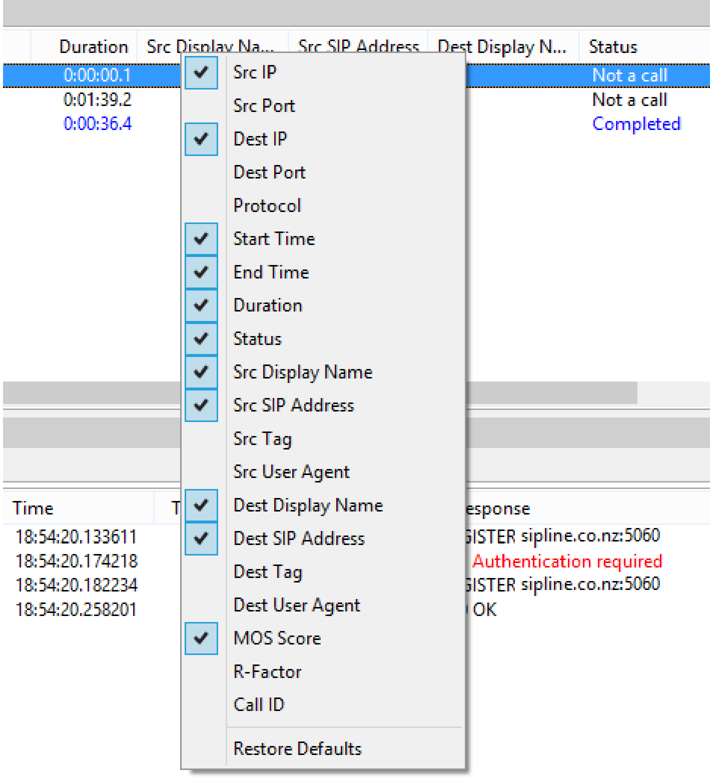
Load CommView Logs – opens and loads one or several CommView for WiFi capture files.
Import Logs – allows you to import capture files created by other packet analyzers.
Generate Report – generates a summary report for the data loaded in VoIP Log Viewer and saves it to disk. When generating a report, settings of the Reports panel located in the main window of VoIP analyzer are used.
Clear VoIP Data – clears data in the current window.
Close Window – closes the window.

Working with Lists in VoIP Analyzer

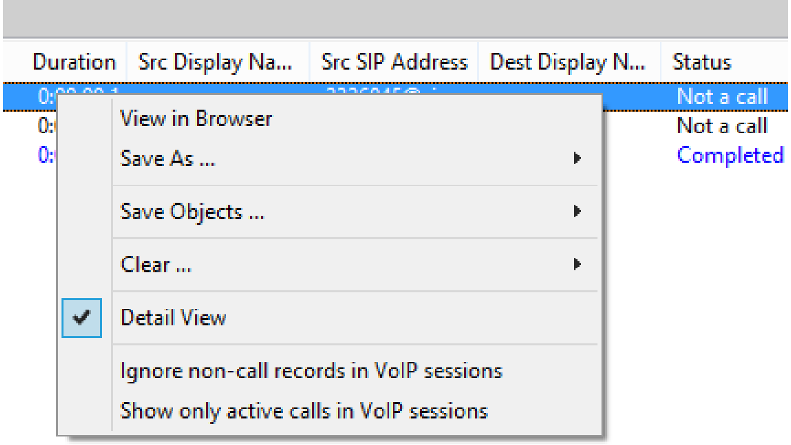
> NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

While the lists that display information in VoIP analyzer contain data of different natures, the style and data presentation principles explained below are shared between these lists.

By default, the lists include only the most frequently used data fields, while all other fields are hidden. To select the fields you would like to be displayed, right-click on the list header and check/uncheck the corresponding options. It is also possible to change their width and the order of displayed data fields by dragging them with your mouse.



Right clicking on the list opens the context menu containing the following items:



View in Browser – opens the current view as an HTML file in a web browser.

Save As… – export all or selected records to a text file.

Save Objects… – saves all or selected objects to a NVF file. Please see the NVF Files chapter for more information on the NVF format.

Clear… – clears all or selected objects or lists. Deleting parent objects leads to the deletion of the child objects; for example, when deleting a SIP call, the respective RTP streams that belong to this call will also be deleted from the **RTP Streams** list.

Detail View - if you are working with a master list, i.e. there are more details related to the selected object, enabling/disabling this option will make the program show/hide the respective details of object. For example, selecting **Detail View** on the **SIP Sessions** list makes the program show or hide detailed information for the selected SIP session, such as summary call information and related RTP streams.

Ignore non-call records in VoIP sessions – hides all records that do not represent actual calls.

Show only active calls in VoIP sessions – hides all records that are no longer active.

NVF Files

NOTE: The VoIP analysis module is only available to VoIP license users or evaluation version users who selected VoIP evaluation mode.

VoIP analyzer allows you to save one or several VoIP data objects to a container file in NVF format. Unlike common capture files, NVF does not contain captured data packets. Rather, this is a set of VoIP object(s) stored in a single file. NVF files are instrumental when you want to save a VoIP call with all the related streams for future analysis.

VoIP objects that can be saved to NVF files are:

- **SIP Sessions**
- **H.323 Sessions**
- **RTP Streams**

To save an object to a NVF file, select one or several objects in the VoIP analyzer lists, right-click to open the context menu, and select the **Save Objects As…** menu item.

SIP or H.323 sessions and respective RTP streams (if any) will be saved to a file. However, if you choose to save the RTP stream, the respective parent SIP or H.323 sessions will not be saved.

You can load the saved NVF file into VoIP Log Viewer window.

Advanced Topics

Monitoring 802.11n, 802.11ac, and 802.11ax Networks

Despite the similarities between the 802.11 a/b/g and 802.11n/ac/ax technologies, there are some peculiarities in 802.11n/ac/ax networks that influence the way such networks should be efficiently monitored. Without going into the specific technical details of the standard, as they are publicly available from many sources on the Internet, this chapter overviews the best monitoring practices and hardware requirements for 802.11n, 802.11ac, and 802.11ax networks.

Adapter Compatibility

Capturing packets of a particular standard requires the use of the adapter that is based on the same or newer standard. For example, capturing 802.11ac packets requires an 802.11ac or 802.11ax adapter; You cannot capture 802.11ac packets using an 802.11n adapter. The list of compatible adapters can be found on the CommView for WiFi download page on our web site. Depending on the configuration of the 802.11n/ac/ax WLAN being monitored, additional requirements to the adapter might apply. They are discussed in detail below.

MIMO, Spatial Streams, and Transmit Beamforming

The use of the MIMO and Transmit Beamforming technology in 802.11n, 802.11ac, and 802.11ax networks is a serious challenge for wireless analyzers. Such networks create a very complex, adaptive signal intensity map with dips and bumps, some as small as a few centimeters in volume. Because a monitoring device is passive, the WLAN being monitored does not attempt to adapt to it. Signals travelling at high rates and transmitted by multiple antennas are also hard to intercept without CRC errors. All of the above means that, generally, you should expect a considerably higher percentage of broken frames when monitoring 802.11n, 802.11ac, and 802.11ax networks versus the older 802.11 a/b/g ones. While this is not a problem when you are performing a site survey or measuring signal strength of particular devices, examining individual TCP streams or troubleshooting problems on the per-packet level may become problematic when too many frames are damaged.

To mitigate these 802.11n/ac/ax-specific factors, consider applying the following techniques:

- Find the best position for the notebook running CommView for WiFi. Rotating it or moving it just a few inches in a different direction may dramatically increase or decrease the signal quality. In fact, even the position of your body or a raised arm may affect the percentage of CRC errors.
- Try to make sure that that the WLAN devices do not operate at their maximum rates. Successful capturing of packets with rates of 100 Mbps and below is far more likely than successful capturing of packets with higher data rates. Although this sounds counter-intuitive, if your monitoring notebook is located next to the AP, moving the client devices a few meters further from the AP will increase rather than decrease the reception quality. An 802.11ax client device located one or two meters from the AP will almost inevitably transmit packets at the rate of 720 or 866 Mbps, whereas the same device located five meters from the AP will drop the rate down to about 200 Mbps, which is beneficial for our purposes.

It is important to remember that the capabilities of your monitoring adapter in terms of the number of supported spatial streams must exceed or be equal to the capabilities of the WLAN being monitored. In other words, you cannot capture packets being sent from a three-stream AP to a three-stream client using an adapter that supports only one or two spatial streams (but you can capture packets being sent, for example, from a two-stream AP to a two-stream client using a three-stream adapter). It is easy to figure out the number of supported spatial streams by looking at the adapter specifications. For example, for 802.11ac, the maximum supported rate of 433 Mbps means a one-stream adapter, 876 Mbps means a two-stream adapter, and 1,300 Mbps means a three-stream adapter.

Channel Bonding in the 2.4 GHz Band

In modern WLANs, the data rate is optionally increased by bonding two 20 MHz channels (40 MHz operation). The 40 MHz operation uses wider bands, compared to 20 MHz bands in 802.11 a/b/g, to support higher data rates. While a Wi-Fi network analyzer equipped with an 802.11n/ac/ax card does not have a problem with capturing two channels simultaneously, it is important to pay attention to the regulatory domains of the hardware being used. In brief, the frequency of the secondary channel in 40 MHz mode depends on the frequency of the primary channel. For example, selecting channel #1 in your hardware means that the primary 20 MHz channel will operate at the frequency of channel #1, while the secondary 20 MHz channel will operate four channels above the primary one, i.e. at the frequency of channel #5. When operating at higher channel numbers, e.g. 10 or 11, adding four to the channel number would mean that the frequency of the secondary channel would go outside of the regulatory domain constraints: in the US, the top channel in the 2.4 GHz band is 11; in most European countries, the top channel is 13. In such cases, the secondary channel uses the frequency that is below the frequency of the primary channel. For example, selecting channel #10 in your hardware means that the primary 20 MHz channel will operate at the frequency of channel #10, while the secondary 20 MHz channel will operate four channels below the primary one, i.e. at the frequency of channel #6.

The potential problem that a field engineer may encounter when working internationally is that the regulatory domain of his monitoring network adapter may be different from the regulatory domain of the Wi-Fi network being monitored. For example, a Germany-based 802.11n WLAN working on channel #9 would bond channels #9 and #13. A monitoring adapter bought in Canada would expect the secondary channel to be #5. This will prevent the adapter from "seeing" the 40 MHz data streams in the wireless analyzer. To handle this situation, consider using hardware that belongs to the same regulatory domain or use the **Sec. channel below in 40 MHz mode** box on the **Capture** pane of the main window. Checking this box will force the adapter to use the secondary channel frequency that is below the primary channel frequency even if the regulatory domain of the network adapter does not require that.

Note that some of the adapters supported by CommView for WiFi, such as Broadcom-based adapters, do not support channel bonding and can capture packets on 20 MHz channels only. Please refer to the Technical Notes for the detailed information. We suggest that you choose one of the adapters marked as "**Recommended**" on the download page; such adapters support channel bonding.

Channel Bonding in the 5 GHz Band

In the 5 GHz band, channel bonding is similar to channel bonding in the 2.4 GHz band, but the number of bonded channels may reach eight in 802.11ac/ax WLANs, which means that channel width may reach 160 MHz. Unlike the 2.4 GHz band, the sets of available bonded channels for the 5 GHz band is strictly defined in the standard. For example, for 40 MHz wide channels, channel 52 is always bonded with channel 56; it cannot be bonded with channel 48. For this reason, the **Sec. channel below in 40 MHz mode** box has no effect when you are capturing channels in the 5 GHz band with a recommended adapter; it automatically selects the correct set of channels. For example, if you select channel 36, the adapter will capture on an 80 MHz wide channel (from 36 to 48). However, in this example, the packets sent using a 20 MHz wide channel would be visible only if they are sent on channel 36. In other words, if you are monitoring an 802.11ac/ax access point that is configured to use channels 36-48 and the AP's primary channel is 36, you will see both the AP's beacons and 80 MHz data packets if you are capturing on channel 36, but you will see only 80 MHz data packets (and no beacons) if you are capturing on channel 40, 44, or 48.

BCC and LDPC Coding

On the hardware level, 802.11n/ac/ax packets are encoded using either Binary Convolutional Code (BCC) coding or Low Density Parity Check (LDPC) coding. BCC is the default coding method used by the majority of 802.11n devices. LDPC is an optional coding method supported by most newer devices. When a client associates to an AP, the HT Capabilities Info element in the association request and association response packets determine the use of one of the two coding methods. For example, if the default BCC mode is being used, the HT Capabilities Info contains the "HT LDPC coding capability: Transmitter does not support receiving LDPC coded packets" field. If the WLAN being monitored uses LDPC coding, your monitoring adapter must support LDPC coding too; otherwise, packets sent at HT rates in one or both directions will be missing or damaged. Capturing LDPC-encoded packets is supported by all the recommended 802.11ac and 802.11ax adapters.

Understanding CRC and ICV Errors

CRC Errors

Each wireless frame consists of the following basic components:

- A MAC header that includes frame control, duration, address, and sequence control information.
- A variable length frame body that contains information specific to the frame type.
- A frame check sequence (FCS) that contains a 4-byte cyclic redundancy code (CRC).

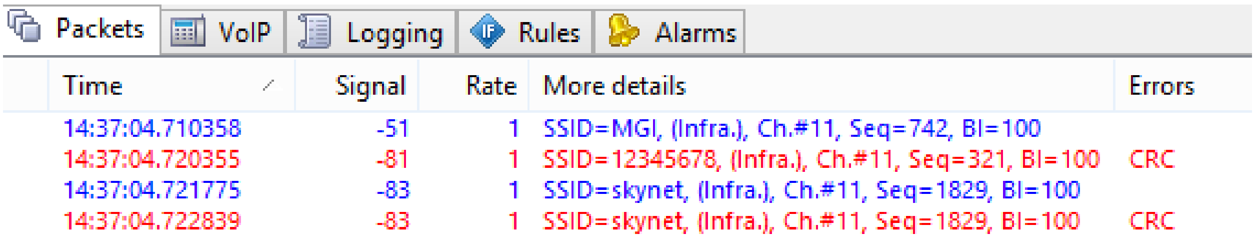
The last component, FCS, is used to check the integrity of the packet on the receiving end. The receiving end computes the CRC value over the received frame and compares the computed value with the actual four bytes at the end of the packet. If the values mismatch, the packet is considered damaged.

The way CommView for WiFi handles such corrupted frames depends on the user-defined settings. By default, such frames are ignored by the application, with the following exceptions:

- They increment the overall packet and byte counters.
- They increment the CRC Error counter on the **Channels** tab.
- They are included in the Packet Size chart in the **Statistics** window.

Damaged frames are not counted in other charts and tables for the obvious reason: No part of a frame with the wrong CRC value is credible. It may have a completely wrong IP address, data payload, etc., although in real life such frames bear a resemblance to the original. For the same reason CRC Errors cannot be attributed to a particular wireless AP or station, as it's impossible to determine the real sender's MAC address.

Nevertheless, the user may want to check the **Capture damaged frames** box in the options, in which case damaged frames will also be shown in the packet list. By default, such frames are marked with red and have the "CRC" identifier shown in the **Errors** column of the **Packets** tab:



Time	Signal	Rate	More details	Errors
14:37:04.710358	-51	1	SSID=MGI, (Infra.), Ch.#11, Seq=742, BI=100	
14:37:04.720355	-81	1	SSID=12345678, (Infra.), Ch.#11, Seq=321, BI=100	CRC
14:37:04.721775	-83	1	SSID=skynet, (Infra.), Ch.#11, Seq=1829, BI=100	
14:37:04.722839	-83	1	SSID=skynet, (Infra.), Ch.#11, Seq=1829, BI=100	CRC

It is important to understand that a frame received with a CRC error by CommView for WiFi may have been received by the destination node without an error. Despite the fact that damaged frames are supposed to be discarded by the destination node without further processing, CommView for WiFi will attempt to decode and even decrypt such frames.

Not all the wireless adapters are capable of passing damaged frames to the application level. Such functionality is guaranteed only for the recommended adapters supported by CommView for WiFi.

ICV Errors

Integrity Check Value (ICV) is a 4-byte checksum used in WEP- and WPA-encrypted frames for verifying the result of decryption. The receiving end computes the ICV value over the data portion of the received frame and compares the computed value with the actual four bytes at the end of the packet's data portion. If the values mismatch, the decryption is considered unsuccessful.

CommView for WiFi is capable of on-the-fly WEP and WPA decryption, provided the correct WEP/WPA key(s) have been entered by the user. The program shows ICV-related information in three different places: On the **Nodes** and **Channels** tabs and in the **Errors** column of the **Packets** tab. The way ICV errors are shown and counted by the program depends on whether the key has been entered as well as on its correctness. There different cases are possible:

1. A key has been entered by the user, and it is correct for the given WLAN.
2. A key has been entered by the user, but it is incorrect for the given WLAN.
3. No key has been entered.

In the first case, you should see very few ICV errors reported by the program. In the second case, all of the captured data frames will be marked with the ICV Error flag because the computed and the actual ICV values will not match if the wrong key is used for decryption. In the third case, no frames will have ICV errors because no decryption attempts will be made.

As explained above, unlike "hard" CRC errors, ICV errors are "soft" errors that depend on the decryption key. Your WLAN may be perfectly healthy, but if you entered the wrong WEP key in CommView for WiFi, you will observer many ICV errors. Because of its "softness," packets with ICV errors are, by default, shown in the same color as any other packets. This can be changed using the program's Options dialog.

If a frame has a CRC error, detecting an ICV error makes no point. Therefore, CommView for WiFi never sets the ICV error flag for frames with CRC errors.

Understanding WPA Decryption

As it has been mentioned throughout this product's documentation, CommView for WiFi is capable of decrypting WEP- and WPA/WPA2-encrypted network traffic on the fly. To take full advantage of this functionality, you should have a good understanding of the underlying cryptographic principles.

WEP (**Wired Equivalent Privacy**) is a mechanism used to provide data security in wireless networks. WEP allows the administrator to define a set of keys (or just one key) for the WLAN. These keys are shared among the clients and access points and are used for encrypting data before it is transmitted. If a client does not have the correct WEP key, it cannot decrypt the received packets or send data to other clients, which prevents unauthorized network access and eavesdropping. WEP decryption is rather straightforward as long as you have the correct key. WEP is a static and stateless encryption system, which means that once you have entered the correct key in the WEP/WPA Keys dialog, CommView for WiFi will be immediately able to decrypt packets.

WPA (Wi-Fi Protected Access) came as a replacement for the less secure WEP standard. WPA addresses many of WEP's security and privacy concerns, significantly increasing the level of data protection and access control for WLANs. Unlike WEP, WPA is a dynamic encryption system that uses rekeying, unique per-station keys, and a number of other measures to improve security. WPA features two modes, PSK (Pre-Shared Key) and Enterprise, which differ in a number of ways. CommView for WiFi supports decryption of WPA in PSK mode.

Given the dynamic nature of WPA encryption, knowing the WPA passphrase alone does not allow you to decrypt traffic immediately after entering the correct passphrase. To be able to decrypt WPA-encrypted traffic, CommView for WiFi must be running and capturing packets during the key exchange phase (key exchange is carried out using the EAPOL protocol). It is important that all of the EAPOL key exchange packets be successfully captured. A damaged or missing EAPOL packet will make it impossible for CommView for WiFi to decrypt packets that will be sent to/from the given station, and capturing the next EAPOL conversation between the AP and station may be required. This is an important distinction in the way WEP and WPA traffic is decrypted.

The principles explained above mean that once you have entered the WPA passphrase, closed the WEP/WPA Keys dialog, and started capturing packets, you will need to wait for the next authentication and key exchange event before the packets can be decrypted for the station that has been authenticated. Naturally, it is not uncommon that the program can decrypt packets to/from one client, but not to/from another, as it may have not yet captured EAPOL packets for all of the clients.

Re-authentication can be triggered by using the Node Reassociation tool, by restarting the AP (for all authenticated stations), or by reconnecting to the network (for the given client).

IMPORTANT: Please note that **packet traffic encrypted with WPA3 cannot be decrypted**. WPA3 uses the passphrase only for authentication; decryption is impossible.

Understanding Signal Strength

Wireless signal strength is traditionally measured in either percentile or dBm (the power ratio in decibels of the measured power referenced to one milliwatt.) By default, CommView for WiFi displays the signal strength in dBm. The level of 100% is equivalent to the signal level of -35 dBm and higher, e.g. both -25 dBm and -15 dBm will be shown as 100%, because this level of signal is very high. The level of 1% is equivalent to the signal level of -95 dBm. Between -95 dBm and -35 dBm, the percentage scale is linear, i.e. 50% is equivalent to -65 dBm.

If measurements in percentile are preferable, you can switch to percentile by using the **Display signal level in dBm** option in Settings => Options => Decoding. When **Display signal level in dBm** is turned on, the signal strength will be shown in dBm on the **Nodes**, **Channels**, and **Packets** tabs. In the packet decoder tree, the level is always shown in both percentile and dBm.

Capturing A-MPDU and A-MSDU Packets

The 802.11n, 802.11ac, and 802.11ax standards allow sending multiple frames per single access to the medium by combining the frames together into one larger frame. There are two forms of frame aggregation: Aggregated Mac Protocol Data Unit (A-MPDU) and Aggregated Mac Service Data Unit (A-MSDU). CommView for WiFi can capture both types of aggregated packets, as explained below.

Received A-MPDU frames are split into individual packets at the hardware level. A-MPDUs can be up to 64 Kbytes in size. When an A-MPDU is captured, it is passed to the application level as a number of disaggregated packets that look like any other packets. These packets are not marked by CommView for WiFi in any special manner. Support for A-MPDUs is mandatory in modern Wi-Fi standards and it is widely used. A-MPDUs can be captured by any adapter that is supported by CommView for WiFi.

Received A-MSDU frames are split into individual packets at the software level. A-MSDUs can be up to 7,935 bytes in size. When an A-MSDU is captured, it is passed to the application level as a single, aggregated packet—i.e., in the form in which it was originally received. If the aggregated packet is not damaged and if it can be decrypted (if decryption is necessary), CommView for WiFi will disaggregate the A-MSDU and will display the individual packets on the packet list. Such packets will be marked as "Subframe #... of A-MSDU #..." in the "More details" column. Additionally, the subframes will be followed by the original aggregated A-MSDU, which will be marked as "A-MSDU #...." If the aggregated packet is damaged or encrypted, only the original A-MSDU will be displayed. A-MSDUs can be captured by any recommended 802.11ac and 802.11ax adapters.

Note that large frames, such as A-MSDUs, are frequently damaged, especially when being sent at high data rates.

Using CommView for WiFi in a Virtual Machine

You can install and use CommView for WiFi inside a virtualized Windows OS running as a guest operating system on a Mac (or PC, if you prefer a virtual environment for whatever reason). In order to do that, you will need virtualization software, such as **VMWare**, **Parallels Desktop for Mac**, or **Virtual Box**.

Guest Operating System

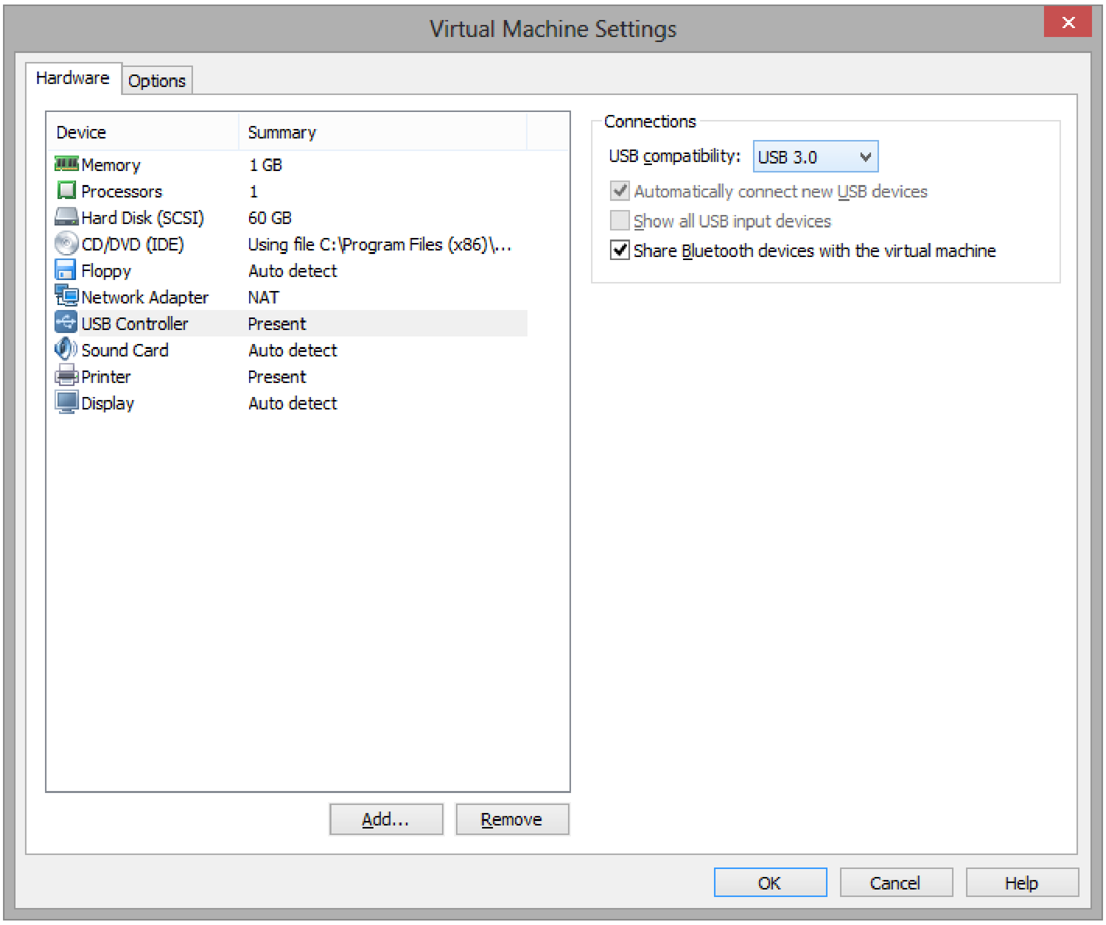
As a guest Windows version, you can use Windows 10, 8,1, 8, or 7, although we recommend Windows 10, 8.1, or 8 for the reasons explained below.

Hardware

To use CommView for WiFi for passive surveys, you need a compatible adapter. When you run our software on a Windows notebook, you can use any of the compatible adapters in different form factors. The list of compatible adapters can be found here. When you run CommView for WiFi inside a virtual Windows machine, you can use **USB adapters only**. Please refer to the adapter list to find the USB adapter you are going to use. We strongly recommend that you choose an adapter marked "Recommended." They are also always available from us directly when you buy the boxed version.

Virtualization Software Configuration

If your virtualization software supports USB 3.0 emulation (which is the case if you are using VMWare or Parallels Desktop for Mac), be sure to use USB 3.0 emulation rather than USB 2.0 emulation, even if the USB port and the Wi-Fi adapter you are going to use are USB 2.0. Support for USB 3.0 requires at least Windows 8 as the guest OS. USB configuration in VMWare is illustrated below.



Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	60 GB
CD/DVD (IDE)	Using file C:\Program Files (x86)\...
Floppy	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Connections

USB compatibility: USB 3.0

☑ Automatically connect new USB devices

□ Show all USB input devices

☑ Share Bluetooth devices with the virtual machine

USB 3.0 emulation is preferable because it dramatically increases the communication speed between the Wi-Fi adapter and guest OS. For example, in some adapters, switching the Wi-Fi channel might take 500 or even 1,000 milliseconds if you use USB 2.0 emulation and only 100 milliseconds if you use USB 3.0 emulation. Considering the fact that CommView for WiFi might switch channels every 250 milliseconds, this difference is dramatic. Using USB 2.0 emulation might slow down the application considerably.

For this reason, we recommend that you **do not use VirtualBox** as virtualization software. At the time of writing, VirtualBox has no USB 3.0 support. If you still want to use VirtualBox, at least use the **Enable USB 2.0 (EHCI) Controller** option; otherwise, your USB Wi-Fi adapter might not work.

Adapter Installation

Plug in the USB adapter into your computer. Once the adapter is plugged in, you will need to configure your virtualization software to use the detected USB device, i.e. disconnect it from the host OS and connect it to the guest OS. The configuration method depends on the specific virtualization software that you use; please refer to the related documentation. After the virtual machine takes control of the adapter, Windows will notify you that a new USB device has been found and will try to find the driver for the device. Click **Help => Driver Installation Guide** in CommView for WiFi to find the instructions for installing our special packet capture driver. Once that driver has been installed, you can restart the application and use it.

Multi-Channel Capturing

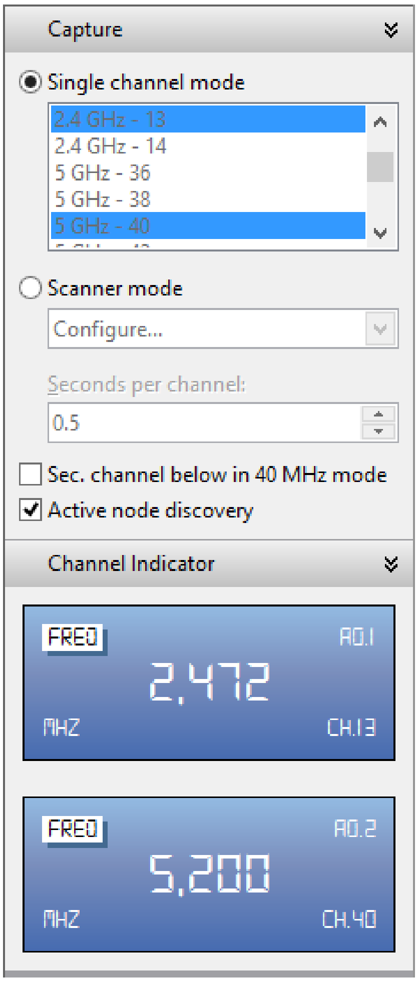
CommView for WiFi is capable of capturing data from multiple channels simultaneously if one uses multiple compatible USB adapters.

The following 802.11ac USB adapters can be used for multi-channel capturing: ASUS USB-AC68, Belkin F9L1109 v1, D-Link DWA-180 rev A1, D-Link DWA-182 rev C1 or D1, Edimax EW-7822UAC, Edimax EW-7833UAC, EnGenius EUB1200AC, Linksys WUSB6300, Linksys WUSB6400M, NETGEAR A6210, Proxim ORiNOCO 9100, Rosewill RNX-AC1200UB, TP-LINK Archer T4U, TP-LINK Archer T4UH, TP-LINK Archer T9UH v2, TRENDnet TEW-805UB, ZyXEL NWD6605, and ZyXEL AC240.

Note that different types of adapters cannot be mixed; all of the adapters should be of the same model. When multiple adapters are connected, the following interface elements are changed:

- The channel selection control on the **Capture** pane allows you to select multiple channels. You can select multiple channels by holding the **Ctrl** key. The number of channels that you select cannot exceed the number of plugged in USB adapters.
- The **Channel Indicator** pane displays multiple indicators, the number of which is equal to the number of plugged in USB adapters.

This is illustrated on the screen shot.



Capture

● Single channel mode

2.4 GHz - 13
2.4 GHz - 14
5 GHz - 36
5 GHz - 38
5 GHz - 40

○ Scanner mode

Configure...

Seconds per channel:

0.5

□ Sec. channel below in 40 MHz mode

☑ Active node discovery

Channel Indicator

When using multiple adapters, please consider the following:

1. Power consumption. A single adapter might need up to 450 mA of power. A single USB 2.0 port can provide up to 500 mA. A single USB 3.0 port can provide up to 900 mA. A typical modern laptop has two USB 3.0 ports, so you should either use one adapter per port, or you can use a USB hub, but if you plug in thee adapters into a USB 3.0 hub, you will exceed the 900 mA limit, which might cause undesirable effects, e.g. the adapters might stop capturing packets silently.

2. Channel switching time. When CommView for WiFi is working in scanner mode, switching channels takes some time, between 20 and 80 milliseconds per adapter. Consider a scan of 12 channels with the scanner interval of 250 ms per channel and the channel switch time of, say, 60 ms. The total time would be (250 + 60) * 12 = 3.72 seconds if you use a single adapter. If you use three adapters, the total time would be (250 + 60 *3) * 4 = 1.72 seconds. That is x2.16 times better, not x3 times better. Thus, adding adapters adds channel switching overhead. If you use 12 adapters, which is possible in theory, it will take 250 + 60 * 12 = 0.97 seconds to scan 12 channels, so you're not gaining much.

That said, we don't recommend using more than two or three adapters.

Spectrum Analysis

Spectrum analysis involves the use of special RF equipment designed to listen to and analyze the frequency bands utilized by Wi-Fi devices. Because these bands are unlicensed, they are often shared with non-Wi-Fi sources of RF signals, such as wireless video cameras, microwave ovens, or cordless phones, which cause interference. The purpose of spectrum analysis is to detect and identify such sources of interference, eliminate them, and/or identify the WLAN channels with minimal interference.

Hardware Requirements

CommView for WiFi can perform spectrum analysis by interfacing with Wi-Spy, a USB-based spectrum analyzer. Wi-Spy can be purchased from TamoSoft or directly from MetaGeek.

CommView for WiFi supports the following Wi-Spy models:

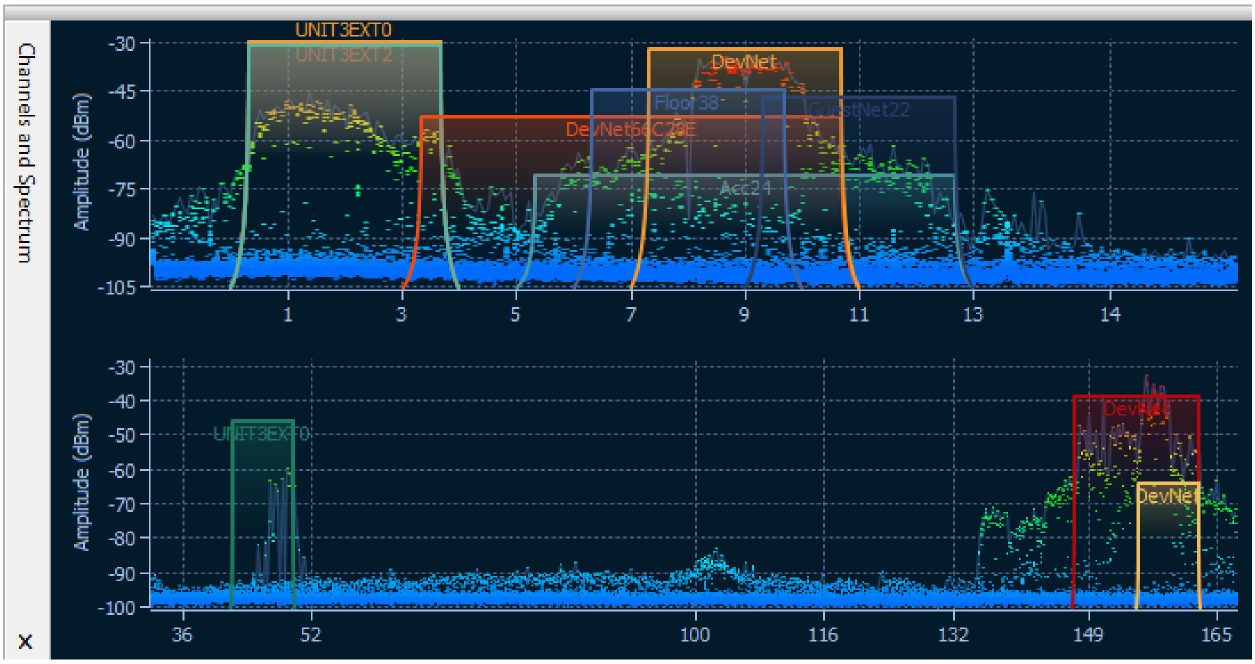
- Wi-Spy DBx (dual-band, 2.4 GHz and 5 GHz)
- Wi-Spy 2.4x (single-band, 2.4 GHz)
- Wi-Spy 2.4i (single-band, 2.4 GHz)

Note that CommView for WiFi DOES NOT support the oldest Wi-Spy model (“Wi-Spy original” with a green logo) or 900x models.

When a dual-band model, Wi-Spy DBx, is used, it continuously sweeps both bands, one after the other. Using two Wi-Spy DBx units simultaneously might improve data quality, as CommView for WiFi would dedicate each of the units to one band only.

Spectrum Data Graphs

When Wi-Spy is plugged in, a live spectrum picture is displayed on the **Channels and Spectrum** pane of the main CommView for WiFi window, as shown below.



The spectrum pane is similar to the one you can see in *Chanalyzer*, a spectrum analysis application by MetaGeek that comes with Wi-Spy. By default, the **Channels and Spectrum** pane displays one or two planar spectrum graphs for single- and dual-band Wi-Spy models, respectively.

The appearance of the graphs can be controlled via the context menu. Select **2.4 GHz**, **5.0 GHz**, or **Dual** to have the spectrum pane display one of the single frequency bands or two bands simultaneously (**5.0 GHz** and **Dual** are available only if you have a dual-band Wi-Spy model.) Select **Current Level** to display a line that shows the current signal amplitude; select **Max Level** to display a line that shows the maximum signal amplitude. The **X-axis** item allows you to select the measurement units of the horizontal axis; you can choose between **Frequency** in MHz and **Channel** numbers. By enabling the **Waterfall** view, you can have the application graph amplitude over time. Select **1/3**, **1/2**, or **2/3 of the window size** to adjust the area of the window occupied by the waterfall graph. The spectrum pane can be detached from the main application window and displayed as a separate floating window. Use the **Detach Window** and **Attach Window** to perform the respective operations. You can also hide the **Channels and Spectrum** pane by checking or unchecking the **View => Channels and Spectrum** item in the main application menu.

Note that in order to view spectrum data in CommView for WiFi, you must close Chanalyzer if it is running; Wi-Spy cannot be accessed and controlled by multiple applications simultaneously.

Capturing High Volume Traffic

When capturing data from a large and busy network segment, you should keep in mind that processing thousands of packets per second might considerably increase the CPU usage and make the application less responsive. The best way to optimize the program's performance is to use rules to filter out the packets you do not need to monitor. For example, sending a 50 MB file between two machines on your WLAN can generate approximately 40,000 NetBIOS packets with the data transfer rate of 5 MB per second, which can be a heavy load for the application. However, normally you do not to need to view every NetBIOS packet being sent, so you can configure CommView for WiFi to capture IP packets only. CommView for WiFi has a flexible system of filters, and you can fine-tune the application to display only the packets that you really need. In addition, if you are interested in the statistics information only (those green histograms, pie charts, and hosts tables), you can use the "Suspend packet output" menu command, which allows you to have statistical data without real-time packet display.

The factors that improve the program's performance:

- A fast CPU (Intel Core i7 is recommended)
- RAM size (8 GB and higher recommended)
- Using rules to filter out unnecessary traffic

Running CommView for WiFi in Invisible Mode

There are two ways to run CommView for WiFi as a hidden process:

1. Launch CommView for WiFi with the "hidden" switch, i.e.:

   ```
   CV.EXE hidden
   ```

2. If CommView for WiFi is already running, you can hide/unhide it by using the "hot key." To hide the application, press ALT+SHIFT+h. To unhide the application, press ALT+SHIFT+u.

Remember that you cannot completely hide any Windows application. When running in invisible mode, one can still see the CommView for WiFi process in Task Manager.

Command Line Parameters

You can use command line parameters to perform the following operations when the program is being launched:

- Load and activate a rule set from a file. Use the "/ruleset" switch followed by the file name and full path, e.g.:

  ```
  CV.EXE /ruleset "C:\Program Files\CommViewWiFi\Rules\POP3Rules.rls"
  ```

  If a file name or its path contains spaces, it must be enclosed in quotation marks (" ").

- Load and activate a WEP/WPA key set from a file. Use the "/keyset" switch followed by the file name and full path, e.g.:

  ```
  CV.EXE /keyset "C:\Program Files\CommViewWiFi\WLAN3Keys.wep"
  ```

  If a file name or its path contains spaces, it must be enclosed in quotation marks (" ").

- Use the specified folder for storing log files. Use the /logdir switch followed by the full path to the folder, e.g.

  ```
  CV.EXE /logdir "C:\Program Files\CommView\Logs"
  ```

- Launch the application without the prompt to install the driver. This is useful when you use CommView for WiFi for loading logs collected from other computers or for connecting to Remote Agents. Use the /noprompt switch, e.g.

  ```
  CV.EXE /noprompt
  ```

- Connect to one or several remote agents. Use the "/ra" switch followed by the IP address or hostname of the Remote Agent you'd like to connect to, followed by the password in quotation marks, followed by the channel number that should be monitored (the channel index is 1-based, i.e. if you need to monitor in scanner mode, use "1"; if you need to monitor the first channel, use "2"), e.g:

  ```
  CV.exe /ra 192.168.0.5 "MyPassword" 2
  ```

  To connect to multiple Remote Agents from the same CommView for WiFi instance, use a batch file that should look like this:

  ```
  START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /noprompt
  PING 1.1.1.1 -n 1 -w 5000 >NUL
  START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /ra 192.168.0.1 "pwd1" 5
  PING 1.1.1.1 -n 1 -w 1000 >NUL
  START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /ra 192.168.0.2 "pwd2" 5
  PING 1.1.1.1 -n 1 -w 1000 >NUL
  START "CV" "C:\Program Files\CommViewWiFi\CV.exe" /ra 192.168.0.3 "pwd3" 5
  PING 1.1.1.1 -n 1 -w 1000 >NUL
  ```

  This script launches CommView for WiFi, waits for 5 seconds to make sure that the application is loaded (we use the PING command to pause because there is no direct way of telling a .BAT file to pause), then we pass to the application the IP addresses, passwords, and adapter numbers of three Remote Agents (with one-second pauses).

You can use all of these parameters, except the last one, at the same time.

Exchanging Data with Your Application

CommView for WiFi provides a simple TCP/IP interface that allows you to process packets captured by CommView for WiFi using your own application in real time. Starting with version 5.0 you may also use this interface for sending packets (similar to the Packet Generator function in CommView for WiFi).

How It Works

CommView for WiFi should be launched with a special command-line argument, "MIRROR", that tells the program to mirror captured packets to an IP address and TCP port of your choice.

Examples:

CV.EXE mirror:127.0.0.1:5555 // mirrors packets to the loopback address, TCP port 5555
CV.EXE mirror:192.169.0.2:10200 // mirrors packets to 192.169.0.2, TCP port 10200

When CommView for WiFi is launched with a switch like this, it tries to establish a TCP session by connecting to the specified IP address and port number. It means that you should already have your application running and listening on the specified port. If CommView for WiFi fails to establish a connection, it will keep on trying to connect every 15 seconds. The same happens if the connection is broken: CommView for WiFi will try to re-establish it every 15 seconds. If the connection is successfully established, CommView for WiFi sends the packets it captures to the specified IP address as they arrive, in real time.

Data Format

The data is transmitted in NCFX format. Please refer to the CommView Log Files Format chapter for the format description.

Sending Packets

Packets may not only be received by your application but also sent as if you were using Packet Generator. Data can be sent to CommView for WiFi using the same TCP connection over which you are receiving the data. The data format is simple: You should send the packet length (a two-byte unsigned integer in the standard little-endian byte order) followed by the data rate index (a two-byte unsigned integer in the standard little-endian byte order) followed by the packet itself. Packet length should not include the four bytes that precede the packet body. Data rate index is zero-based; it should contain the index of the rate as shown in the Packet Generator. Consider the following example:

String to be sent in hex: D4 00 00 00 80 1F 02 66 C2 8E. The length of this string is 10 bytes.
Rate to be used: 5.5 Mbps. This is the third item in the "802.11 data rate" drop-down list in the Packet Generator.
Resulting buffer to be sent: 0A 00 02 00 D4 00 00 00 80 1F 02 66 C2 8E.

If the adapter is not opened or it does not support packet injection, the packet is silently discarded.

Sample Projects

Two simple demo applications that listen for inbound connections, extract packets from the stream, and display raw data are available.

- http://www.tamos.com/products/commwifi/samp_mirr_c7.zip. This is a Visual Studio project with C++ source code.
- http://www.tamos.com/products/commwifi/samp_mirr_d7.zip. This is a Delphi project with Pascal source code. If you want to compile the project, you will need the popular ICS components suite by Francois Piette, available at http://www.overbyte.be.

Bandwidth

When mirroring data to a remote computer, make sure that the link between CommView for WiFi and the computer to which the data is being mirrored is fast enough to transfer all the data being captured. If CommView for WiFi captures 500 Kbytes/sec, and your link can handle only 50 Kbytes/sec, you'd inevitably have "traffic jams," which might result in various problems (e.g., Winsock may just stop sending data under some Windows versions).

Custom Decoding

CommView for WiFi allows you to use two types of your own custom decoders.

Simple Decoder

If you implement this type of decoder, the output of your decoder will be displayed in the additional column in the **Packets** tab. Your decoder must be a 32-bit DLL file named "Custom.dll" that exports the only procedure named "Decode." The prototype of this procedure is shown below in C and Pascal:

```
extern "C" {

void __stdcall Decode(unsigned char *PacketData, int PacketLen, char *Buffer, int BufferLen);

}

procedure Decode (PacketData: PChar; PacketLen: integer; Buffer: PChar; BufferLen: integer); stdcall;
```

The DLL must be located in the CommView for WiFi application folder. When you launch CommView for WiFi, it looks for "Custom.dll" in the application folder and loads it into memory. If the "Decode" entry point is found, CommView for WiFi adds a new column named "Custom" to the packet list.

When a new packet is captured and is about to be displayed, CommView for WiFi calls the "Decode" procedure and passes the packet contents to the DLL. The "Decode" procedure must process the packet data and copy the result to the supplied buffer. The first argument is the pointer to the packet data, the second argument is the data length, the third argument is the pointer to the buffer where the results of your decoding must be copied to, and the forth argument is the buffer size (currently always 1024 bytes). The buffer is allocated and freed by CommView for WiFi, so do not attempt to reallocate or free it. The result that you copied to the buffer will be displayed as a string in the "Custom" column.

Your procedure must be fast enough to handle thousands of packets per second; otherwise, it may slow down the application. Do not forget to use the STDCALL calling convention. Two demo DLLs are available. They demonstrate a very simple operation: The output of the "Decode" function is the hex code of the packet's last byte. Your own decoder can be as complex as you wish.

- http://www.tamos.com/products/commview/cust_decoder_c.zip. This is a Visual Studio project with C++ source code.
- http://www.tamos.com/products/commview/cust_decoder_d.zip. This is a Delphi project with Pascal source code.

Complex Decoder

If you implement this type of decoder, the output of your decoder will be displayed as additional items in the packet decoder tree. For information on the implementation of this decoder, please download the following file:

http://www.tamos.com/products/commview/complex_decoder_c7.zip

This type of decoder can be written in Microsoft Visual C++ only, as it is built using C++ classes.

Technical Support

Technical support for custom decoders is provided on the "best effort" basis. We may not be able to answer your programming-related questions.

CommView Log Files Format

CommView and CommView for WiFi use the data format described below for writing captured packets to .NCF or .NCFX files. This is an open data format that you can use for processing log files generated by CommView in your applications, as well as for exchanging data with your application directly (this method is described in this help file).

NCFX Format

This new format was introduced in CommView for WiFi 7.3. Older CommView for WiFi versions and current CommView (non-Wi-Fi) versions use the old NCF format described in the corresponding section below.

Packets are recorded consecutively. Two or more headers, the structure of which is given below, prepend each packet body. All header fields with the length exceeding one byte use little-endian order and are unsigned.

General Header – Mandatory. Length = 20 bytes.

Field name	Length (bytes)	Description
Data length	4	The length of the packet, including the length of this and the following headers and including the length of the packet contents (body).
Year	2	Packet date (year)
Month	1	Packet date (month)
Day	1	Packet date (day)
Hours	1	Packet time (hours)
Minutes	1	Packet time (minutes)
Seconds	1	Packet time (seconds)
Microseconds	4	Packet time (microseconds)
Medium type	1	The type of the packet medium. 0x01 for Wi-Fi packets, 0x00 for Ethernet packets.
Decryption flag	1	0x01 if the packet has already been decrypted by CommView for WiFi and is being saved in decrypted form. 0x00 otherwise.
Direction	1	For Ethernet packets, packet direction: 0x00 for pass-through, 0x01 for inbound, 0x02 for outbound. For Wi-Fi packets, always 0x00.
Reserved1	1	Currently unused
Reserved2	1	Currently unused

RF Header – Mandatory. Length = 20 bytes.

Field name	Length (bytes)	Description
RF Header length	2	The length of this header, including the length of all additional extensions (headers), if any.
Packet status and modulation	2	A bitmask where one or several of the following bits are set: Bit 0 – the packet is damaged (wrong FCS) Bit 1 – Packet sent using an HT PHY rate (802.11n) Bit 2 – Packet sent using an VHT PHY rate (802.11ac) Bit 3 – Packet sent using an HE PHY rate (802.11ax) Bit 4 – HE modulation, 0 – OFDM, 1 – OFDMA, valid only if Bit 3 is set.
Frequency band	2	0x40 for 5 GHz, 0x80 for 2.4 GHz
Channel	2	Wi-Fi channel
Noise in dBm	1	Noise level in dBm, as an unsigned value. E.g., -90 dBm is stored as 90.
Signal in dBm	1	Signal level in dBm, as an unsigned value. E.g., -30 dBm is stored as 30.
Signal in percent	1	Signal level as percentage
Reserved	1	Currently unused
PHY Rate	4	PHY data transmission rate in Mbps multiplied by 10
Extensions' presence	4	A bitmask indicating the presence of additional extensions (headers) following this RF header. For example, if the bits 3, 2, and 0 are set, then this RF header is followed by an extension of type 0, then the extension of type 2, and then the extension of type 3.

Currently Supported Extensions

MCS Header Type 0 – Optional. Size = 4 bytes.

Note that the MCS Header Type 0 is never added if you capture packets using a pre-802.11ac adapter. MCS information is added only if use 802.11ac or 802.11ax adapters for capturing.

Field name	Length (bytes)	Description
MCS Index	1	MCS index
Number of streams	1	Number of MIMO spatial streams less 1; i.e. the 0x00 value means one stream.
Channel width	1	Channel width If bit 4 of the **Packet status and modulation** field equals 0 (OFDM modulation): 0x00 – 20 MHz, 0x01 – 40 MHz, 0x02 – 80 MHz, 0x03 – 160 MHz. If bit 4 of the **Packet status and modulation** field equals 1 (OFDMA modulation): 0x00 - 26-tone RU, 0x01 – 52-tone RU, 0x02 – 106-tone RU, 0x03 – 242-tone RU, 0x04 – 484-tone RU, 0x05 – 996-tone RU, 0x06 – 1992-tone RU (996x2-tone RU)
GI	1	Guard Interval: 0x00 - 0.8µs, 0x01 - 0.4µs, 0x02 - 1.6µs, 0x03 - 3.2µs

The packet body follows the headers. The packet body does not contain the 4-byte FCS at the end.

Example #1: A 350-byte long beacon packet sent at the legacy PHY rate of 6 Mbps would be stored as:

[20 bytes of the General Header, in which the **Data length** field is set to 390] + [20 bytes of the RF header, in which the **RF Header length** field is set to 20 and in which **the Extensions' presence** field is set to 0x00000000] + [350 bytes of the packet body]

Example #2: A 1002-byte long data packet sent at the VHT PHY rate of 72.2 Mbps would be stored as:

[20 bytes of the General Header, in which the **Data length** field is set to 1046] + [20 bytes of the RF header, in which the **RF Header length** field is set to 24 and in which the **Extensions' presence** field is set to 0x00000001] + [4 bytes of the MCS Header] + [1002 bytes of the packet body]

NCF Format

This format is used in CommView (any version) and CommView for WiFi version 7.2 and older. Newer CommView for WiFi versions (7.3 and newer) use the NCFX format described in the corresponding section above.

Packets are recorded consecutively. A 24-byte header, the structure of which is given below, prepends each packet body. All header fields with the length exceeding 1 byte use little-endian byte order.

Field name	Length (bytes)	Description
Data Length	2	The length of the packet body that follows the header
Source Data Length	2	The original length of the packet body that follows the header (without compression). If no compression is being used, the value of this field is equal to the value of the previous field.
Version	1	Packet format version (0 for the current implementation)
Year	2	Packet date (year)
Month	1	Packet date (month)
Day	1	Packet date (day)
Hours	1	Packet time (hours)
Minutes	1	Packet time (minutes)
Seconds	1	Packet time (seconds)
Microseconds	4	Packet time (microseconds)

<table>
<tr><th>Field name</th><th>Length (bytes)</th><th>Description</th></tr>
<tr><td><b>Flags</b></td><td>1</td><td>Bit flags:
<table>
<tr><td>Medium</td><td>0...3</td><td>Medium type for the packet (0 - Ethernet, 1 - WiFi, 2 - Token Ring)</td></tr>
<tr><td>Decrypted</td><td>4</td><td>The packet has been decrypted (applicable to WiFi packets only)</td></tr>
<tr><td>Broken</td><td>5</td><td>The packet was corrupted, i.e. had the incorrect CRC value (applicable to WiFi packets only)</td></tr>
<tr><td>Compressed</td><td>6</td><td>The packet is stored in compressed form</td></tr>
<tr><td>Reserved</td><td>7</td><td>Reserved</td></tr>
</table></td></tr>
<tr><td><b>Signal Level</b></td><td>1</td><td>Signal level in percent (applicable to WiFi packets only)</td></tr>
<tr><td><b>Rate</b></td><td>1</td><td>Data transmission rate in Mbps multiplied by 2 (applicable to WiFi packets only)</td></tr>
<tr><td><b>Band</b></td><td>1</td><td>Transmission band. 0x01 for 802.11a, 0x02 for 802.11b, 0x04 for 802.11g, 0x08 for 802.11a-turbo, 0x10 for 802.11 SuperG, 0x20 for 4.9 GHz Public Safety, 0x40 for 5 GHz 802.11n/ac, 0x80 for 2.4 GHz 802.11n/ac. (applicable to WiFi packets only)</td></tr>
<tr><td><b>Channel</b></td><td>1</td><td>Channel number (applicable to WiFi packets only)</td></tr>
<tr><td><b>Direction</b></td><td>1</td><td>For non-WiFi packets, packet direction. 0x00 for pass-through, 0x01 for inbound, 0x02 for outbound. For WiFi packets, the high order byte for the packet rate, if the one-byte Rate field cannot accommodate the value (i.e. the value is higher than 255).</td></tr>
<tr><td><b>Signal Level (dBm)</b></td><td>1</td><td>Signal level in dBm (applicable to WiFi packets only)</td></tr>
<tr><td><b>Noise Level (dBm)</b></td><td>1</td><td>Noise level in dBm (applicable to WiFi packets only)</td></tr>
<tr><td><b>Data</b></td><td>Variable</td><td>Packet body (unmodified, as transmitted over the media). If the compression flag is set, the data is compressed using the publicly available Zlib 1.1.4 library. The length of this field is recorded in Data Length.</td></tr>
</table>

The total header length is 24 bytes.

If packets are stored in compressed form, the **Data Length** field contains the length of data after compression, whilst the **Source Length** field contains the original data length. If a packet is uncompressed, both fields contain the same value.

Information

How to Purchase CommView for WiFi

This program is a 30-day evaluation version. You can purchase the fully functional, unrestricted version of the program by visiting our Web site. Two license types are currently available for CommView for WiFi: **Standard** license and **VoIP** license. The more expensive VoIP license enables all the application features, including VoIP analyzer, whereas the standard license does not enable VoIP analyzer.

Check our Web site for current pricing on single-user and multi-user licenses. One licensed copy of CommView for WiFi may be used by a single person who uses the software personally on one computer. A second copy may be installed on one additional portable computer. Please refer to the End User License Agreement that is displayed when you install the application for the official, detailed description of our licensing policy.

As a registered user, you will receive:

- Fully functional, unrestricted copy of the software
- Free updates that will be released within 1 year from the date of purchase
- Information on updates and new products
- Free technical support

We accept credit card orders, orders by phone and fax, checks, purchase orders, and wire transfers. Prices, terms, and conditions are subject to change without notice: please check our web site for the latest product offerings and prices.

http://www.tamos.com/order/