Testing the fabric of IP communications™

WinEyeQ

Revision 1.7.1

June 20, 2007

Touchstone Technologies, Inc.
228 North York Road, Suites C & D
Hatboro, PA 19040
Tel: 215-672-6550
Fax: 215-672-6551

www.touchstone-inc.com

Table of Contents

Introduction

The WinEyeQ VoIP call monitor and protocol analyzer is the ideal tool for anyone who needs to monitor Voice and Video over IP calls and Voice quality, detect errors in VoIP traffic, debug signaling problems or capture media streams. WinEyeQ's intuitive user-interface makes setup and operation a snap.

With WinEyeQ you view your network traffic in an intuitive manner. From network overview to media stream and protocol details, each piece of information is presented in context. WinEyeQ's analysis does not stop at the call flow level; however, it provides unparalleled analysis of each individual call component making difficult diagnostics simple.

WinEyeQ is designed for the advanced 32 bit Windows operating systems. The following operating systems are supported:

Windows 2000 Professional, Windows 2000 Advance Server, Windows XP Professional, Windows 2003 Server.

WinEyeQ's capabilities automatically scale with the hardware on which it is installed.

Minimum recommended configuration:

- 2.4 MHz Pentium 4 Processor
- 512MB Ram
- 60 GB hard drive
- 1280x1024

WinEyeQ is optimized for 1280 x 1024 displays.

The WinEyeQ software is copy protected and is licensed for use on a single machine. Please make sure that you install WinEyeQ on the machine with which you intend to use it. Installation of WinEyeQ on multiple machines is not possible without authorization from Touchstone.

The following pages will demonstrate how to install, setup, and get started with WinEyeQ. The next session is an overview of the latest additions.

Version 1.5.0 Summary

New Definitions

Component
A tangible, measurable, or quantifiable element of an environment.

Data Scope
A graphical representation of a logical group of components organized in a "zoom-able" or variable-power fashion. Depths vary based upon logical grouping level, ranging from telescopic through microscopic.

Histogram
This is a historical representation of a component's value.

Anonymous or Rogue Media Streams
Any audio or video stream transmitted via RTP that WinEyeQ does not associate with an active or watched call.

Comments
Initially conceived as strictly a VoIP analyzer with monitoring capabilities; WinEyeQ is evolving into a comprehensive core component for monitoring, analyzing and diagnosing today's converging networks. The addition of Data Scope presentations and support for anonymous or "Rogue" media streams provide both breadth and depth to WinEyeQ's capabilities.

New Features
Continuing with WinEyeQ's "VoIP-centric" approach, Data Scopes provide a dramatic, immediately intuitive picture of the VoIP and non-VoIP components of your network. These groupings represent a broadening of scope for WinEyeQ, enabling engineers to have a clear, high-level picture of the network. This capability allows them to quickly identify and detect anomalies while simultaneously providing the ability to drill-down on any component at any time.

Another, much-requested capability makes its debut in 1.5.0. WinEyeQ now supports the detection, tracking, quantifying and qualifying of "Rogue" RTP media streams for both audio and video. These streams are defined as any RTP-based media connections that have been detected outside of analyzed capability exchanges. This new capability allows WinEyeQ to be used in any media-rich environment to analyze, quantify and qualify both audio and video streams regardless of the signaling protocol used to provide session control.

Version 1.5.1 Summary

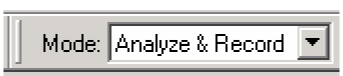
New Features

This version of WinEyeQ contains a Mode of Operation feature. There are three Modes of operation:

Analyze Network

This is the normal mode of operation for WinEyeQ. Packets are captured either from a live network or read in from files of previously captured data. VoIP calls are assembled and displayed on the screen. Individual call metrics are displayed. Various reports may be generated and network statistics are calculated and displayed. This is the suggested mode of operation.

Analyze and Record

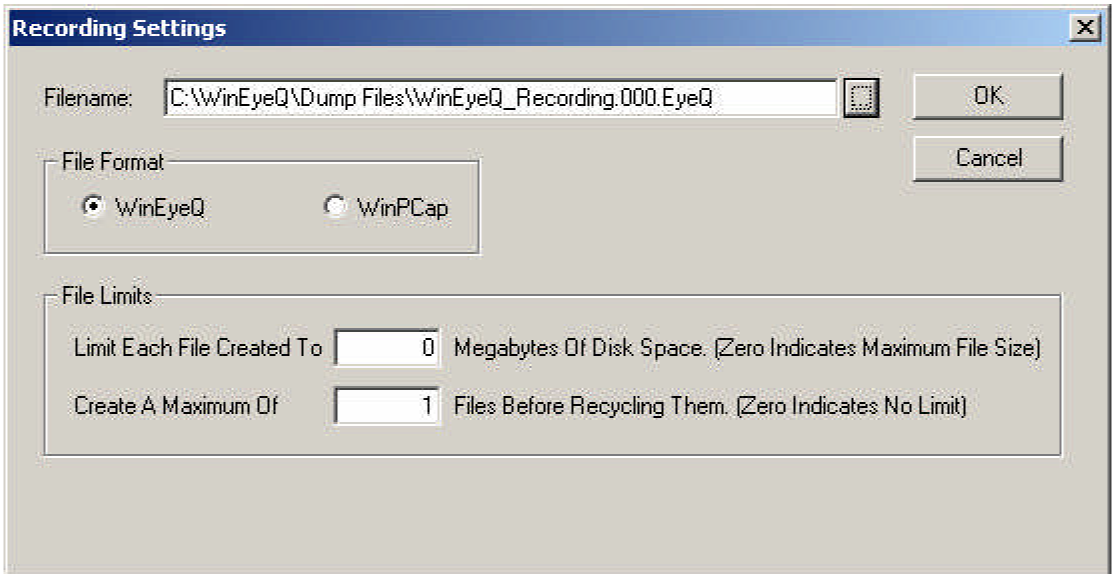


This mode of operation is the same as the Analyze Network mode except that a trace file of all the packets received by WinEyeQ is also created. The user can specify the name of the file and its format, either native WinEyeQ or WinPcap, and the maximum file size. This mode of operation could be used create a trace of an error condition that includes the events that lead up to that condition.

Record Only

This mode of operation only creates a trace file of the packets received by WinEyeQ. The packets are not examined and nothing is displayed on the screen. The user can specify the name of the file and its format, either native WinEyeQ or WinPcap, and the maximum file size. This mode of operation can be used to create trace files for offline analysis.

If you start WinEyeQ in Analyze & Record Mode or Record Only Mode, the following dialog will be displayed:



Please enter the name of the file you want to create, the format for that file, the maximum size of each file that will be created, and the maximum number of files to create.

When WinEyeQ begins recording (using the above example), it will create up to 10 files in the WinEyeQ format, each up to 100 megabytes in size. The first file created will be named WinEye_Recording.000.EyeQ. If it reaches 100 megabytes in size, it will be closed and a new file named WinEye_Recording.001.EyeQ will be created. If that file reaches 100 megabytes, it will be closed and another file named WinEye_Recording.002.EyeQ will be created and so on up to a maximum of 10 files. When 10 files have been created, the file-naming scheme will start over again with WinEye_Recording.000.EyeQ.

Note: The trace files that WinEyeQ creates can grow very large especially if there is a lot of traffic on the network. Be sure to filter out as much unnecessary traffic as possible (See Selecting the Network Adapter and Packet Capture Filter).

Version 1.5.2 Summary

New Features

This version of WinEyeQ implements a new folder structure that separates reports, captures, traces, etc. out of the main WinEyeQ folder. At the present time the folder names are fixed and are as follows:

Audio Capture Files

Audio streams (Rogue or from Watched calls) that are captured will be created here. These streams are in their raw form, i.e. as if they were taken directly from the output of the CODEC that generated them.

Video Capture Files

Video streams (Rogue or from Watched calls) that are captured will be created here. These streams are in their raw form, i.e. as if they were taken directly from the output of the CODEC that generated them.

Trace Files

When the user selects 'Call Trace,' 'Watch Trace,' or 'Error Trace,' the trace files will be created here. These trace files are text files that show each packet of a call.

Reports

All user-selected reports will be created here.

Record Files

When the user selects "Record Watched Calls," the recorded files will be created here.

Dump Files

When the user selects "Analyze and Record" or "Record Only" in the "Mode" dropdown list, the recorded files will be created here.

Capture Files

When the user selects "Capture Watched Calls" or "Capture Calls With Errors," the recorded files will be created here.

Version 1.5.3 Summary

New Features

This version of WinEyeQ allows the user to capture rogue media streams to the disk by right clicking the stream on the Audio or Video channels screen, then select Start Capture or Stop Capture.

There is a new Alert / Alarm that detects duplicate media stream destinations, i.e. two different source endpoints sending to the same destination endpoint.

WinEyeQ will now not report a SIP response of 486 Busy as an error.

Version 1.5.4 Summary

New Features

WinEyeQ added support for H.264 Video and AAC LD Audio for H.323 calls.

There is a new tab on the Active Calls and Watched Calls screen that provides metrics for data (neither audio nor video) channels.

The select adapter screen now accepts a range of IP addresses.

A WinEyeQ user can now configure the jitter buffer and international QoS settings.

Support has been added to decode and analyze RTCP XR messages. A new RTCP XR report saves this information to the disk.

All WinEyeQ reports now support size, interval, and time of day constraints. The current report file will be closed and a new one opened when the report reaches a certain size (in megabytes), or periodically (hours and minutes) or at a certain time of the day (midnight for example).

There is a new idle timeout parameter on the Settings menu: Calls Tab. This parameter specifies the amount of time a call will be considered active when it is not transmitting data in one direction or the other. The other idle timeout parameter is for calls that are not transmitting in both directions.

Version 1.7.0 Summary

New Features

In past versions of WinEyeQ, there was ‘Maximum Calls’ configuration parameter. This parameter was the maximum number of calls and registrations that WinEyeQ would track and was based on the version of the application (Professional, Lite, and Demo). There are now two parameter values, first, ‘Maximum Calls’ which limits the number of calls and second, ‘Maximum Registrations’ which limits the number of registrations. These two parameters are independent of each other but are still limited by the version of the program. The maximum number of registrations is twice the number of call allowed.

There is now a ‘Top Talkers’ sub-tab on Endpoints screen. This tab shows the endpoints that have placed / received the most calls, have been connected the longest, and have used the most bandwidth.

WinEyeQ now has the ability to capture media streams in raw or packetized format. Previously the streams were only captured in the raw format. The packetized format preserves the RTP header information of each packet that is saved to the disk. Both of these file formats can be used by Touchstone’s call generators to generate RTP test patterns or another application that can post process the media file.

A 'Recent Calls' tab has been added to the main screen. This screen shows the calls that have completed successfully after they have been removed from the Active Calls screen. Calls that are unsuccessful are still added to the Recent Errors screen.

This version of WinEyeQ now can generate SNMP traps. The traps are triggered by exceeding Alert / Alarm thresholds as configured by the user. See Appendix B for SNMP samples.

A new call scoring method has been added to WinEyeQ. This provides a simple way for the user to evaluate the quality of the call. Each call is given a letter grade and a numerical score. Each media stream present as well as the signaling time is factored together to for an overall call score. Please see Appendix C for scoring details.

An option has been added to the Reports tab that ensures that all report files will have unique names.

Version 1.7.1 Summary

Changes for Release 1.7.1

- Corrected problem using SNMP default IP address 255.255.255.255
- Replaced file extension *.cap with *.pcap in all file dialogs

Installation Types

WinEyeQ on CD-ROM

If you received WinEyeQ on CD-ROM, please use the following procedure:

- Insert the WinEyeQ CD in your CD-ROM drive.
- The installation program should start automatically. If it does not, use Windows Explorer to browse the CD and double-click the Setup.exe file.
- Continue to the next section.

WinEyeQ via E-Mail

If you received WinEyeQ via E-Mail, please use the following procedure:

- Double-click on the e-mail attachment.
- Select "Save to Disk" option and select a temporary folder to store the self-extracting file.
- Use Windows Explorer to browse to the folder in which you saved the self-extracting file.
- Double-click the self-extracting file. Select a folder with which to extract the files.
- Use Windows Explorer to browse to the folder you extracted the files in and double-click the Setup.exe file.
- Continue to the next section in this document.

WinEyeQ via the Internet

If you downloaded WinEyeQ via the internet, please use the following procedure:

- WinEyeQ's setup.exe is compressed using WinZip. Download wineyeq.zip and extract the setup.exe to a temporary location on the destination computer.
- Double-click on the Setup.exe file.
- Continue to the next section in this document.

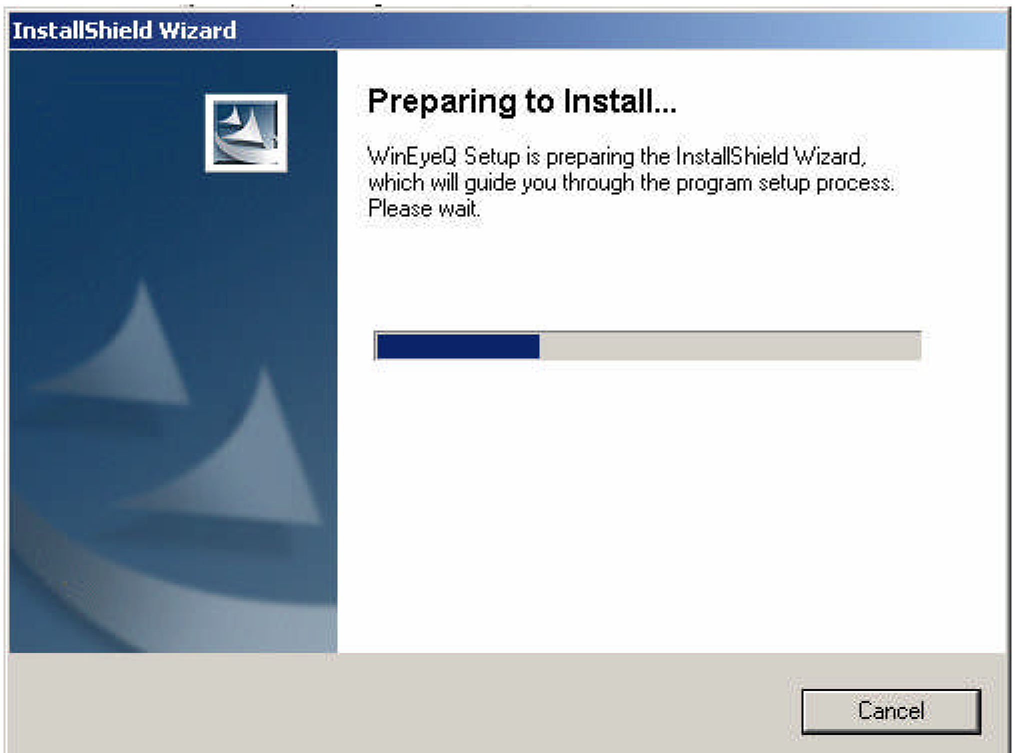
WinEyeQ Installation

The next few screens will appear during the installation process. Please follow the directions carefully using the "Next" button to navigate forward and the "Back" button to return to a previous page.

WinEyeQ Install Screen 1

Preparing Setup Wizard

Wait for the wizard to complete or press the "Cancel" to quit the installation.

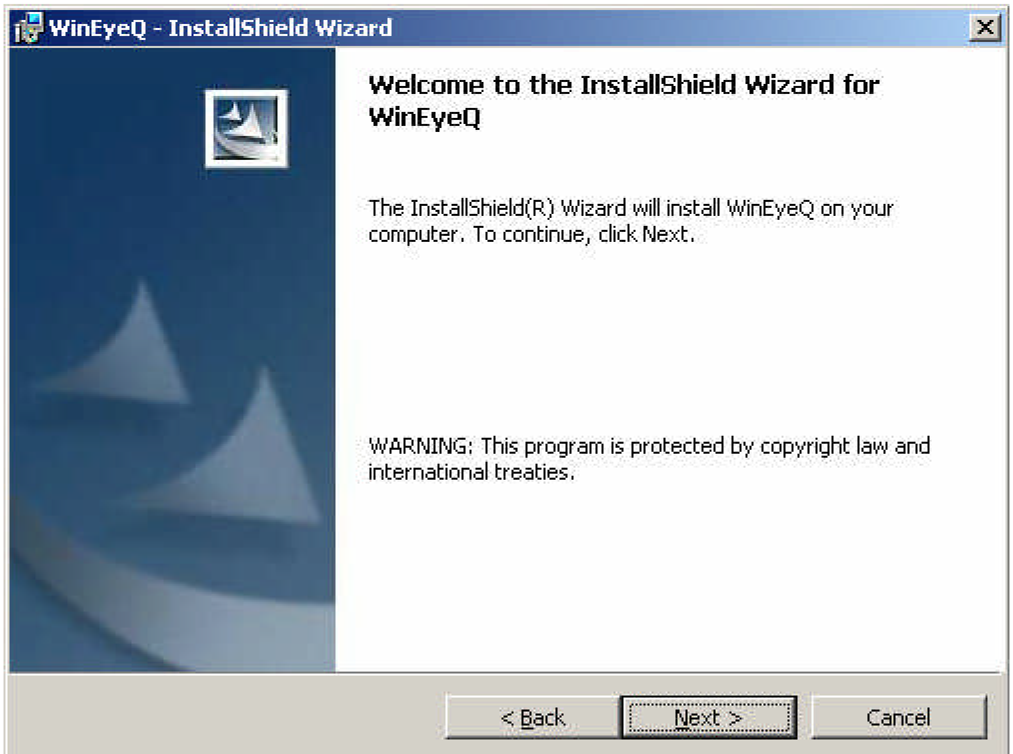


WinEyeQ Install Screen 2 - Beginning the Installation

Press the "Next" button to continue the installation or "Cancel" to quit.

WinEyeQ Install Screen 3 - Beginning the Installation

Press the "Next" button to continue the installation or "Cancel" to quit.



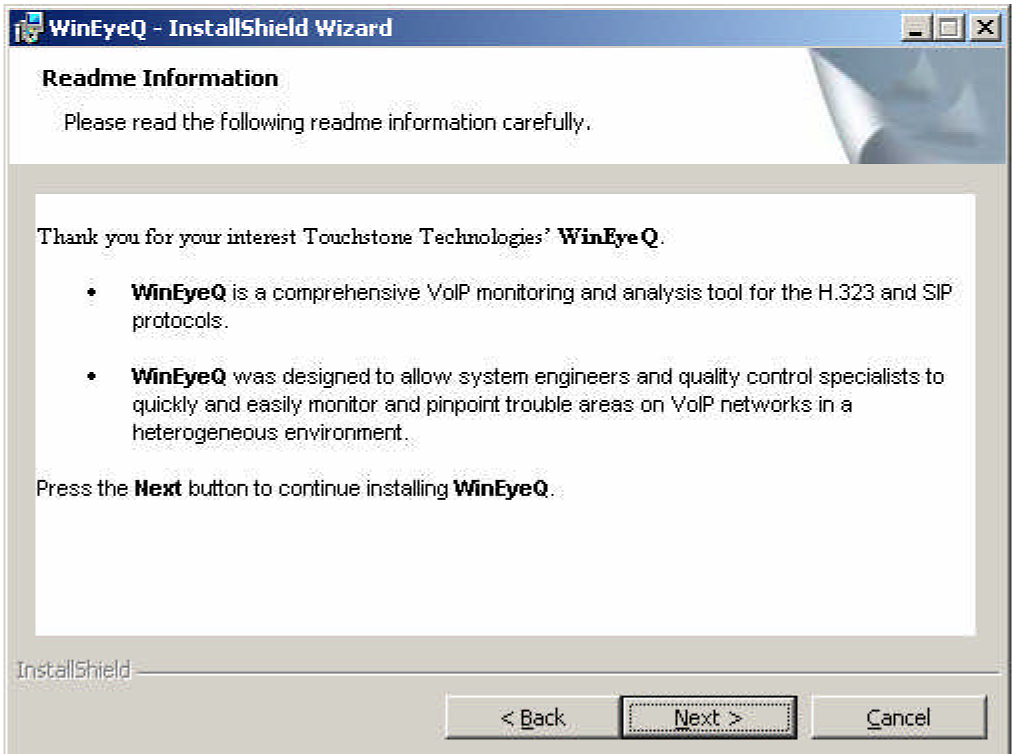
WinEyeQ Install Screen 4 - End-User License Agreement

Carefully read the End-User License Agreement. If you accept the terms, select the "I Accept" option, if you do not; select the "I do not accept" option.

Press the "Next" button to continue the installation or "Cancel" to quit.

WinEyeQ Install Screen 5 - Readme Information

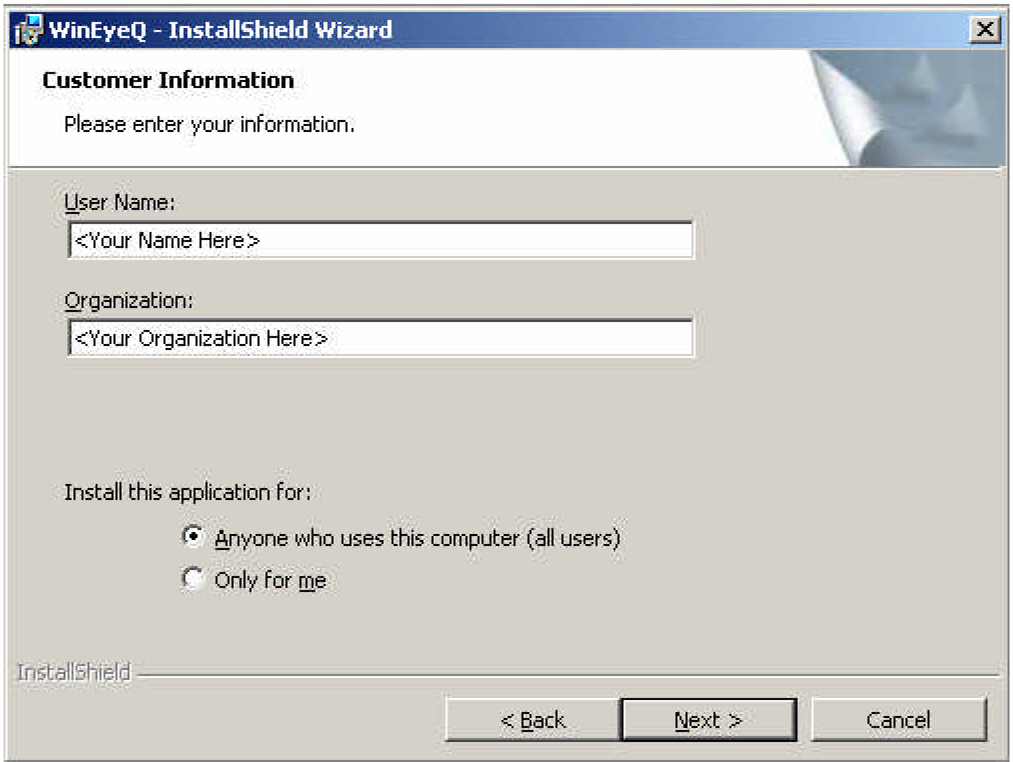
Press the "Next" button to continue the installation or "Cancel" to quit.



WinEyeQ Install Screen 6 - Customer Information

Please fill in your customer information and select the appropriate security option.

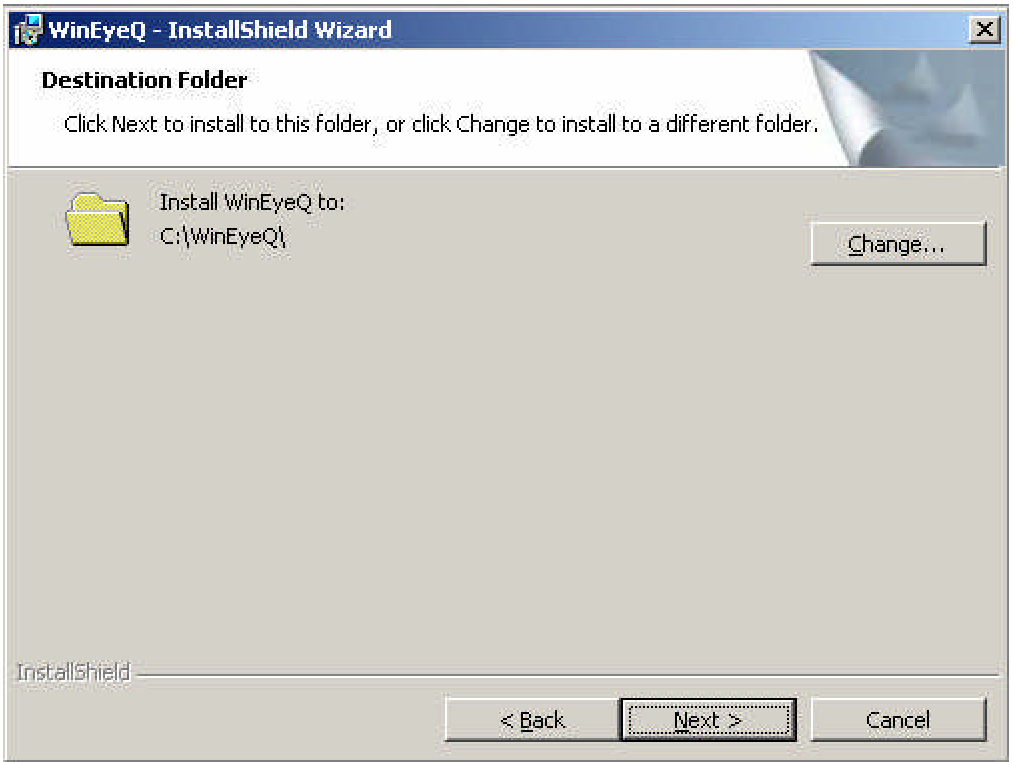
Press the "Next" button to continue the installation or "Cancel" to quit.



WinEyeQ Install Screen 7 - Destination Folder

Please select the folder in which you would like to install WinEyeQ and its components.

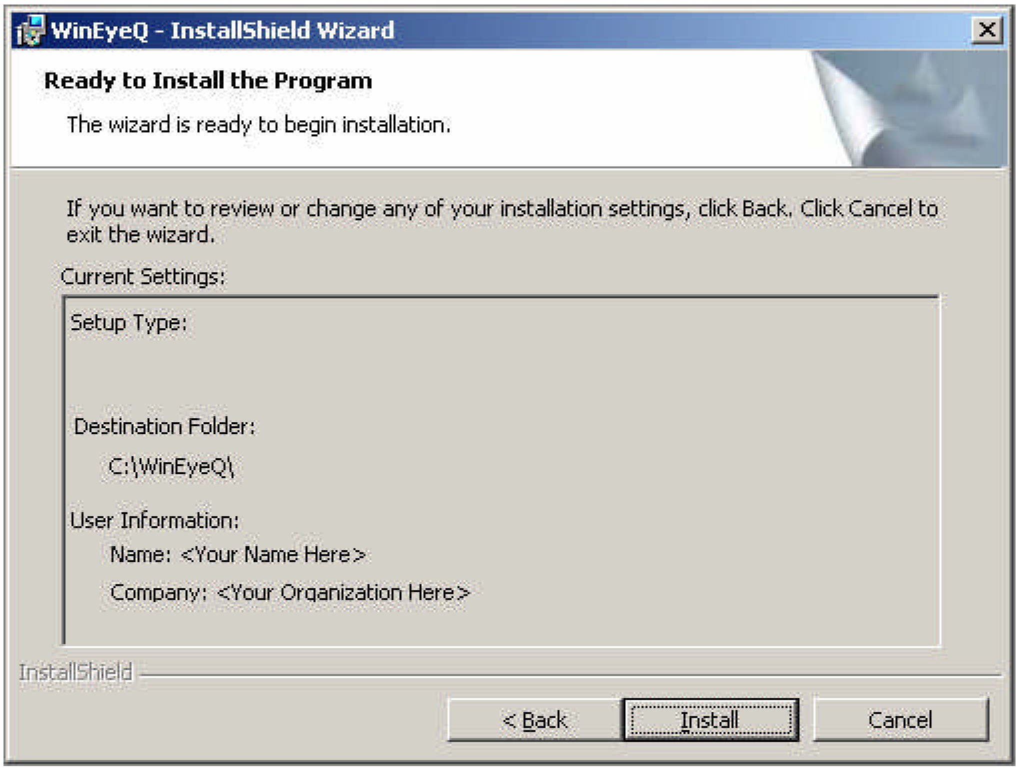
Press the "Next" button to continue the installation or "Cancel" to quit.



WinEyeQ Install Screen 8 - Ready to Install

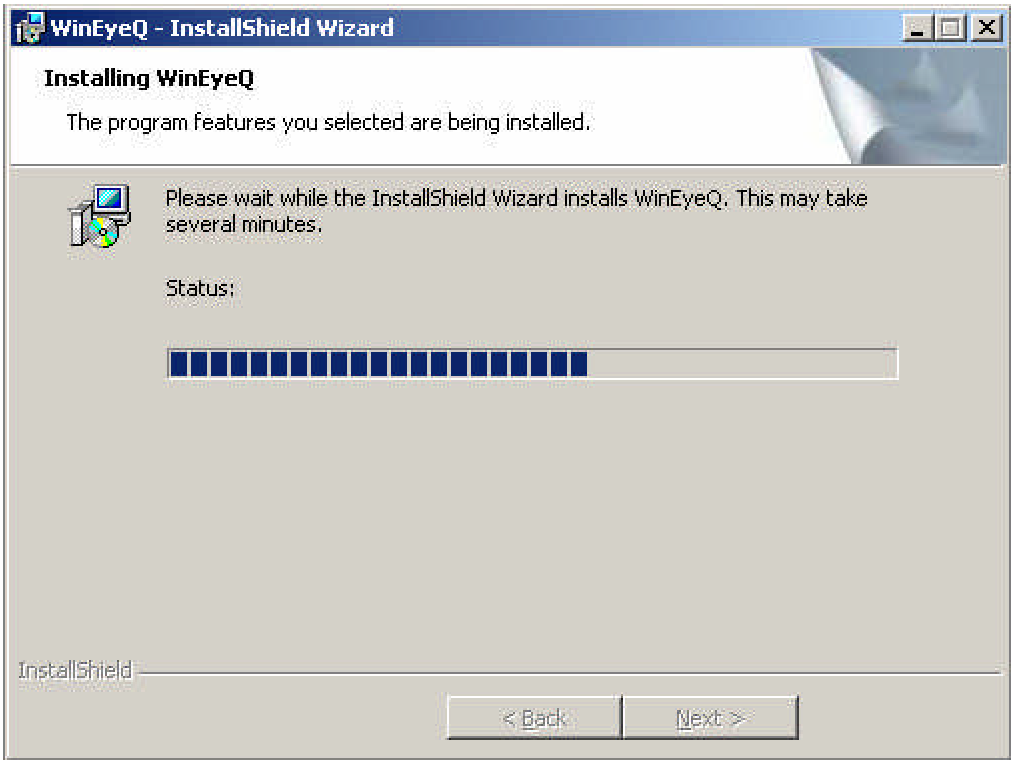
Please review the information, if you need to correct anything, use the "Back" button to navigate to the appropriate screen, make your changes and use the "Next" button to advance back to this point.

Press the "Install" button to continue the installation or "Cancel" to quit.



WinEyeQ Install Screen 9 - Installing WinEyeQ

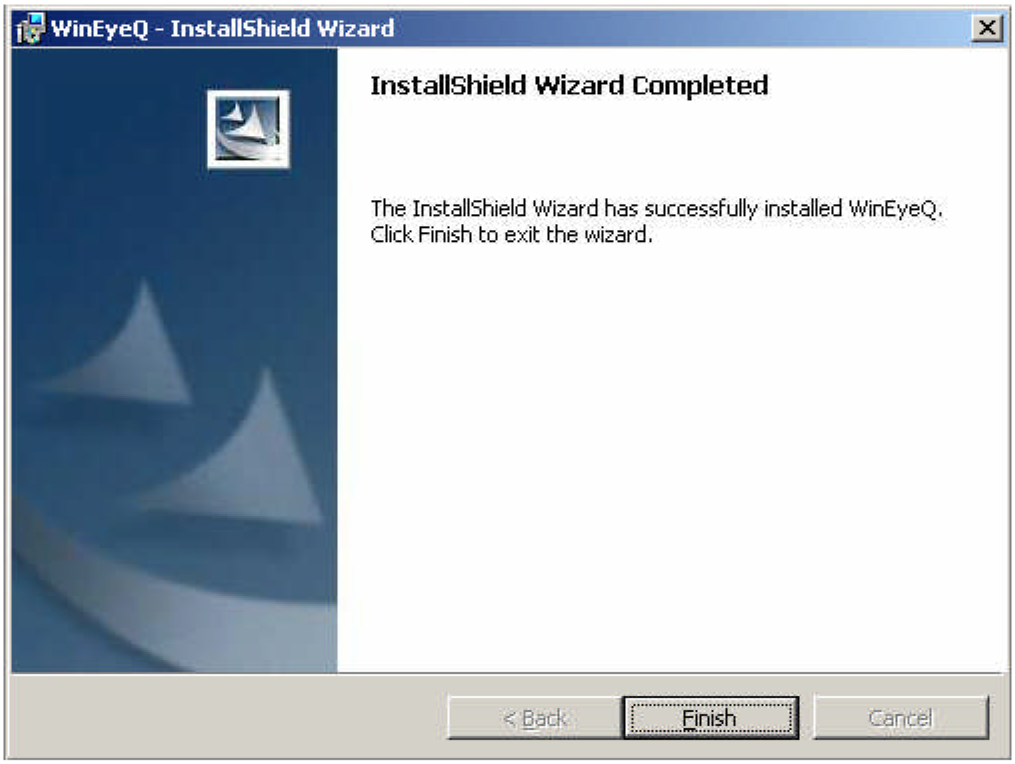
This screen will appear during the installation to inform you of the progress. Typically this screen will only appear for a very brief period of time.



WinEyeQ Install Screen 10 - Installation Complete

This screen will appear at the completion of the installation process. Any errors that may have occurred will be reported at this time. Should you encounter any errors, please contact Touchstone for technical assistance at +215.672.6550 or support@touchstone-inc.com.

Press the "Finish" button to complete the installation.

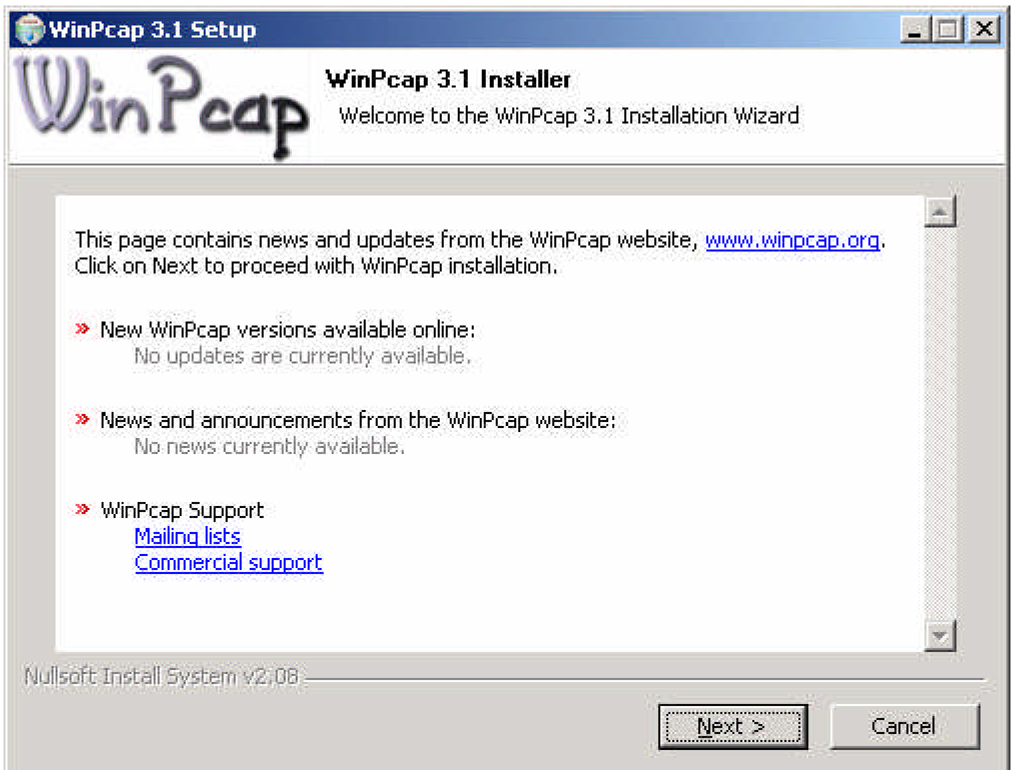


WinPcap Installation

Before the installation is complete, it is necessary to install the WinPcap driver. If you have installed other products that use this driver (such as Ethereal), you will probably need to restart the computer after installation. The following screens will appear during the WinPcap installation process. Please follow the directions carefully using the "Next" button to navigate forward and the "Back" button to return to a previous page.

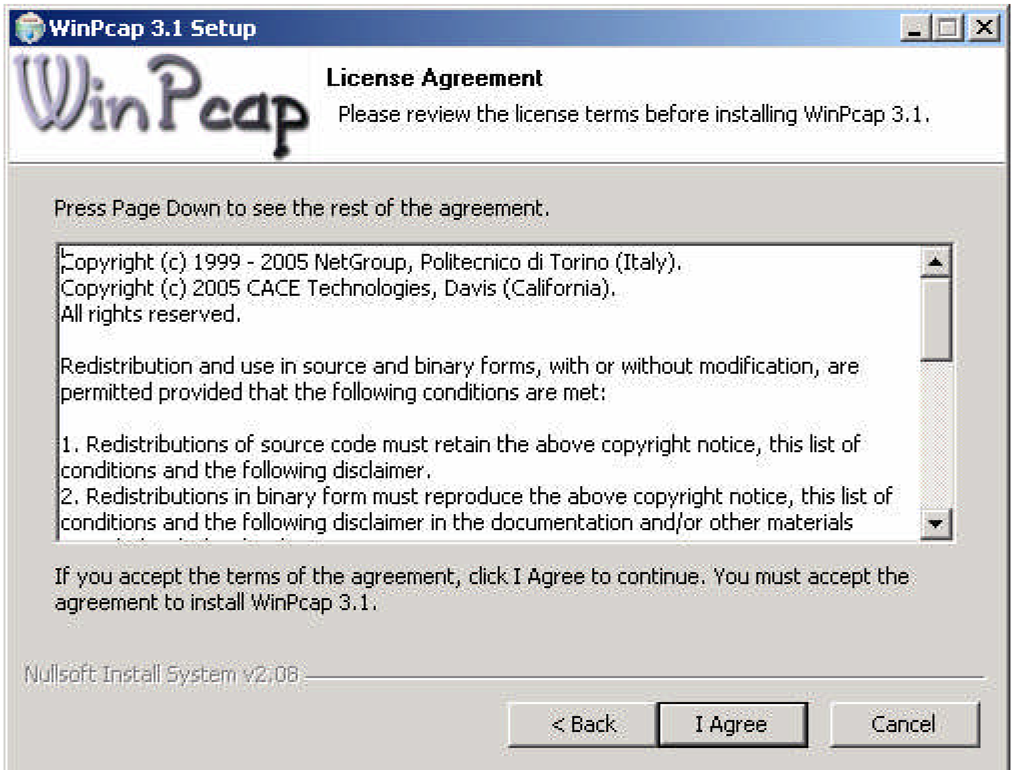
WinPCap Install Screen 1 - Welcome to the installation Wizard

Press the "Next" button to continue or the "Cancel" to quit the installation.



WinPcap Install Screen 2 - End-User License Agreement

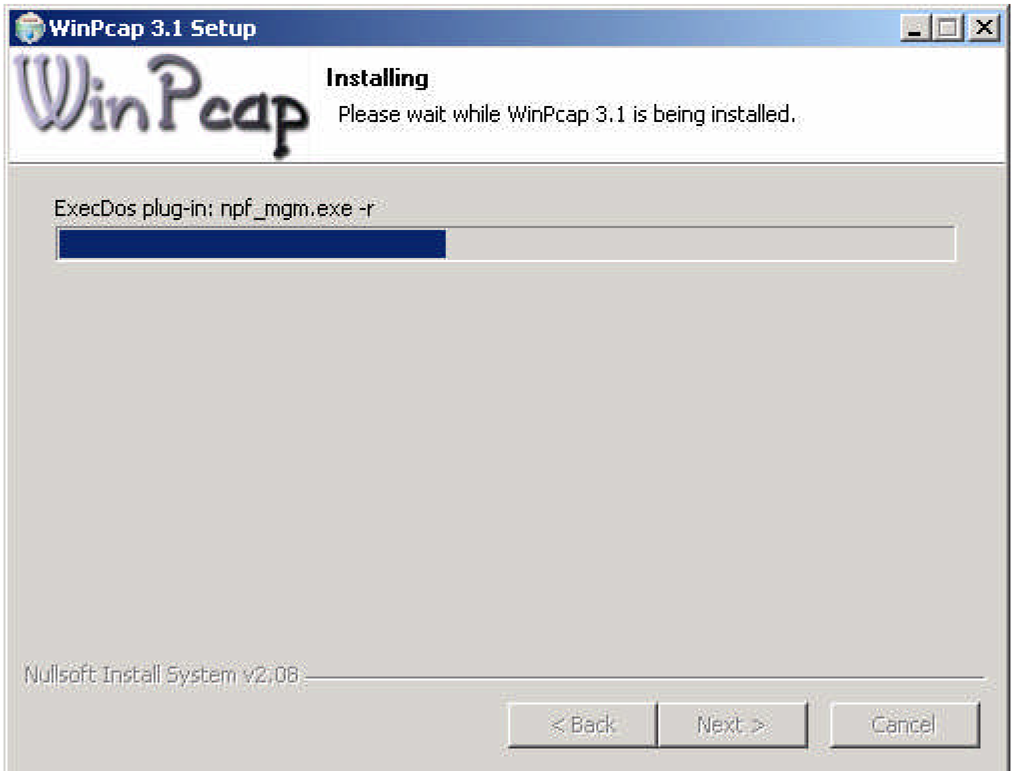
Carefully read the License Agreement. If you accept the terms, press the "I Agree" button, if you do not, press the "Cancel" button.



Press the "Next" button to continue the installation or "Cancel" to quit.

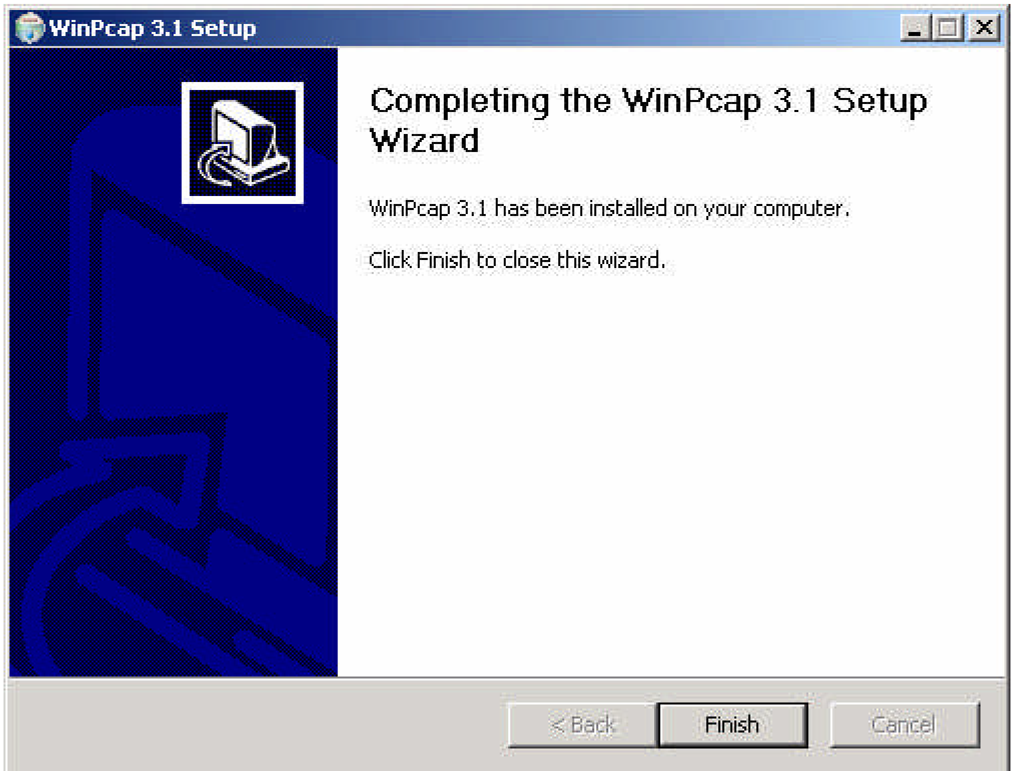
WinPcap Install Screen 3 - Installation Progress

This screen will appear during the installation process.



WinPcap Install Screen 4 - Installation Complete

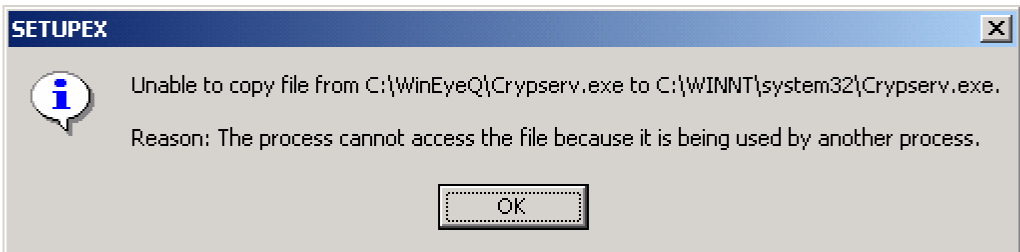
The following screen will appear at the completion of the WinPcap installation.



Installation Notes

The installation process will create a shortcut on your Windows desktop for the WinEyeQ application. The "Start" menu's "Programs" section will also contain an entry for WinEyeQ. You may use either of these to run your WinEyeQ application.

If there are other applications from Touchstone Technologies installed on your PC, a message similar to the one below may appear at the conclusion of the installation.



You can safely ignore this message.

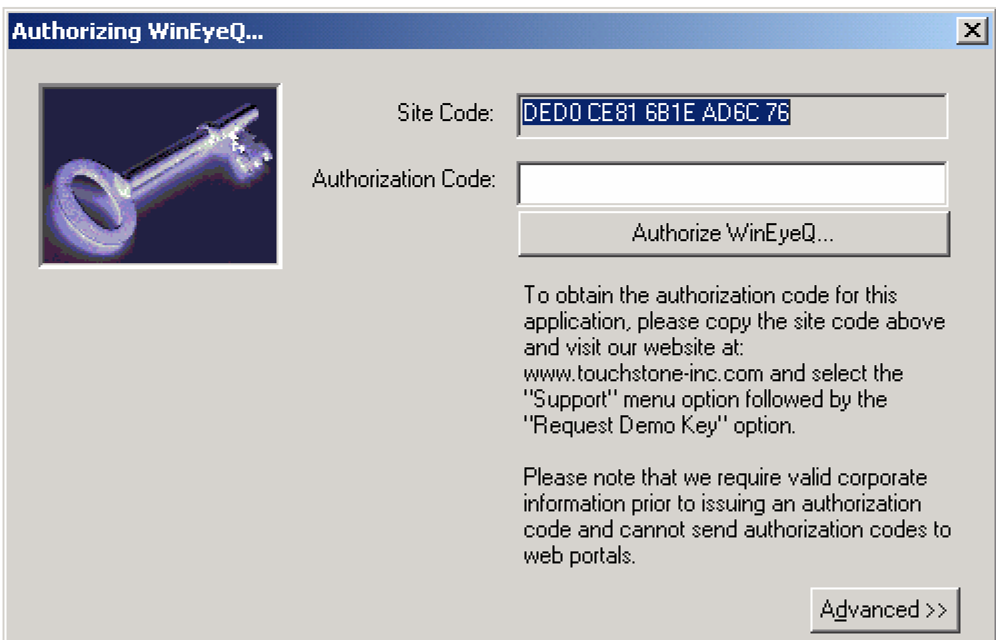
Running WinEyeQ for the First Time

WinEyeQ software is copy protected and is licensed for use on a single machine. The first time you run WinEyeQ, you will be provided with a site code. You must contact Touchstone in order to obtain the authorization code to enable the software.

Once the software is authorized, it may not be installed on any other machines without a new authorization code from Touchstone. If you have installed the software on a machine in error, do not authorize that installation. Re-install it on the appropriate machine prior to contacting Touchstone for the authorization code.

Obtaining the WinEyeQ Authorization Code

When you first run WinEyeQ the following authorization dialog will appear:



In the field labeled "Site Code" a series of numbers and letters will appear. To authorize the application, contact Touchstone with the **exact** value of the site code field. Touchstone will provide the code to enter in the "Authorization Code" field. You must enter this **exactly** as it is provided to you in order to enable the software. It is strongly suggested that you 'copy' the site code into an email that you send to Touchstone, and then 'paste' the authorization code from the email you receive from Touchstone. Once you have enabled the software, you are just moments away from being able to construct your first test scenarios!

Transferring a License

The method of transferring a license is the same for all Touchstone Technologies products. For demonstration purposes WinEyeQ will be used to explain the license transfer procedure.

At the time of installation there are two options for licensing WinEyeQ. The first is to have a new key issued from Touchstone Technologies, and the second is to transfer a license from an existing WinEyeQ application to the newly installed version of WinEyeQ. Touchstone's software licenses are fully transferable from PC to PC within a customer's physical location. To transfer a license to a different location, please contact Touchstone Technologies at (215) 672-6550.

A floppy diskette or USB memory device is required to transfer a license.

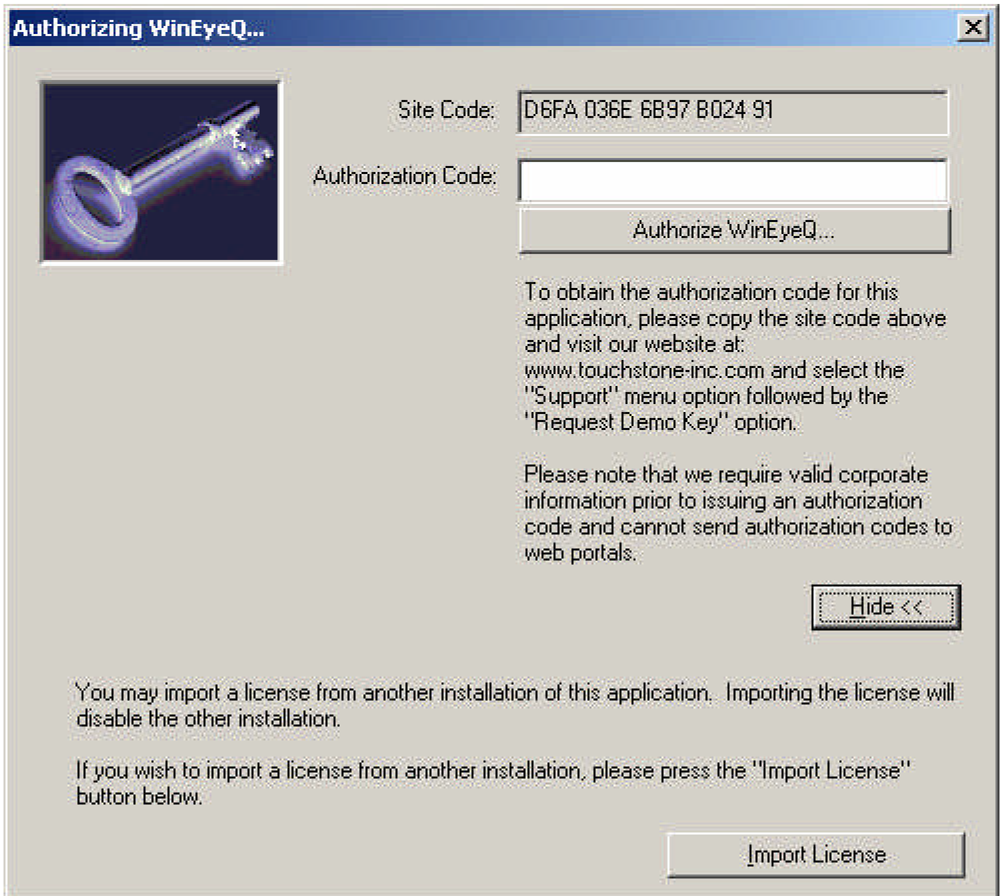
There are three basic steps in transferring a license:

- Initialize transfer media on the PC with newly installed WinEyeQ.
- Export license from the PC with the originally installed WinEyeQ.
- Import license to the PC with newly installed WinEyeQ.

Note: Touchstone Technologies licenses will have to be re-issued if:

- The original installation directory of WinEyeQ is:
    - Copied or moved to a new directory on the original PC.
    - Copied or moved to a different PC.
    - Renamed
- One of the hidden files (deltapts.ckn or deltapts.inf) is deleted or modified.
- The license service (crypserv.exe) is stopped or uninstalled.

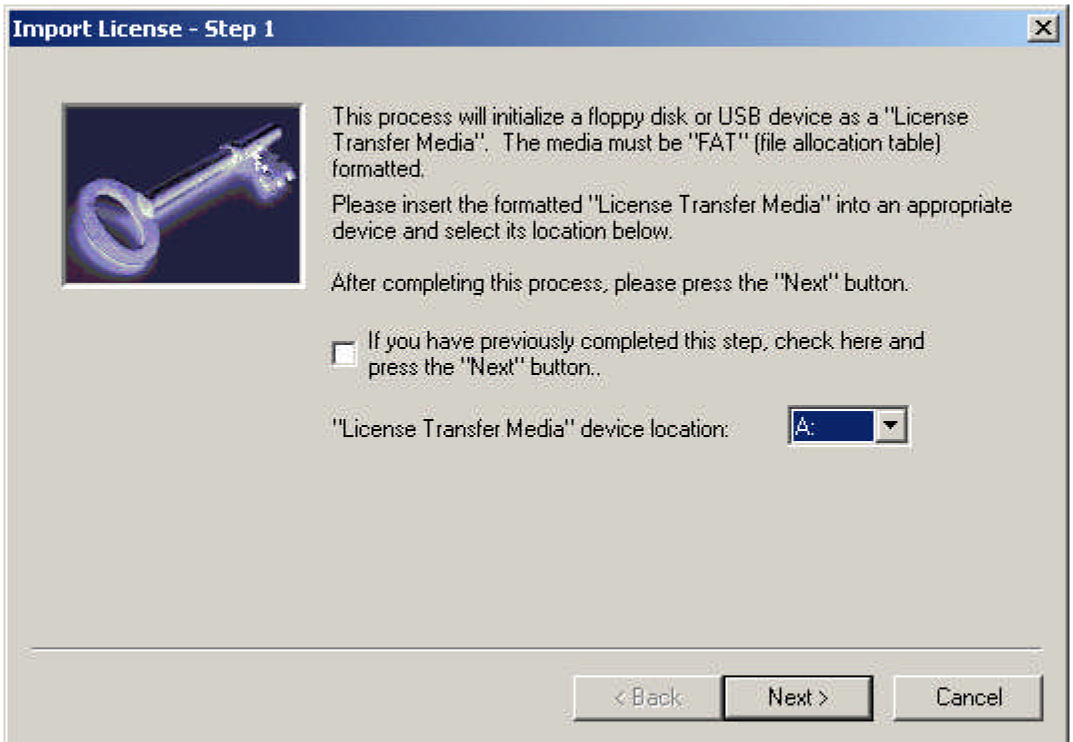
After a new installation is finished and the application is run for the first time, an 'Authorizing WinEyeQ' screen will appear. By clicking on the 'Advanced' button, an expanded dialog will be displayed:



Press the 'Import License' button to begin the license transfer procedure.

Step One - Import License, Media Initialization

The first step of the 'Import License' transfer requires initialization of a diskette or USB device that will be used as the 'License Transfer Media'.

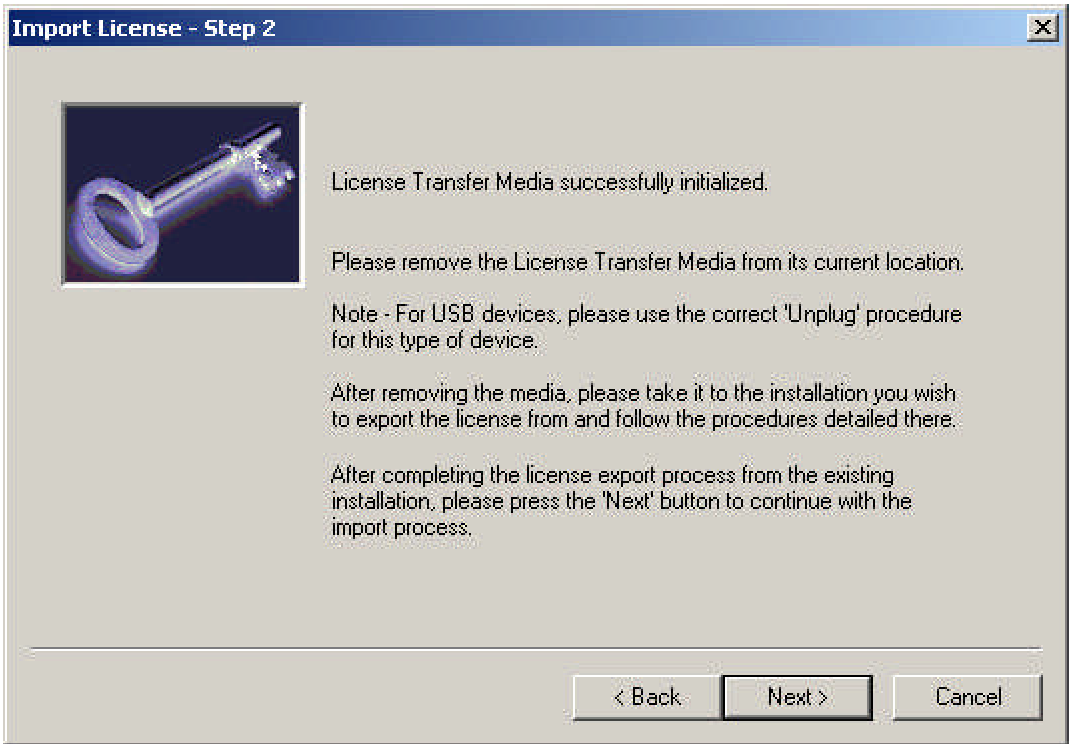


To initialize the transfer media, select the drive to be used as the transfer device, insert the transfer media and press the 'Next' button.

Note: If you have completed this step from a previous execution of WinEyeQ and already have the initialized transfer media, click the checkbox and then press the 'Next' button.

When step one is complete, the transfer media is initialized.

The 'Import License - Step 2' dialog will then appear:



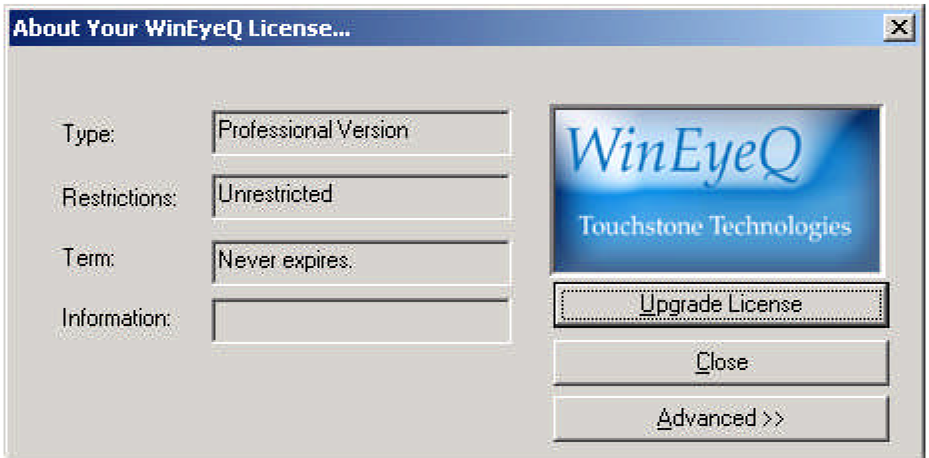
The next step is to eject or unplug the transfer media and take it to the PC that has the license you want to remove.

Note: For USB devices please follow the correct unplug procedure for your device.

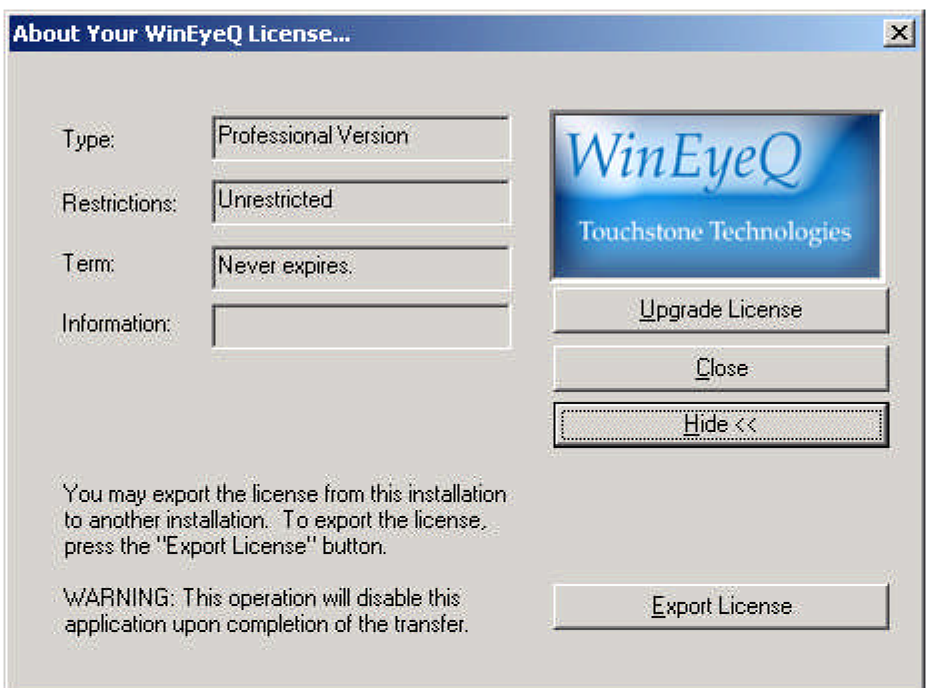
Step Two - Export License

On the PC that you have selected to remove the WinEyeQ license, click on the 'Help' menu and then select 'Licensing Information'.

The Following dialog will appear:



Next click on the 'Advanced' button to expand the dialog:



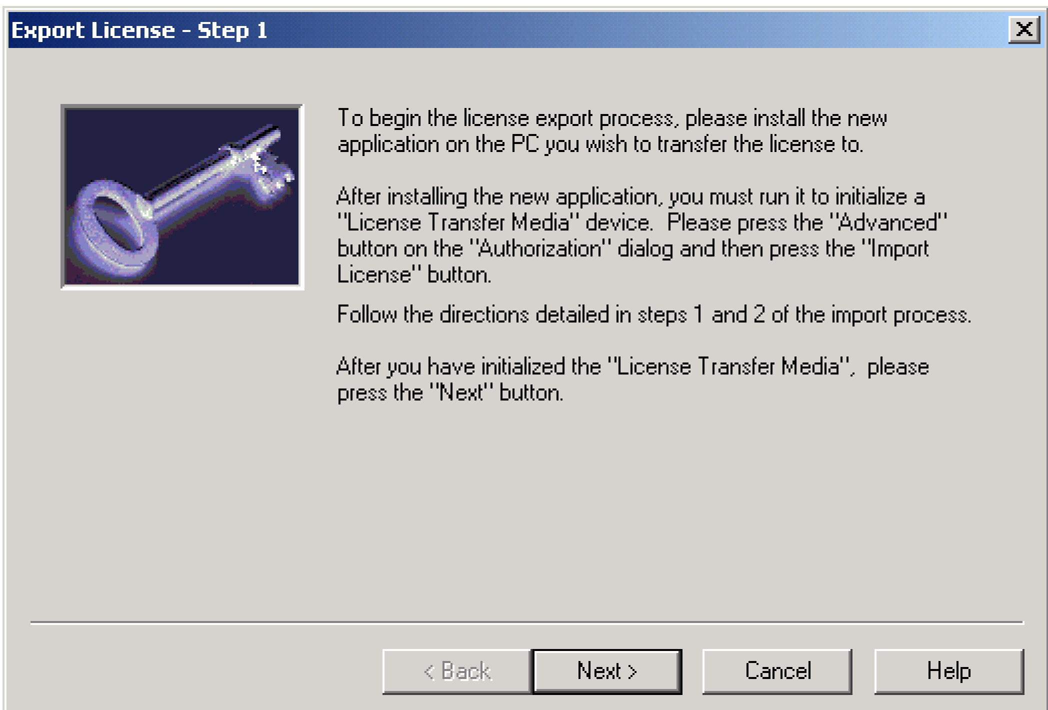
Now click on the 'Export License' button.

A warning dialog will be displayed next. It instructs you to read the procedure carefully and that the version of WinEyeQ currently running will be disabled after the procedure is completed.

If you are certain you want to transfer this license, press 'Yes,' if not, press 'No'.

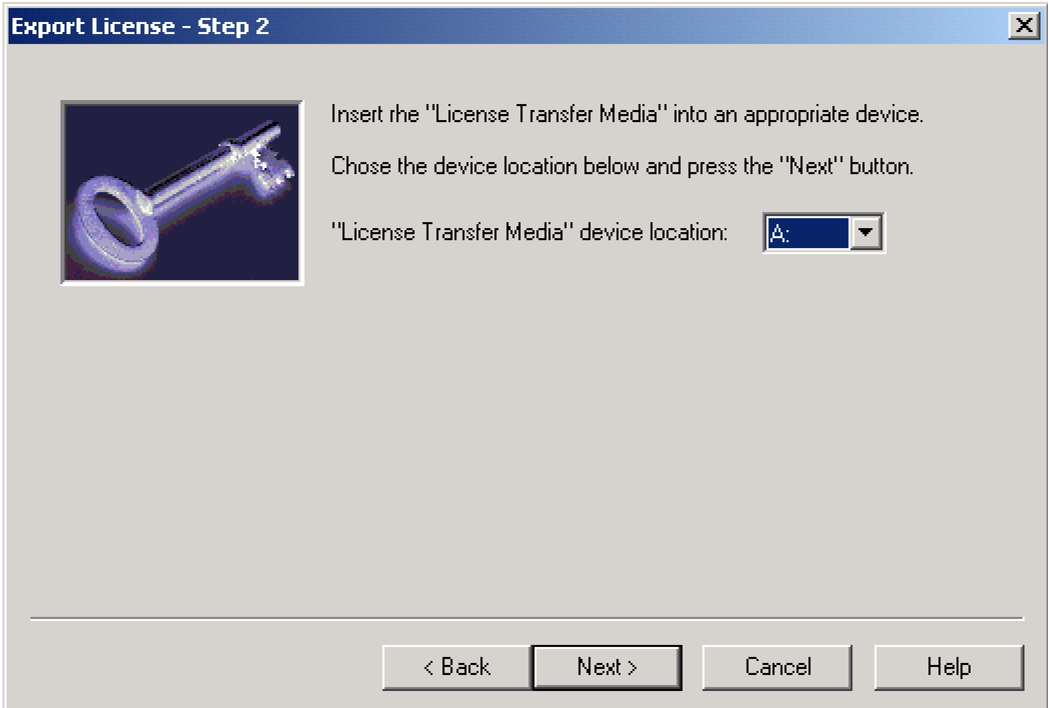
The existing WinEyeQ application will not be uninstalled nor will any WinEyeQ files be removed from the WinEyeQ directory, the software will simply be disabled. Later if you wish, you can re-enable the application with a new license from Touchstone or with a WinEyeQ license transferred from another PC.

Step one of the export procedure displays the following dialog:



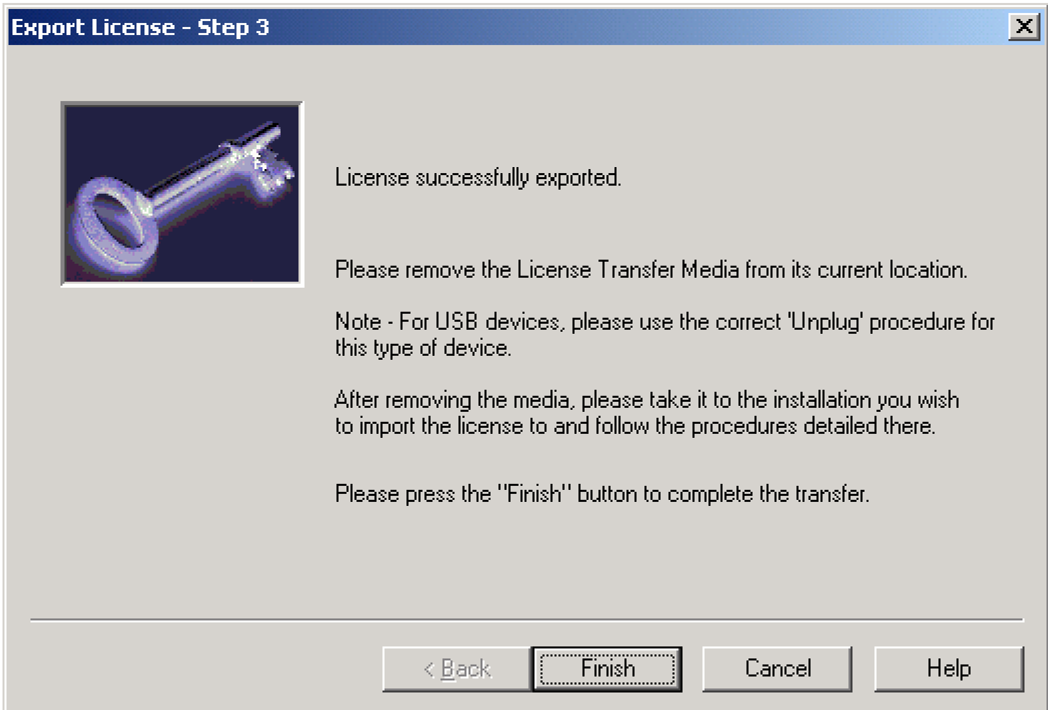
Click the 'Next' button.

Step two of the license export procedure displays the following dialog:



Insert the transfer media that was initialized from 'Step One – Media Initialization,' select the drive to be used as the transfer device and press the 'Next' button.

When the license has been successfully exported, the following dialog will appear:



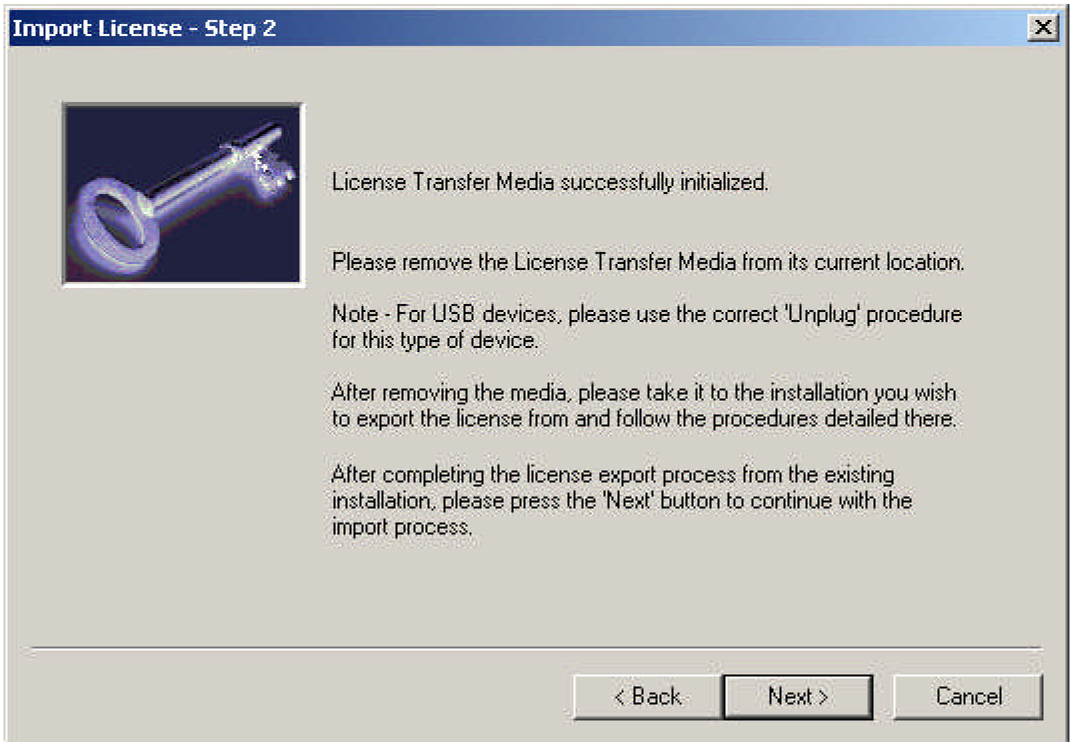
When the 'Finish' button is pressed, the application will terminate. This completes the license export.

Remove and take the 'License Transfer Media' to the newly installed WinEyeQ.

Note: For USB devices please follow the correct unplug procedure for your device.

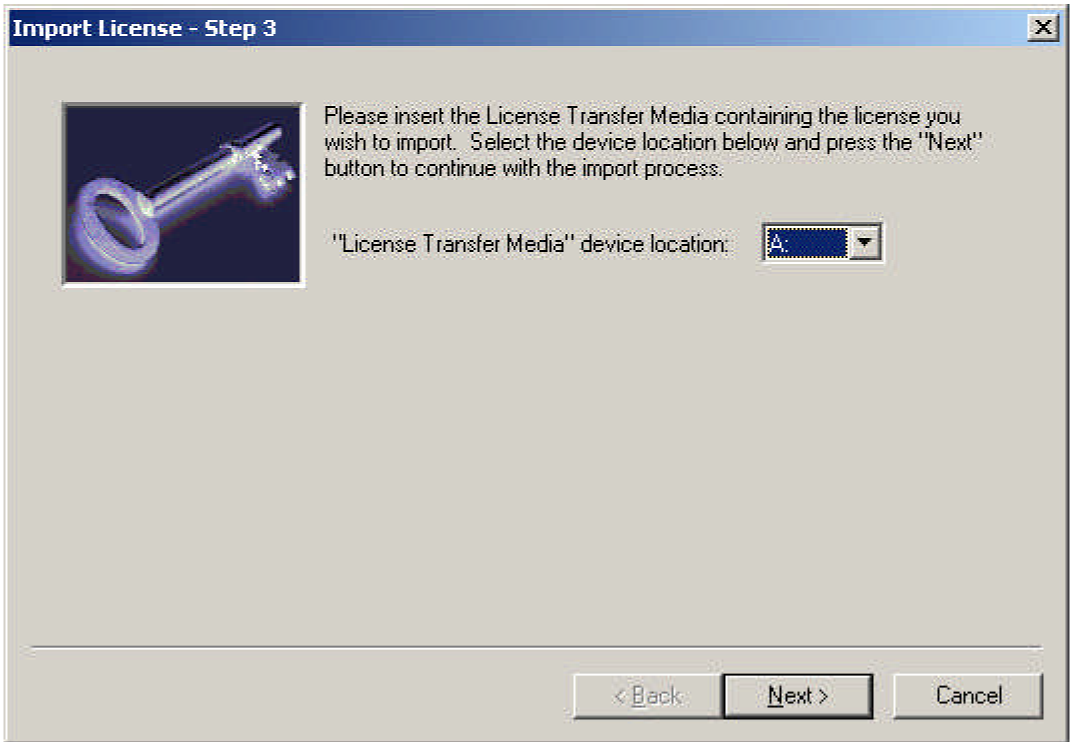
Step Three - Install Exported License

The PC with the newly installed version of WinEyeQ should still have the following screen displayed, 'Import License – Step 2':



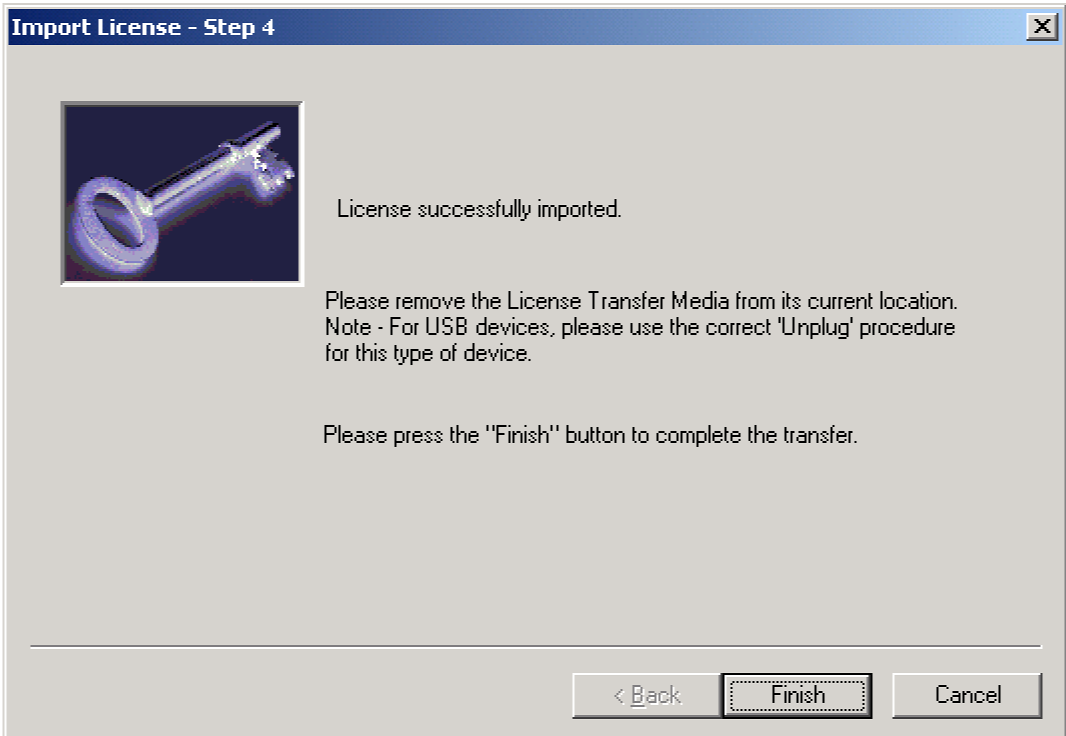
After the export procedure is complete, and you have the license on the transfer media, insert or plug in the media and then press the 'Next' button.

Select the proper 'License Transfer Media':



Press the 'Next' button when done.

When the license has been successfully imported, the following dialog will appear:



The newly installed WinEyeQ is now fully enabled and ready to run when you press the 'Finish' button.

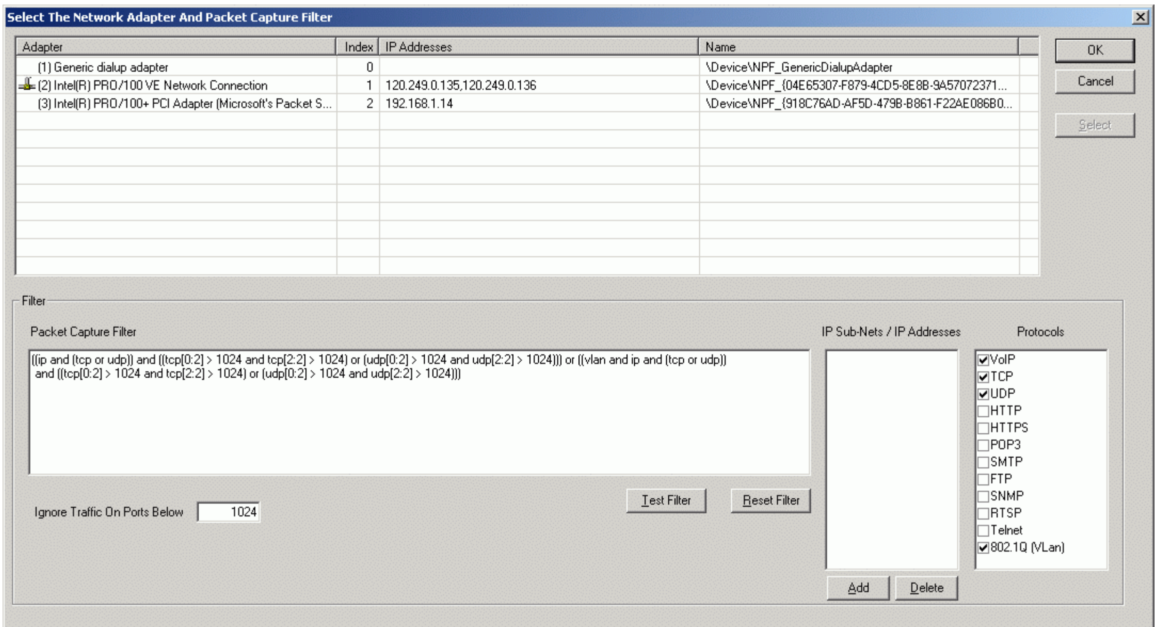
License Transfer Instruction Chart

Action	New Installation	Existing Installation
1.Install New Software	Select the machine on which you would like to install the new instance of the product and follow the installation instructions. Once installed, run the application and the licensing dialog will appear.	
2. Initialize License Transfer Media	When the new installation asks for the Authorization code, press the 'Advanced' button then, press the 'Import License' button. This will bring up a dialog that asks you to initialize a 'License Transfer Media Device'. This device may be a diskette or USB device. Enter the letter of the drive where the transfer media is located and press the 'Next' button. Once you have pressed the 'Next' button, you may remove the License Transfer Device. You must then take that diskette or USB device to the PC that has the license you want to export.	

Action	New Installation	Existing Installation
3. Export License		Run the application on the PC that has the license you want to export, go to the Help menu and press Licensing Information. Press the 'Advanced' button to reveal the advanced options. Once visible, press the 'Export License' button. Follow the step-by-step directions to export the license onto the License Transfer Media Device. Remove the License Transfer Media Device. The existing installation is now deactivated. Return to the new installation.
4. Import License	Insert your License Transfer Device into the appropriate device. Follow the instructions to import the license. The new installation is now activated.	

Selecting the Network Adapter

One of the first steps in preparing to run WinEyeQ is to select the network adapter you wish to monitor. WinEyeQ will automatically display the Select Adapter screen immediately after starting it for the first time. You may also access this dialog from the Edit | Select Adapter menu item.



On the top part of the screen is a list of the Network Adapters that WinEyeQ has discovered on your PC. Select the adapter you want to monitor by clicking the adapter line and then pressing 'Select' or by just double clicking the adapter line.

This window will be discussed in great detail later in the manual.

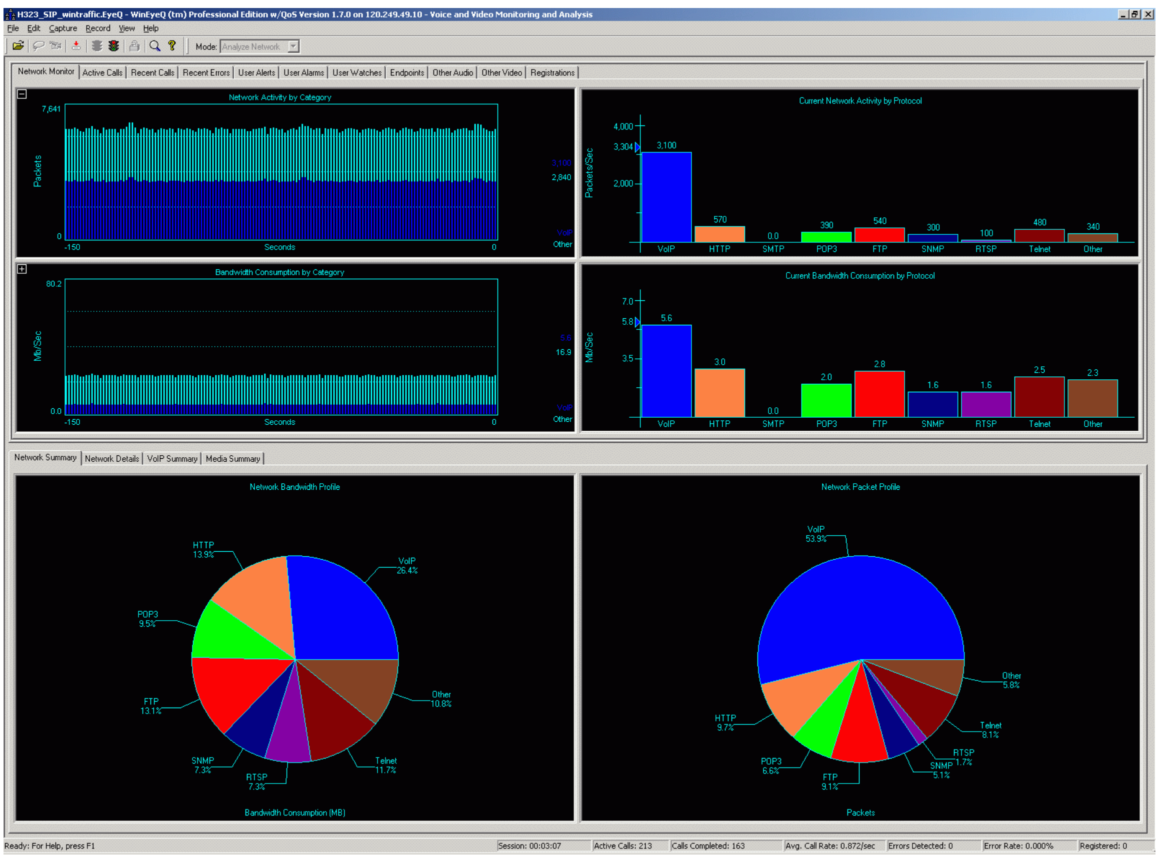
WinEyeQ User Interface

WinEyeQ was designed to facilitate diagnostics by representing the network in a natural, intuitive, top-down manner. This presentation allows users to "drill-down" into areas of interest at the same time bypassing information that is neither relevant nor interesting at the moment.

Data Scopes™

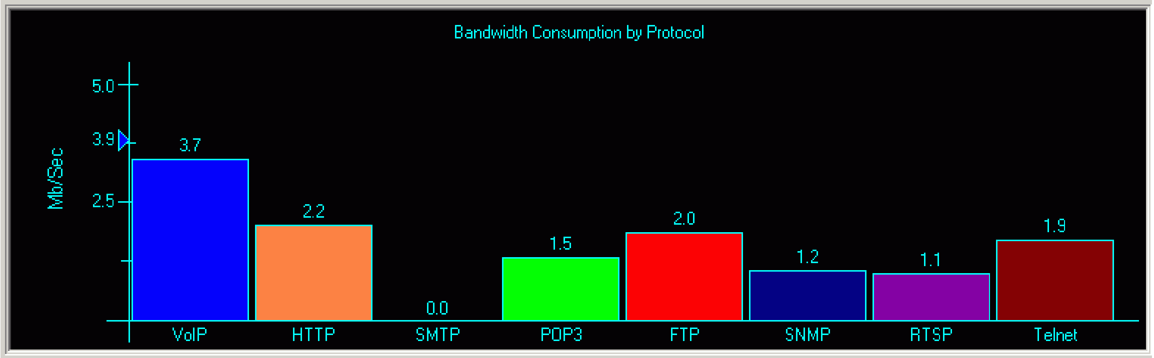
Version 1.5.0 of WinEyeQ implemented a new series of graphical representations of both the Voice and Video over IP and non-VoIP components of your network. The "Data Scope" metaphor reinforces WinEyeQ's drill-down user-interface approach. Each Data Scope™ is represented at its topmost level by a view of logically grouped components (e.g. network protocols) in a view that can be toggled between a pie chart and a bar chart. Each of these components has at least one level of depth beyond the first, which minimally would be a historical representation of the values of the component over time, which we refer to as a "histogram". At its most complex, the topmost Data Scope™ will be the highest representation of a series of cascading views which each end at a histogram. The following gives you an overview of the typical mechanism of a Data Scope™ for isolating the G.723 bandwidth utilization on a live VoIP network.

Network Monitor View



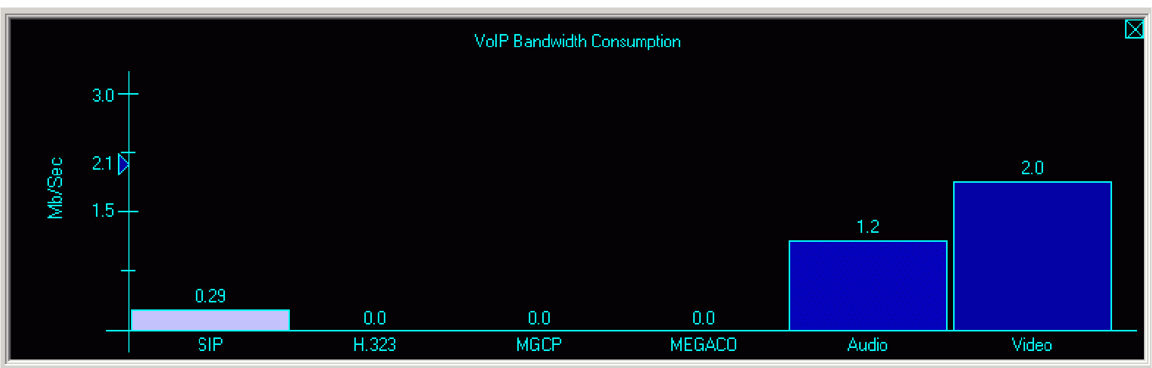
If we zero in on the Network Bandwidth Data Scope™ (found in the bottom of the upper right quadrant), we see a Data Scope™ that appears as follows:

Network Bandwidth Consumption; top view



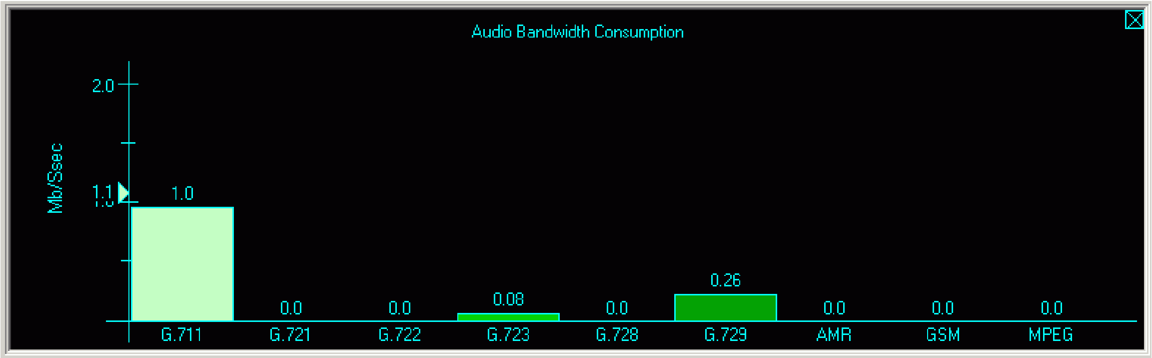
Notice that the components are grouped logically and that this Data Scope™ provides a high-level view of the bandwidth utilization of the various protocols on the network. The leftmost component is the VoIP component. To further explore the bandwidth utilization of the VoIP component, we can drill down by double-clicking on it. This action would yield a view of the VoIP breakdown as:

VoIP Bandwidth Consumption; level 2



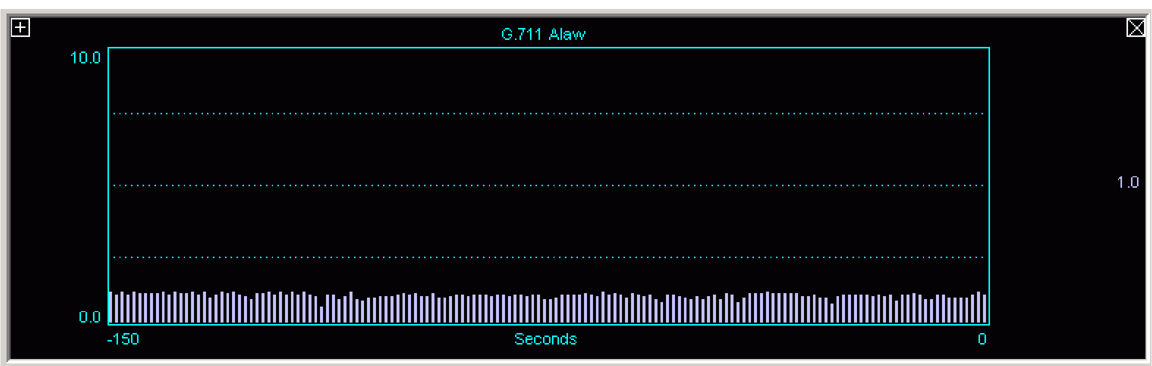
Once again, the components of this sub-level Data Scope™ are grouped logically, representing the top-level view of the bandwidth utilization of the VoIP components. The leftmost component is the SIP component, followed by H.323, Audio, and Video components. To further explore the bandwidth utilization of the Audio component, we can drill down by double-clicking on it. This action would yield a view of the Audio components as:

Audio Bandwidth Consumption; level 3



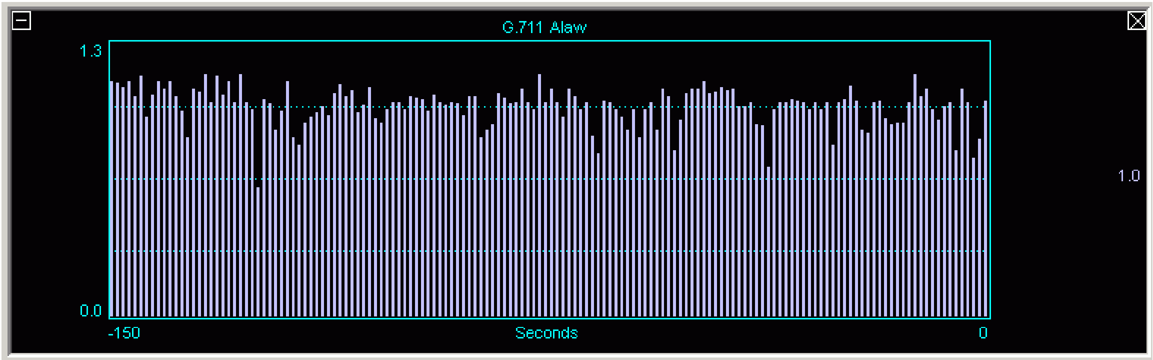
The components of this sub-level Data Scope™ are grouped logically representing the bandwidth utilization of the audio component by codec type. The leftmost component is the G.711 codec, which also has a sub-level Data Scope™ further refining it to the Alaw and Ulaw components. To further explore the bandwidth utilization of the G.723 component, we can drill down by double-clicking on it. This action would yield a view of the G.723 component as:

G.711 Bandwidth Consumption Histogram; level 4

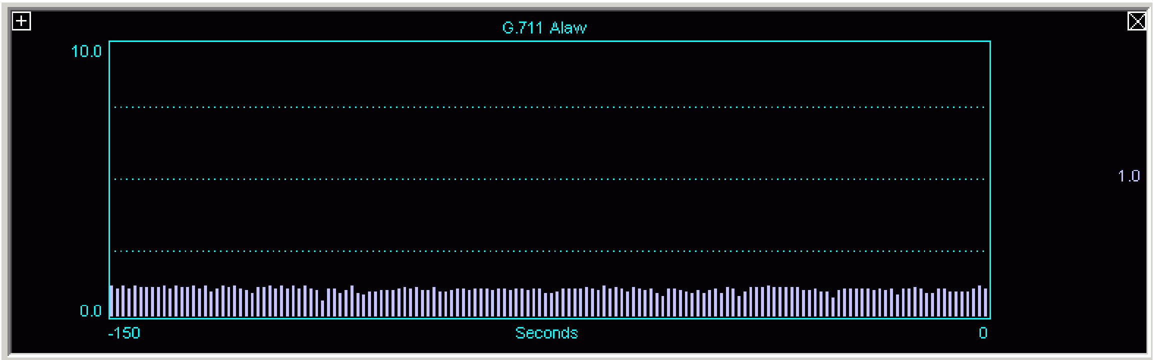


By clicking the "+" sign on the histogram, we can "Zoom In" on the series of values.

G.711 Bandwidth Consumption Histogram; zoomed



By clicking the "-" sign on the histogram, we can "Zoom Out" on the series of values back to:



Once you reach the histogram of a component you are at the end of the journey. You may back out from any sub-level at any time by using the "X" in the upper-right corner. The following section provides the user-interface tips and tricks for using the data scopes:

Data Scopes™ in Bar Graph View provide high-water marks for the component with the highest value on the scope. These marks, indicated by an arrow on the left scale, have the same color as the component that they are associated with. These watermarks are re-calculated every 10 updates of the Data Scope.

Navigational Tips

- Right-click the background area of a Data Scope™ to toggle between Bar Graph View and Pie Chart View.
- Double-click components to drill-down.
- Click the "X" box on a sub-level component to navigate backwards.
- Right-click any component to view its histogram.
- Click the "+" box to zoom-in the scale on a histogram.
- Click the "-" box to zoom-out the scale on a histogram.

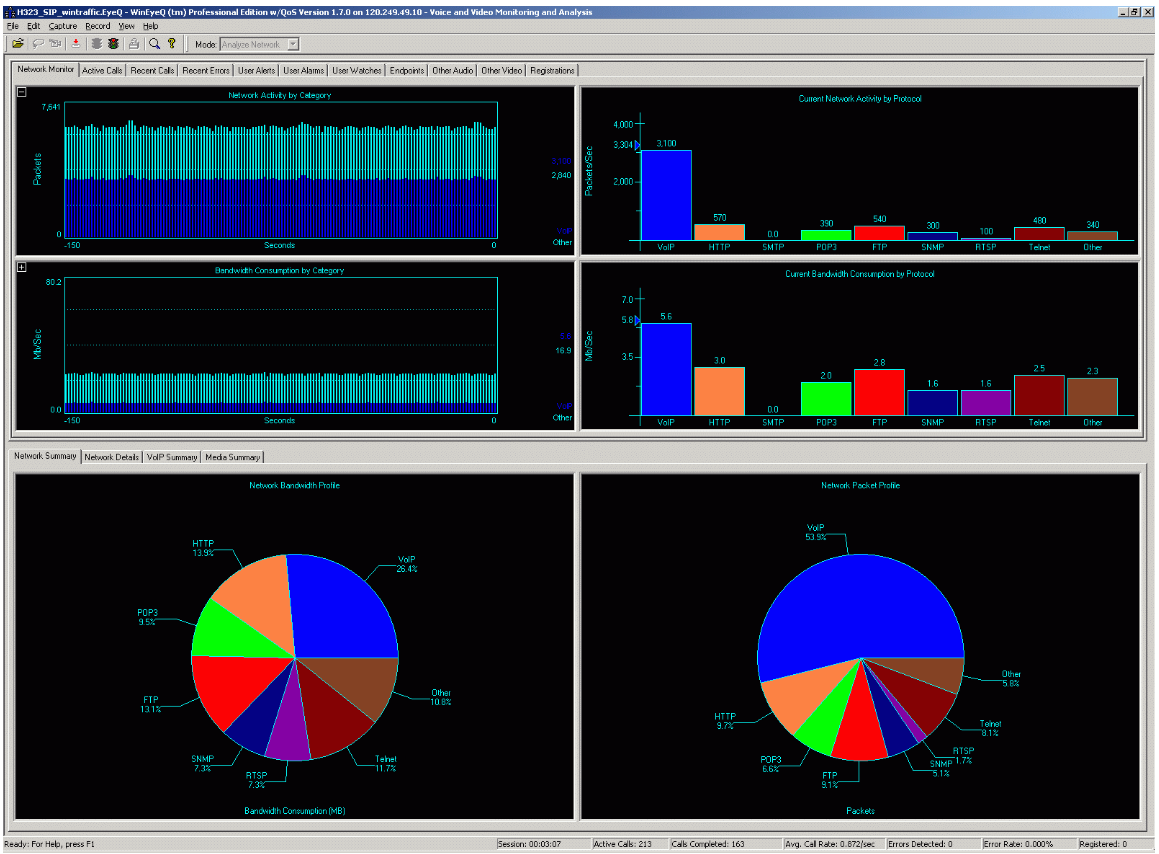
User Interface: Step-By-Step

WinEyeQ's user interface is comprised of eleven (11) major views each containing up to eleven (11) sub-views. The ten major views represent the following categories:

- Network Monitor
- Active Call
- Recent Calls
- Recent Errors
- User Alerts
- User Alarms
- User Watches
- Endpoints
- Other Audio Channels
- Other Video Channels
- Registrations

The Network Monitor View

For the main view (Network Monitor) the Data Scopes™ are paired in Activity/Bandwidth pairs for logical groups of components. For example, Network Protocol Activity and Network Bandwidth Consumption by Protocol are paired together.

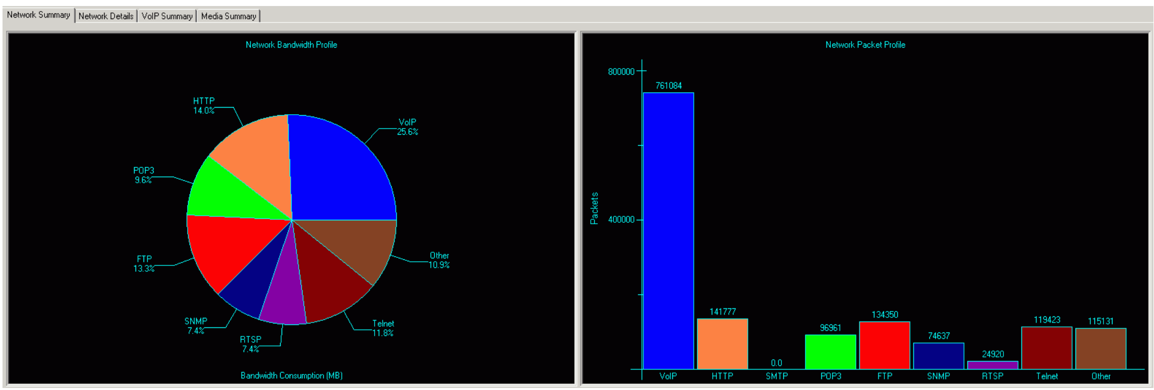


The Network Monitor View is designed to provide an overall picture of VoIP and Non-VoIP network traffic and resource utilization both instantaneously (top half) and historically (bottom half). You may elect to "drill into" any of the component elements as demonstrated earlier. The network monitor view has the following sub-views:

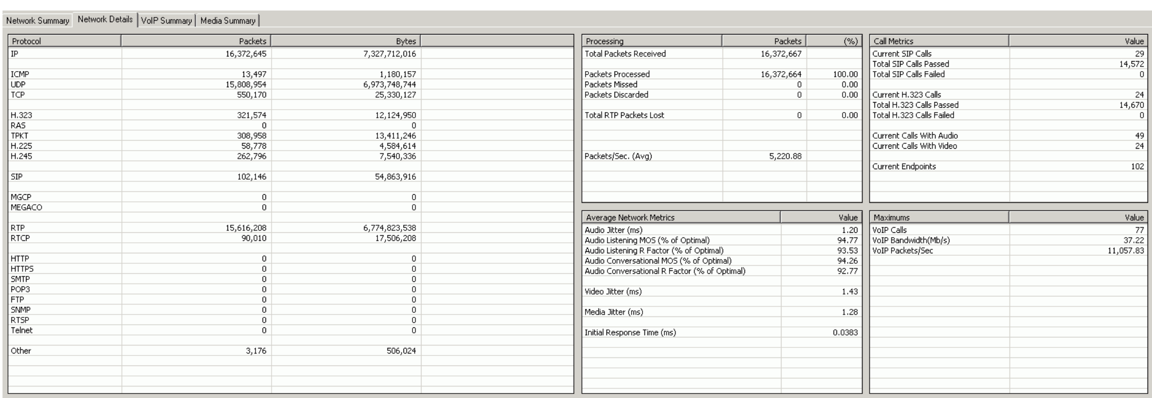
- Network Summary
- Network Details
- VoIP Summary
- Media Summary

Network Summary

This view presents the high-level Data Scopes™. The graphs represent the Network Bandwidth and Packet Profiles by component over the duration of the session. In this example, the Network Packet Profile Data Scope™ is in Bar Chart Mode while the Network Bandwidth Summary is in Pie Chart Mode. These modes can be toggled back and forth by right clicking on the background of the Data Scope™.



Network Details



This view provides a numerical summary of the packets and byte counts analyzed by layer. The layers include:

- IP, ICMP, UDP, TCP
- H.323, RAS, TPKT, H.225, H.245
- SIP
- MGCP, MEGACO
- RTP, RTCP
- HTTP, HTTPS, SMTP, POP3, FTP, SNMP, RTSP, Telnet, Other

Additional network metrics include:

<u>Processing</u>:

<u>Total Packets Received</u>: The total number of packets that WinEyeQ has received from the WinPcap driver.
<u>Packets Processed</u>: The number of packets that WinEyeQ has processed and analyzed.
<u>Packets Missed</u>: The number of packets that the WinPcap driver has been unable to send to WinEyeQ.
<u>Packets Discarded</u>: The number of packets that WinEyeQ has discarded due to packet overload.
<u>Total RTP Packet Lost</u>: The total number of RTP packets that were expected minus the total number actually received.
<u>Packets per Second (Average)</u>: The average number of packets per second that WinEyeQ has processed since the analyzer was started.

<u>Call Metrics</u>:

Current SIP Calls
Total SIP Calls Passed
Total SIP Calls Failed
Current H.323 Calls
Total H.323 Calls Passed
Total H.323 Calls Failed
Current Calls with Audio
Current Calls with Video
Current Endpoints

<u>Average Network Metrics</u>:

<u>Audio Jitter (ms)</u>: The average jitter (as calculated from RFC 3550) for all audio streams of all completed calls.
<u>Audio Listening MOS (% of Optimal)</u>: The average Listening MOS score attained for all audio streams of all completed calls. See below.
<u>Audio Listening R Factor (% of Optimal)</u>: The average Listening R factor attained for all audio streams of all completed calls. See below.
<u>Audio Conversational MOS (% of Optimal)</u>: The average Conversational MOS score attained for all audio streams of all completed calls. See below.
<u>Audio Conversational R Factor (% of Optimal)</u>: The average Conversational R factor attained for all audio streams of all completed calls. See below.
<u>Video Jitter (ms)</u>: The average jitter (as calculated from RFC 3550) for all video streams of all completed calls.

Media Jitter (ms): The combined average of the audio and video jitter values.
Initial Response Time (ms): The average time it took for the called endpoint to return its first response to the calling endpoint.

Maximums:

VoIP Calls: The maximum number of concurrent calls that WinEyeQ has analyzed.
VoIP Bandwidth (Mb/s): The highest VoIP bandwidth analyzed.
VoIP Packets / Sec: The highest number of VoIP packets per second analyzed.
Packets/Second: The highest number of packets per second analyzed.

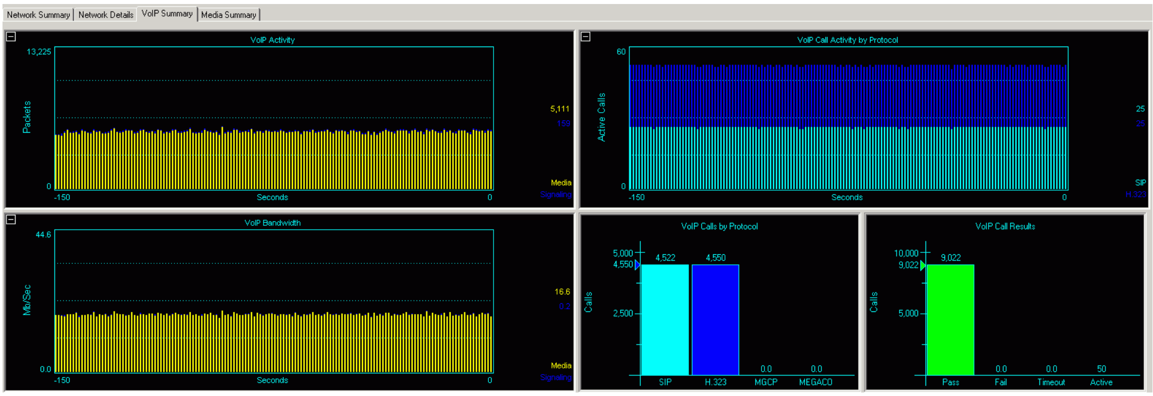
Optimal MOS Scores and R Factors.

Different codec types have different highest attainable Listening and Conversational MOS scores and R factors. WinEyeQ computes the normalized average network MOS scores and R factors by taking the MOS scores and R factors calculated for the audio media stream and dividing them by their theoretical maximum values. For example, if a G.728 audio stream received a Listening MOS score of 3.5, the normalized value would be 86.6 %. If a G.723.1 5.3 kb audio stream received a Listening MOS score of 3.5, the normalized value would be 96.9 %.

Note: Please see Appendix A for a chart of theoretical maximum MOS scores and R factors.

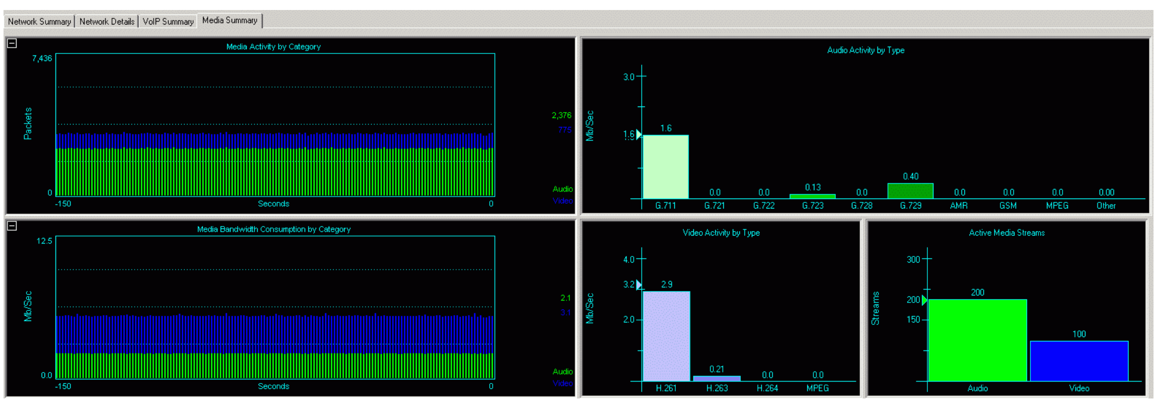
VoIP Summary

The VoIP Summary paints a picture of the packet and bandwidth activity of the VoIP signaling and media components as well as detailing call activity by protocol, call distribution by protocol, and call status history.

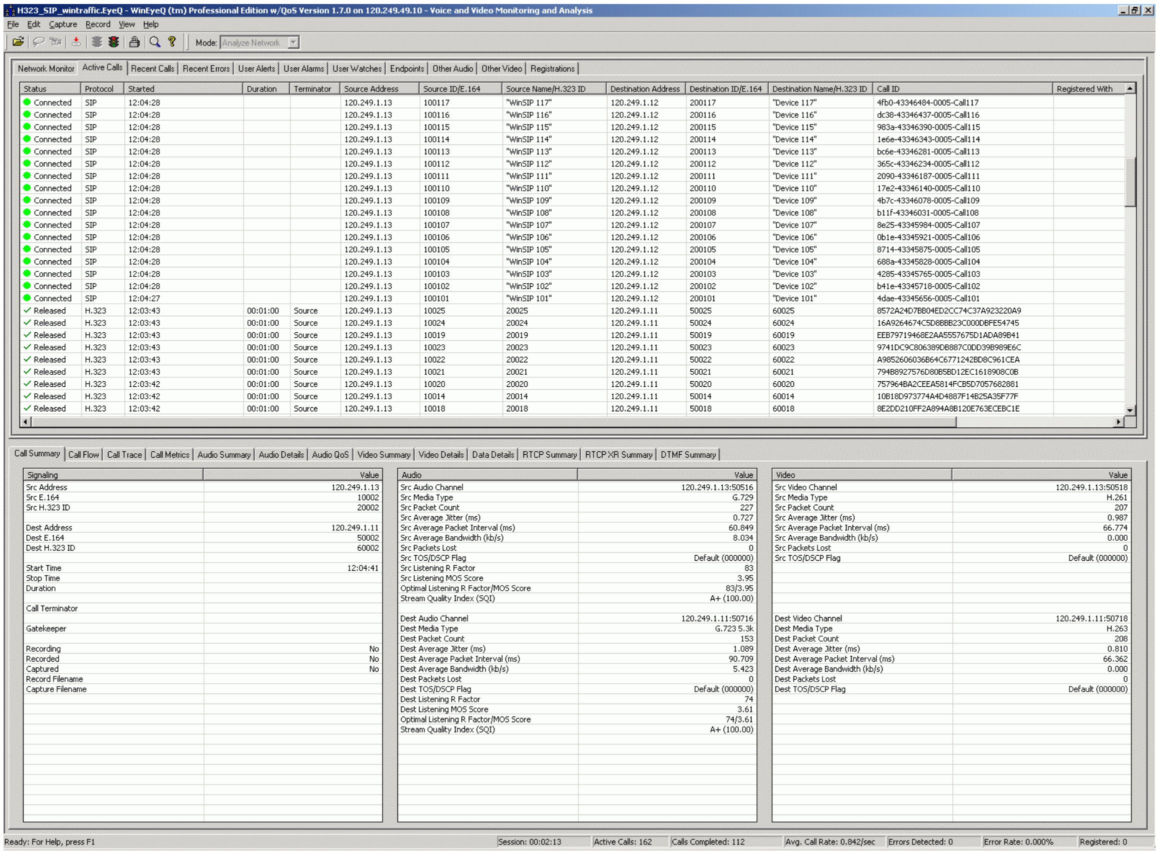


Media Summary

The Media Summary shows the bandwidth consumption and activity of the media components of the VoIP activity on your network. The bandwidth and packet activity are broken down by audio and video components. The right half of the screen breaks audio and video down by codec type as well as summarizing the active audio and video streams on the network.



Active Calls View



The active calls view is designed to provide an in-depth view of each VoIP call and its status. Each call is represented by an entry in the topmost report; the entries are updated once every second. This view contains the following columns:

<u>Call Status</u>: The current status of the call. These may be things such as connecting, ringing, connected, error, etc.

<u>Protocol</u>: The values for this field are SIP or H.323.

<u>Started</u>: This is the time (local time) that the call was started.

<u>Duration</u>: The length of time the call is (or was) active.

<u>Terminator</u>: Which side of the call (Source or Destination) terminated the call.

<u>Source Address</u>: The address of the call initiator (caller).

Source ID/E.164: The SIP user ID or H.323 E.164 alias of the caller.

Source Name/H.323 ID: The SIP display name or H.323 ID of the caller.

Destination Address: The address of the call receiver (party called).

Destination ID/E.164: The SIP user ID or H.323 E.164 alias of the party called.

Destination Name/H.323 ID: The SIP display name or H.323 ID of the party called.

Call ID: The SIP or H.323 call ID associated with this call.

Registered With: The gatekeeper's IP address for H.323 calls, or the Proxy's IP address for SIP calls.

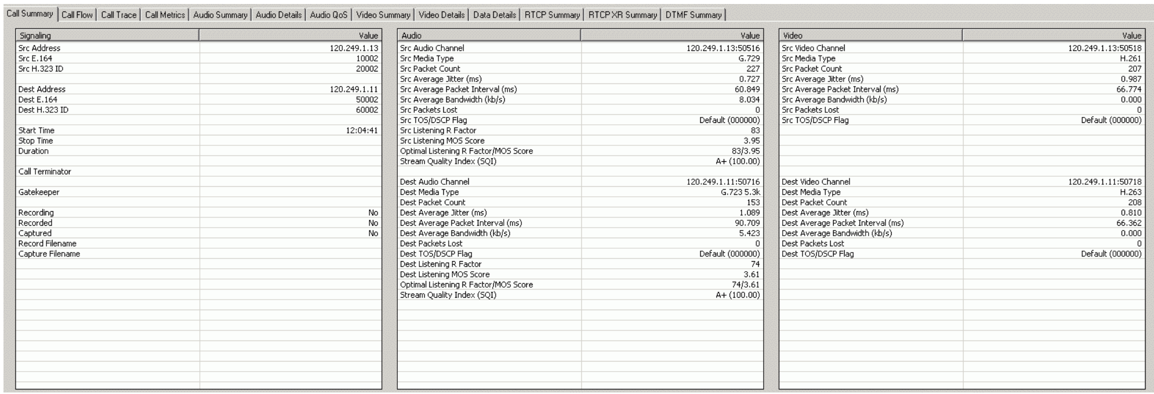
Conference ID: The conference ID (H.323 calls only).

Each individual call has the following sub-views.

- Call Summary
- Call Flow (ladder diagram)
- Call Trace
- Call Metrics
- Audio Summary
- Audio Details
- Audio QoS
- Video Summary
- Video Details
- Data Details
- RTCP Summary
- RTCP XR Summary
- DTMF Summary

Note: To display information about a particular call, select it (click the call line) in the call list. Whenever a call is selected, it will remain "locked" in the view for as long as you wish to view its details.

Call Summary



This sub-view provides a summary of the call elements including source and destination addresses for signaling and media. There are three panes on this sub-view.

Signaling Pane

Source Address: The IP address of the calling endpoint.
Source ID/Source E.164: The source ID (SIP) or E.164 (H.323) of the calling endpoint.
Source Name/Source H.323 ID: The source name (SIP) or H.323 ID (H.323) of the calling endpoint.
Destination Address: The IP address of the called endpoint.
Destination ID/E.164: The source ID (SIP) or E.164 (H.323) of the called endpoint.
Destination Name/H.323 ID: The source name (SIP) or H.323 ID (H.323) of the called endpoint.
Start Time: The time the first packet was seen on the network.
Stop Time: The time the last packet was seen on the network.
Duration: The difference between the start and stop time.
Call Terminator: The endpoint that terminated the call.
Proxy/Gatekeeper: The address of the proxy (SIP) or gatekeeper (H.323) that participated in the call.
Recording: Whether or not the call is presently being recorded.
Recorded: Whether or not the call was recorded.
Captured: Whether or not the call was captured.
Record Filename: The file name of the record file.
Capture Filename: The file name of the capture file.

Audio Pane

Source Audio Channel: The IP address and port of the calling endpoint.
Source Media Type: The type of codec being used to send the audio.
Source Packet Count: The number of packets sent on this channel.
Source Average Jitter (ms): The average jitter value (as calculated from RFC 3550) for this channel.
Source Average Packet Interval (ms): The average inter-arrival time of packets on this channel.
Source Average Bandwidth (kb/s): The average bandwidth, in kilobits per second, calculated for this channel.
Source Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received.
Source TOS/DSCP Flag: The value of the Type of Service (TOS) / Differentiated Services Code Point (DSCP) flag in the IP header field.
Source Listening R Factor: The current Listening R factor for this media stream.
Source Listening MOS Score: The current Listening MOS Score for this media stream.
Optimal Listening R Factor / MOS Score: The highest scores that are attainable for this codec.
Stream Quality Index: The ratio of the current R Factor and MOS score to there optimal values.

Destination Audio Channel: The IP address and port of the called endpoint.
Destination Media Type: The type of codec being used to send the audio.
Destination Packet Count: The number of packets sent on this channel.
Destination Average Jitter (ms): The average jitter value (as calculated from RFC 3550) for this channel.
Destination Average Packet Interval (ms): The average inter-arrival time of packets on this channel.
Destination Average Bandwidth (kb/s): The average bandwidth, in kilobits per second, calculated for this channel.
Destination Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received.
Destination TOS/DSCP Flag: The value of the Type of Service (TOS) / Differentiated Services Code Point (DSCP) flag in the IP header field.
Destination Listening R Factor: The current Listening R factor for this media stream.
Destination Listening MOS Score: The current Listening MOS Score for this media stream.

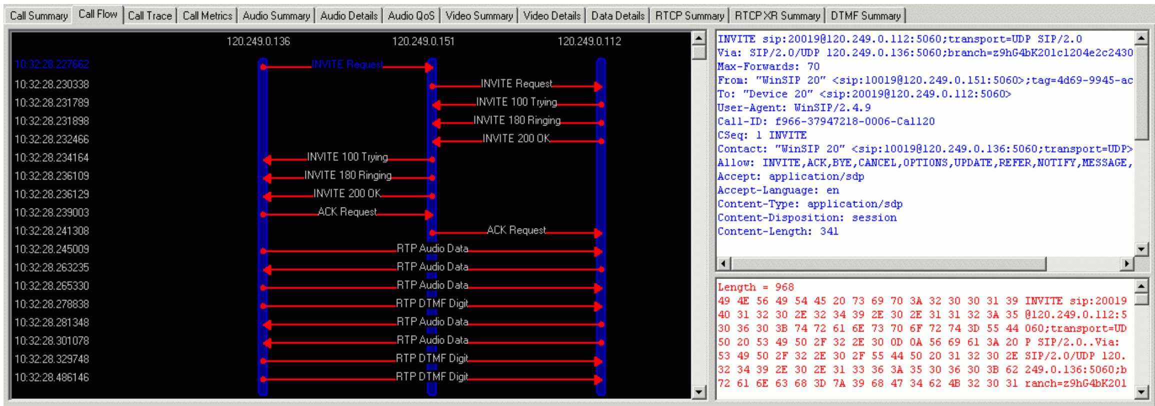
Optimal Listening R Factor / MOS Score: The highest scores that are attainable for this codec.
Stream Quality Index: The ratio of the current R Factor and MOS score to there optimal values.

Video Pane

Source Video Channel: The IP address and port of the calling endpoint.
Source Media Type: The type of codec being used to send the Video.
Source Packet Count: The number of packets sent on this channel.
Source Average Jitter (ms): The average jitter value (as calculated from RFC 3550) for this channel.
Source Average Packet Interval (ms): The average inter-arrival time of packets on this channel.
Source Average Bandwidth (kb/s): The average bandwidth, in kilobits per second, calculated for this channel.
Source Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received.
Source TOS/DSCP Flag: The value of the Type of Service (TOS) / Differentiated Services Code Point (DSCP) flag in the IP header field.

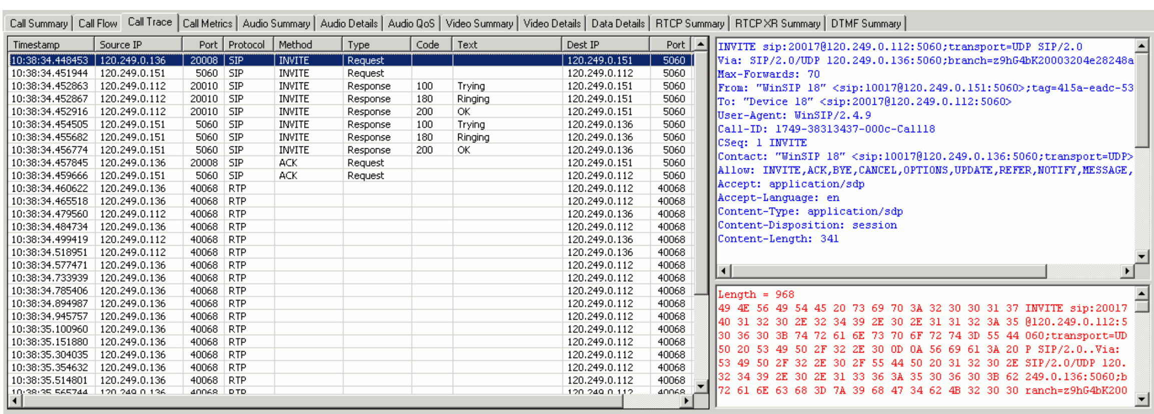
Destination Video Channel: The IP address and port of the called endpoint.
Destination Media Type: The type of codec being used to send the Video.
Destination Packet Count: The number of packets sent on this channel.
Destination Average Jitter (ms): The average jitter value (as calculated from RFC 3550) for this channel.
Destination Average Packet Interval (ms): The average inter-arrival time of packets on this channel.
Destination Average Bandwidth (kb/s): The average bandwidth, in kilobits per second, calculated for this channel.
Destination Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received.
Destination TOS/DSCP Flag: The value of the Type of Service (TOS) / Differentiated Services Code Point (DSCP) flag in the IP header field.

Call Flow



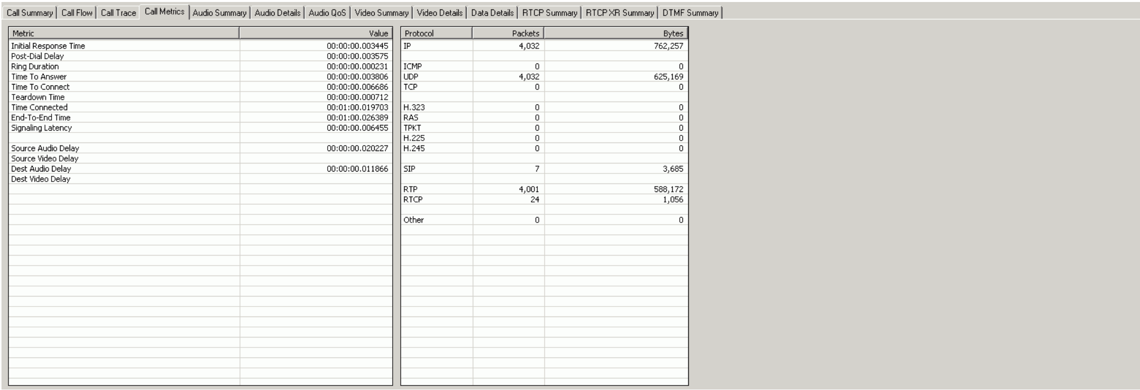
This sub-view provides a time-stamped ladder diagram view of the call flow (signaling, media and media quality packets). Each "rung" in the ladder may be highlighted to display the decoded packet in both ASCII and hexadecimal representations.

Call Trace



This sub-view provides a time stamped protocol specific display of the call flow (signaling, media and media quality packets). Each entry in the report may be highlighted to display the decoded packet in both ASCII and hexadecimal representations.

Call Metrics



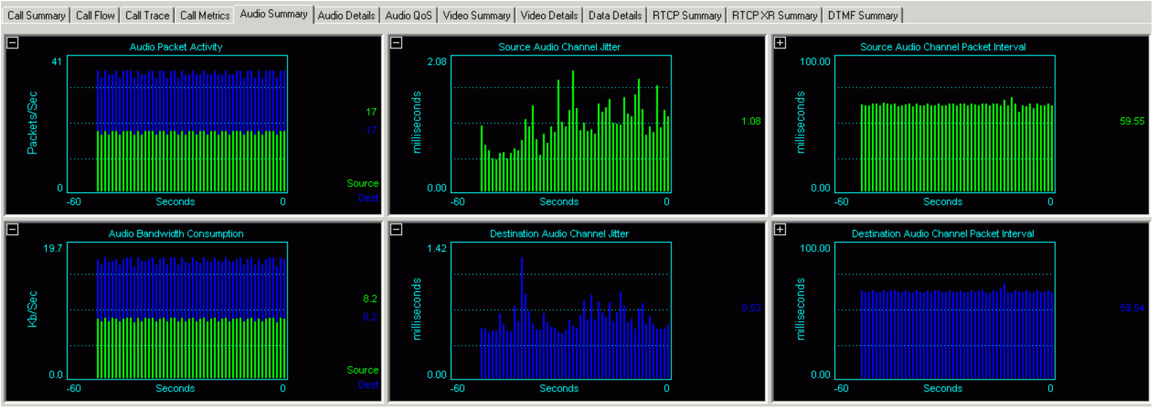
Metric	Value
Initial Response Time	00:00:00.003445
Post-Dial Delay	00:00:00.003575
Ring Duration	00:00:00.000231
Time To Answer	00:00:00.003806
Time To Connect	00:00:00.006686
Teardown Time	00:00:00.000712
Time Connected	00:01:00.019703
End-To-End Time	00:01:00.026389
Signaling Latency	00:00:00.006455
Source Audio Delay	00:00:00.020227
Source Video Delay	
Dest Audio Delay	00:00:00.011866
Dest Video Delay	

Protocol	Packets	Bytes
IP	4,032	762,257
ICMP	0	0
UDP	4,032	625,169
TCP	0	0
H.323	0	0
RAS	0	0
TPKT	0	0
H.225	0	0
H.245	0	0
SIP	7	3,685
RTP	4,001	588,172
RTCP	24	1,056
Other	0	0

This sub-view provides a summary of the call elements including metric measurements for response times and signaling interval and packets and byte counts analyzed by each protocol layer.

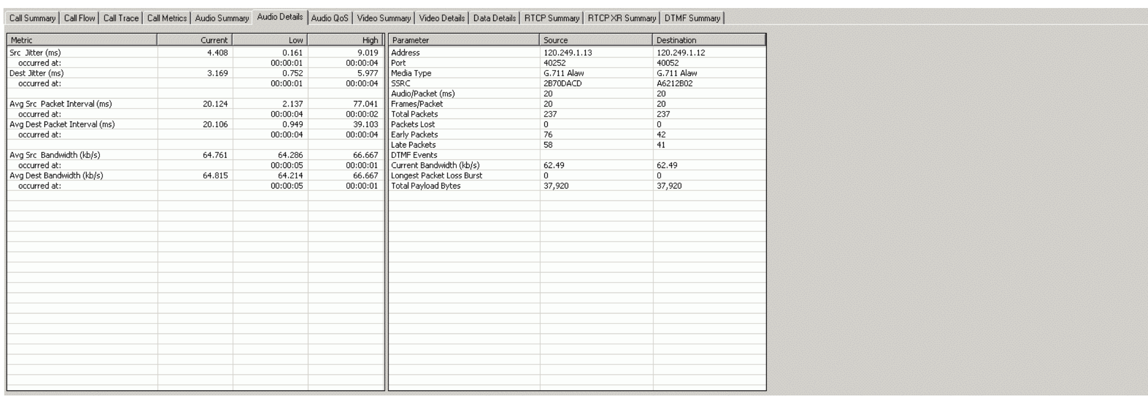
<u>Initial Response Time</u>: The length of time it took for the first message that was sent by the calling endpoint to be acknowledged by the called endpoint or proxy/gatekeeper.
<u>Post-Dial Delay</u>: The length of time from the start of the call until the start of the ring.
<u>Ring Duration</u>: The length of time the call was ringing.
<u>Time to Answer</u>: The length of time from the start of the call until it was answered.
<u>Time to Connect</u>: The length of time it took for the call to be connected.
<u>Teardown Time</u>: The length of time it took for the call close sequence to take place.
<u>Time to Connect</u>: The length of time from when the call was connected until the close sequence started.
<u>End to End Time</u>: The length of time from the start of the call until it was completed.
<u>Signal Latency</u>: The length of time it took for the call to connect plus disconnect.
<u>Source Audio Delay</u>: The length of time from when the call was connected until the first source audio packet was sent.
<u>Source Video Delay</u>: The length of time from when the call was connected until the first source video packet was sent.
<u>Destination Audio Delay</u>: The length of time from when the call was connected until the first destination audio packet was sent.
<u>Destination Video Delay</u>: The length of time from when the call was connected until the first destination video packet was sent.
<u>Time to Admit (H.323)</u>: The length of time it took for the gatekeeper to acknowledge the ARQ message.

Audio Summary



This view provides jitter and latency measurements for the audio stream being sent by the calling and called parties. Included with the graphical representations of jitter and latency are the high low and current values for each as well as the stream type, the sender's IP address and port, the receiver's IP address and port, the number of packets lost and the DTMF sequences if present within the stream (RFC 2833 section 3 Named Telephony Events).

Audio Details



Metric	Current	Low	High
Src Jitter (ms)	4.408	0.161	9.019
occurred at:		00:00:01	00:00:04
Dest Jitter (ms)	3.169	0.752	5.977
occurred at:		00:00:01	00:00:04
Avg Src Packet Interval (ms)	20.124	2.137	77.041
occurred at:		00:00:04	00:00:02
Avg Dest Packet Interval (ms)	20.106	0.949	39.103
occurred at:		00:00:04	00:00:04
Avg Src Bandwidth (kb/s)	64.761	64.286	66.667
occurred at:		00:00:05	00:00:01
Avg Dest Bandwidth (kb/s)	64.815	64.214	66.667
occurred at:		00:00:05	00:00:01

Parameter	Source	Destination
Address	120.249.1.13	120.249.1.12
Port	40252	40052
Media Type	G.711 Alaw	G.711 Alaw
SSRC	2B70DACD	A6212B02
Audio/Packet (ms)	20	20
Frames/Packet	20	20
Total Packets	237	237
Packets Lost	0	0
Early Packets	76	42
Late Packets	58	41
DTMF Events		
Current Bandwidth (kb/s)	62.49	62.49
Longest Packet Loss Burst	0	0
Total Payload Bytes	37,920	37,920

This sub-view provides summary information including jitter and interval measurements for the audio streams. The high, low and current values for each stream as well as the stream type, the sender's IP address and port, the receiver's IP address and port, the number of packets lost and the DTMF sequences if present within the stream (RFC 2833 section 3 Named Telephony Events). This sub-view contains two panes.

Metrics Pane

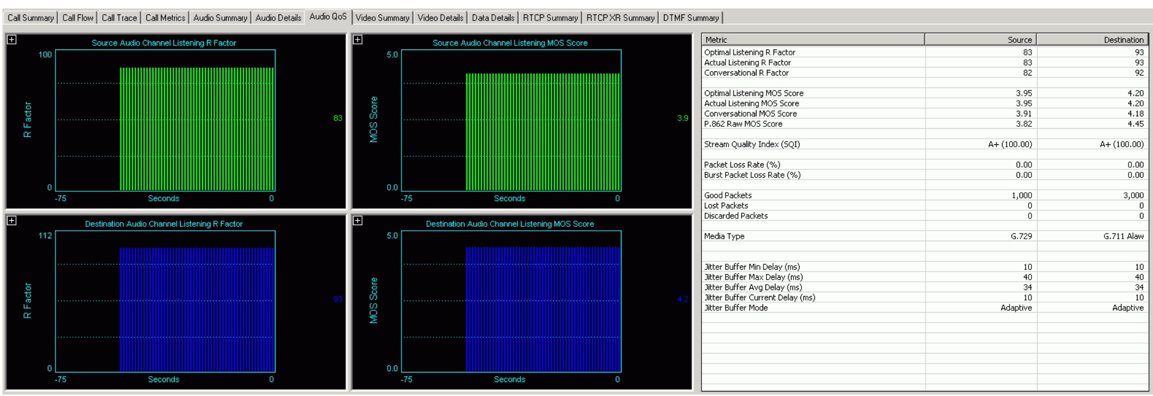
Source Jitter (ms): The average, low, and high jitter measurements calculated for the source audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low source jitter values were calculated.
Destination Jitter (ms): The average, low, and high jitter measurements calculated for the destination audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination jitter values were calculated.
Average Source Packet Interval (ms): The average, low, and high inter-arrival time of packets on the source audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low source packet interval values were calculated.
Average Destination Packet Interval (ms): The average, low, and high inter-arrival time of packets on the destination audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination packet interval values were calculated.
Average Source Bandwidth: The average, low, and high bandwidth, in kilobits per second, calculated for the source audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low source bandwidth values were calculated.
Average Destination Bandwidth: The average, low, and high bandwidth, in kilobits per second, calculated for the destination audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination bandwidth values were calculated.

Parameters Pane

Address: The IP addresses for the source and destination channels.
Port: The port numbers for the source and destination channels.
Media Type: The codec type for the source and destination channels.
SSRC: The synchronization source for the source and destination channels.
Audio/Packet (ms): The length of audio time contained in each packet for the source and destination channels.
Frames/Packet: The number of audio frames contained in each packet for the source and destination channels.
Total Packets: The number of packets counted for the source and destination channels.
Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received for the source and destination channels.

Early Packets: The number of packets considered early as configured on the Edit Menu | Settings | Advanced Tab for the source and destination channels.
Late Packets: The number of packets considered late as configured on the Edit Menu | Settings | Advanced Tab for the source and destination channels.
DTMF Events: The value of the DTMF digits (RFC 2833) for the source and destination channels.
Current Bandwidth (kb/s): The bandwidth, in kilobits per second, calculated during the last second for the source and destination channels.
Longest Packet Loss Burst: The count of the longest sequence of lost packets for the source and destination channels.
Total Payload Bytes: The number of bytes in the payload portion of the packet for the source and destination channels.

Audio QoS



This sub-view provides a real-time display of the R-factor and MOS scores for each stream. The R-factor/MOS scoring feature is a non-intrusive measurement technique available for the WinEyeQ call monitor. WinEyeQ passively measures the characteristics of live VoIP calls and reports quality scores in real-time. The algorithm used to obtain the R-Factor/MOS quality scores accurately models the way that time-varying impairments, most notably burst packet loss and possible jitter buffer discards, affect perceived speech quality. This sub-view has three panes.

Listening R Factor Pane

This pane displays the source audio (upper) and destination audio (lower) Listening R Factors in real-time.

Listening MOS Score Pane

This pane displays the source audio (upper) and destination audio (lower) Listening MOS Scores in real-time.

Metrics Pane

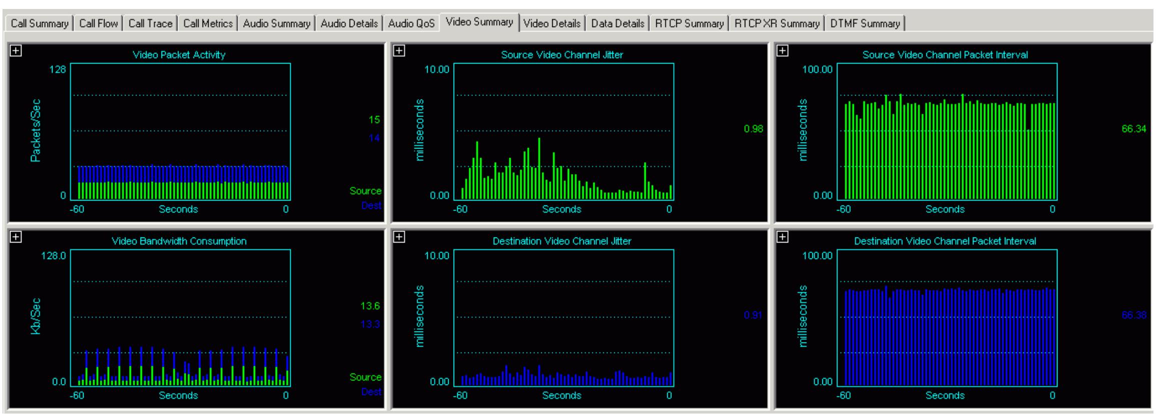
Optimal Listening R Factor: The highest score that is attainable for this codec.
Actual Listening R Factor: The current value of the Listening R Factor for the source and destination audio streams.
Conversational R Factor: The current value of the Conversational R Factor for the source and destination audio streams.
Optimal Listening MOS Score: The highest score that is attainable for this codec.
Actual Listening MOS Score: The current value of the Listening MOS Score for the source and destination audio streams.
Conversational MOS Score: The current value of the Conversational MOS Score for the source and destination audio streams.
P.862 Raw MOS Score: The current value of the P.862 Raw MOS Score for the source and destination audio streams.
Stream Quality Index: The ratio of the current R Factor and MOS score to their optimal values.
Packet Loss Rate (%): The total number packets that were lost divided by the total number of packets that were received.
Burst Packet Loss Rate (%): The packet loss rate encountered for burst conditions for the source and destination audio streams.
Good Packets: The number of packets received from the source and destination audio streams.
Lost Packets: The number of network lost packets from the source and destination audio streams.
Discarded Packets: The number of discarded packets due to excessive delay or extremely early arrival detected for the source and destination audio streams.
Media Type: The codec type for the source and destination audio streams.
Jitter Buffer Minimum Delay (ms): The minimum jitter buffer emulator delay in milliseconds occurring during a call for the source and destination audio streams.
Jitter Buffer Maximum Delay (ms): The maximum jitter buffer emulator delay in milliseconds occurring during a call for the source and destination audio streams.
Jitter Buffer Average Delay (ms): The average jitter buffer emulator delay in milliseconds occurring during a call from the source and destination audio streams.

Jitter Buffer Current Delay (ms): The current jitter buffer emulator delay in milliseconds from the source and destination audio streams.
Jitter Buffer Mode: The type of jitter buffer (adaptive of fixer) being used for the source and destination audio streams. This is configured on the Edit Menu | Settings | QoS Tab.

The quality scores for MOS range from 0 to 4.5 and the R factor measurements range from 0 to 105 depending on codec type. The guidelines for interpreting the R-factor and MOS scores are shown in the table below for the G.711 codec:

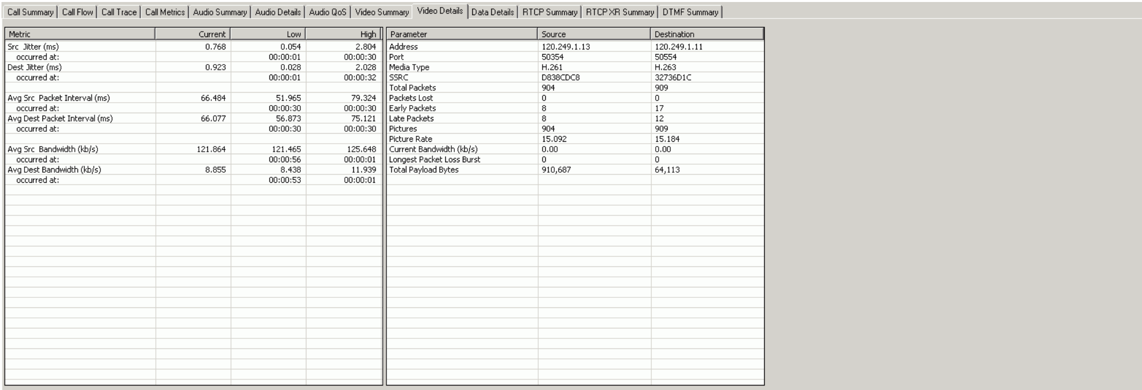
Desirability Scale	R-factor Range	MOS Range
Desirable	94 - 80	4.4 - 4.0
Acceptable	80 - 70	4.0 - 3.6
Reach Connection	70 - 50	3.6 - 2.6
Not recommended	50 - 0	2.6 - 0

Video Summary



This view provides jitter and latency measurements for the video stream being sent by the calling and called parties. Included with the graphical representations of jitter and latency are the high low and current values for each stream, as well as the stream type, the sender's IP address and port, the receiver's IP address and port, the number of packets lost, the bandwidth consumption, the number of pictures detected, and the picture rate.

Video Details



This sub-view provides summary information including jitter and interval measurements for the video streams. The measurements include high, low, and current values for each stream. As well as the stream type, the sender's IP address and port number, the receiver's IP address and port number, the packets lost, the number of pictures detected, and the picture rate. This sub-view contains two panes.

Metrics Pane

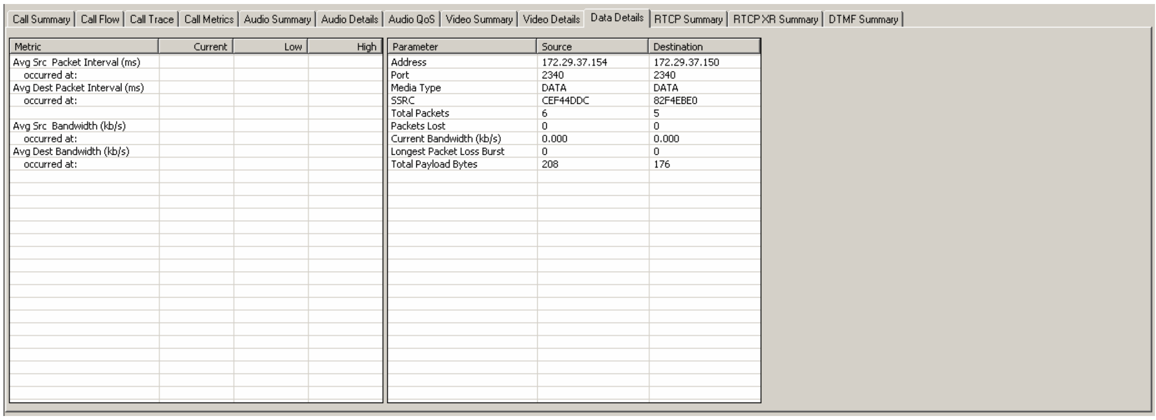
<u>Source Jitter (ms)</u>: The average, low, and high jitter measurements calculated for the source video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low source jitter values were calculated.
<u>Destination Jitter (ms)</u>: The average, low, and high jitter measurements calculated for the destination video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low destination jitter values were calculated.
<u>Average Source Packet Interval (ms)</u>: The average, low, and high inter-arrival time of packets on the source video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low source packet interval values were calculated.
<u>Average Destination Packet Interval (ms)</u>: The average, low, and high inter-arrival time of packets on the destination video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low destination packet interval values were calculated.
<u>Average Source Bandwidth</u>: The average, low, and high bandwidth, in kilobits per second, calculated for the source video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low source bandwidth values were calculated.

Average Destination Bandwidth: The average, low, and high bandwidth, in kilobits per second, calculated for the destination video stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination bandwidth values were calculated.

Parameters Pane

Address: The IP addresses for the source and destination channels.
Port: The port numbers for the source and destination channels.
Media Type: The codec type for the source and destination channels.
SSRC: The synchronization source for the source and destination channels.
Total Packets: The number of packets counted for the source and destination channels.
Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received for the source and destination channels.
Early Packets: The number of packets considered early as configured on the Edit Menu **|** Settings **|** Advanced Tab for the source and destination channels.
Late Packets: The number of packets considered late as configured on the Edit Menu **|** Settings **|** Advanced Tab for the source and destination channels.
Pictures: The number of picture start codes counted for the source and destination channels.
Picture Rate: The number of pictures per second calculated for the source and destination channels.
Current Bandwidth (kb/s): The bandwidth, in kilobits per second, calculated during the last second for the source and destination channels.
Longest Packet Loss Burst: The count of the longest sequence of lost packets for the source and destination channels
Total Payload Bytes: The number of bytes in the payload portion of the packet for the source and destination channels.

Data Details



This sub-view provides summary information including interval measurements for the data streams, the high, low and current values for each stream as well as the stream type, the sender's IP address and port, the receiver's IP address and port, and the number of packets lost. There are two panes on this sub-view.

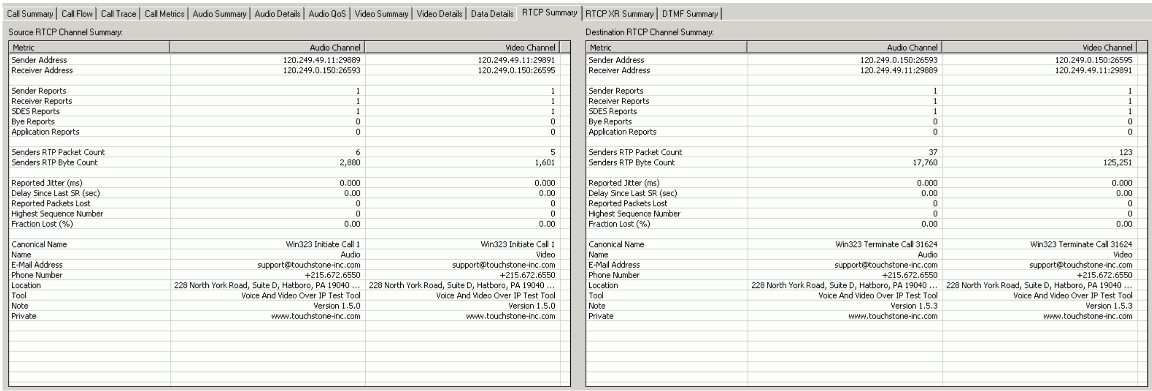
Metrics Pane

Average Source Packet Interval (ms): The average, low, and high inter-arrival time of packets on the source video stream.
Occurred at:: The time, relative to the start of the call, that the high and low source packet interval values were calculated.
Average Destination Packet Interval (ms): The average, low, and high inter-arrival time of packets on the destination video stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination packet interval values were calculated.
Average Source Bandwidth: The average, low, and high bandwidth, in kilobits per second, calculated for the source video stream.
Occurred at:: The time, relative to the start of the call, that the high and low source bandwidth values were calculated.
Average Destination Bandwidth: The average, low, and high bandwidth, in kilobits per second, calculated for the destination video stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination bandwidth values were calculated.

Parameters Pane

Address: The IP addresses for the source and destination channels.
Port: The port numbers for the source and destination channels.
Media Type: The codec type for the source and destination channels.
SSRC: The synchronization source for the source and destination channels.
Total Packets: The number of packets counted for the source and destination channels.
Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received for the source and destination channels.
Current Bandwidth (kb/s): The bandwidth, in kilobits per second, calculated during the last second for the source and destination channels.
Longest Packet Loss Burst: The count of the longest sequence of lost packets for the source and destination channels
Total Payload Bytes: The number of bytes in the payload portion of the packet for the source and destination channels.

RTCP Summary



Call Summary | Call Flow | Call Trace | Call Metrics | Audio Summary | Audio Details | Audio QoS | Video Summary | Video Details | Data Details | RTCP Summary | RTCP XR Summary | DTMF Summary

Source RTCP Channel Summary:

Metric	Audio Channel	Video Channel
Sender Address	120.249.49.11:29889	120.249.49.11:29891
Receiver Address	120.249.0.150:26593	120.249.0.150:26595
Sender Reports	1	1
Receiver Reports	1	1
SDES Reports	1	1
Bye Reports	0	0
Application Reports	0	0
Senders RTP Packet Count	6	5
Senders RTP Byte Count	2,880	1,601
Reported Jitter (ms)	0.000	0.000
Delay Since Last SR (sec)	0.00	0.00
Reported Packets Lost	0	0
Highest Sequence Number	0	0
Fraction Lost (%)	0.00	0.00
Canonical Name	Win323 Initiate Call 1	Win323 Initiate Call 1
Name	Audio	Video
E-Mail Address	support@touchstone-inc.com	support@touchstone-inc.com
Phone Number	+215.672.6550	+215.672.6550
Location	228 North York Road, Suite D, Hatboro, PA 19040 ...	228 North York Road, Suite D, Hatboro, PA 19040 ...
Tool	Voice And Video Over IP Test Tool	Voice And Video Over IP Test Tool
Note	Version 1.5.0	Version 1.5.0
Private	www.touchstone-inc.com	www.touchstone-inc.com

Destination RTCP Channel Summary:

Metric	Audio Channel	Video Channel
Sender Address	120.249.0.150:26593	120.249.0.150:26595
Receiver Address	120.249.49.11:29889	120.249.49.11:29891
Sender Reports	1	1
Receiver Reports	1	1
SDES Reports	1	1
Bye Reports	0	0
Application Reports	0	0
Senders RTP Packet Count	37	123
Senders RTP Byte Count	17,760	125,251
Reported Jitter (ms)	0.000	0.000
Delay Since Last SR (sec)	0.00	0.00
Reported Packets Lost	0	0
Highest Sequence Number	0	0
Fraction Lost (%)	0.00	0.00
Canonical Name	Win323 Terminate Call 31624	Win323 Terminate Call 31624
Name	Audio	Video
E-Mail Address	support@touchstone-inc.com	support@touchstone-inc.com
Phone Number	+215.672.6550	+215.672.6550
Location	228 North York Road, Suite D, Hatboro, PA 19040 ...	228 North York Road, Suite D, Hatboro, PA 19040 ...
Tool	Voice And Video Over IP Test Tool	Voice And Video Over IP Test Tool
Note	Version 1.5.3	Version 1.5.3
Private	www.touchstone-inc.com	www.touchstone-inc.com

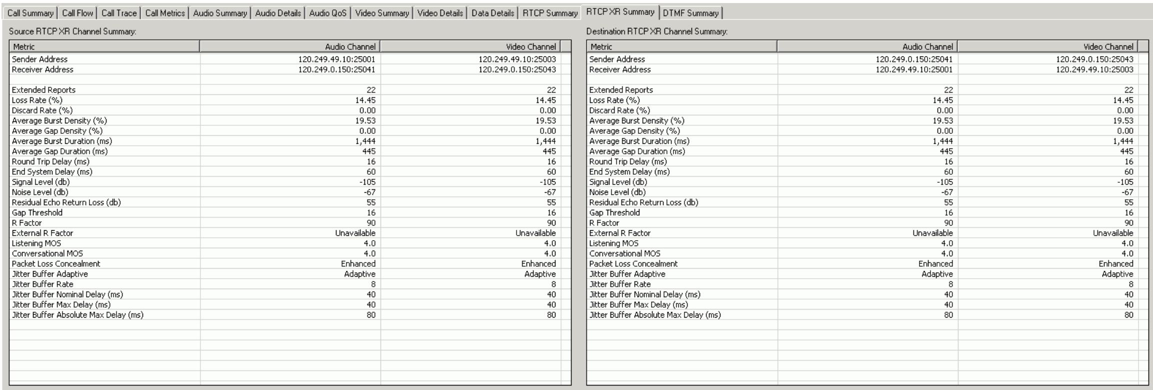
This sub-view provides summary information that has been gathered from the RTCP packets that WinEyeQ has analyzed for the audio and video streams that have been sent by both endpoints of the call. This sub-view has two panes that are identical except for source and destination.

RTCP Channel Summary Pane

<u>Sender Address</u>: The IP address and port number of the sending RTCP channel.
<u>Receiver Address</u>: The IP address and port number of the receiving RTCP channel.
<u>Sender Reports</u>: The number of RTCP Sender Reports sent.
<u>Receiver Reports</u>: The number of RTCP Receiver Reports sent.
<u>SDES</u>: The number of RTCP SDES Reports sent.
<u>Bye Reports</u>: The number of RTCP Bye Reports sent.
<u>Application Reports</u>: The number of RTCP Application Reports sent.
<u>Senders Packet Count</u>: The total number of RTP data packets transmitted by the sender since starting transmission.
<u>Senders Byte Count</u>: The total number of payload octets transmitted in RTP data packets by the sender since starting transmission.
<u>Reported Jitter (ms)</u>: The jitter measurement calculated on the stream being received from the other endpoint.
<u>Delay Since Last SR (sec)</u>: The delay, expressed in units of 1/65536 seconds, between receiving the last SR packet from the remote endpoint and sending this reception report block.
<u>Reported Packets Lost</u>: The total number of RTP data packets from the remote endpoint that have been lost since the beginning of reception.

Highest Sequence Number: The low 16 bits contain the highest sequence number received in an RTP data packet from the remote endpoint, and the most significant 16 bits extend that sequence number with the corresponding count of sequence number cycles.
Fraction Lost (%): The fraction of RTP data packets from the remote endpoint lost since the previous SR or RR packet was sent, expressed as a fixed point number with the binary point at the left edge of the field.
Canonical Name: A unique end-point identifier.
Name: The real name used to describe the source.
E-Mail Address: The email address is formatted according to RFC 2822.
Phone Number: The phone number (should be formatted with the plus sign replacing the international access code).
Location: The geographic user location.
Tool: The application or tool name.
Note: This is intended for transient messages describing the current state of the source.
Private: This item is used to define experimental or application-specific extensions.

RTCP XR Summary



Source RTCP XR Channel Summary:

Metric	Audio Channel	Video Channel
Sender Address	120.249.49.10:25001	120.249.49.10:25003
Receiver Address	120.249.0.150:25041	120.249.0.150:25043
Extended Reports	22	22
Loss Rate (%)	14.45	14.45
Discard Rate (%)	0.00	0.00
Average Burst Density (%)	19.53	19.53
Average Gap Density (%)	0.00	0.00
Average Burst Duration (ms)	1,444	1,444
Average Gap Duration (ms)	445	445
Round Trip Delay (ms)	16	16
End System Delay (ms)	60	60
Signal Level (db)	-105	-105
Noise Level (db)	-67	-67
Residual Echo Return Loss (db)	55	55
Gap Threshold	16	16
R Factor	90	90
External R Factor	Unavailable	Unavailable
Listening MOS	4.0	4.0
Conversational MOS	4.0	4.0
Packet Loss Concealment	Enhanced	Enhanced
Jitter Buffer Adaptive	Adaptive	Adaptive
Jitter Buffer Rate	8	8
Jitter Buffer Nominal Delay (ms)	40	40
Jitter Buffer Max Delay (ms)	40	40
Jitter Buffer Absolute Max Delay (ms)	80	80

Destination RTCP XR Channel Summary:

Metric	Audio Channel	Video Channel
Sender Address	120.249.0.150:25041	120.249.0.150:25043
Receiver Address	120.249.49.10:25001	120.249.49.10:25003
Extended Reports	22	22
Loss Rate (%)	14.45	14.45
Discard Rate (%)	0.00	0.00
Average Burst Density (%)	19.53	19.53
Average Gap Density (%)	0.00	0.00
Average Burst Duration (ms)	1,444	1,444
Average Gap Duration (ms)	445	445
Round Trip Delay (ms)	16	16
End System Delay (ms)	60	60
Signal Level (db)	-105	-105
Noise Level (db)	-67	-67
Residual Echo Return Loss (db)	55	55
Gap Threshold	16	16
R Factor	90	90
External R Factor	Unavailable	Unavailable
Listening MOS	4.0	4.0
Conversational MOS	4.0	4.0
Packet Loss Concealment	Enhanced	Enhanced
Jitter Buffer Adaptive	Adaptive	Adaptive
Jitter Buffer Rate	8	8
Jitter Buffer Nominal Delay (ms)	40	40
Jitter Buffer Max Delay (ms)	40	40
Jitter Buffer Absolute Max Delay (ms)	80	80

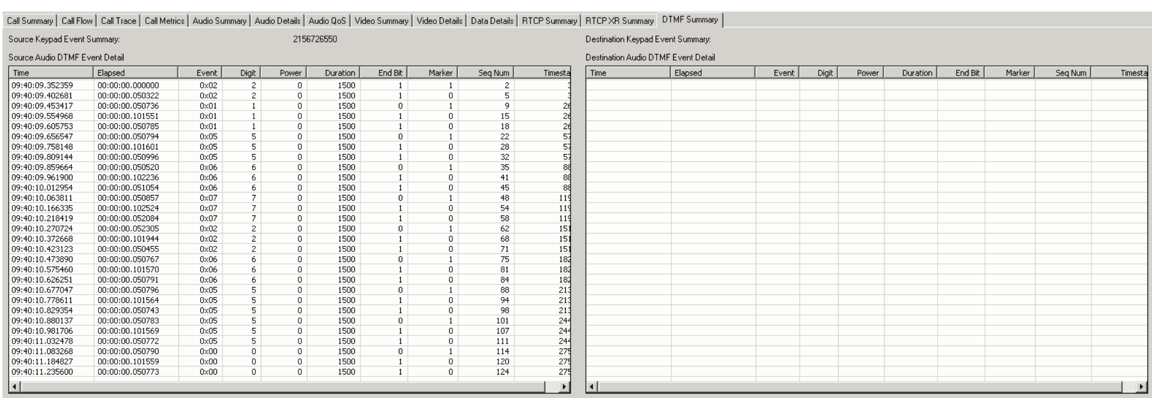
This sub-view provides summary information that has been gathered from the RTCP XR packets that WinEyeQ has analyzed for the audio and video streams that have been sent by both endpoints of the call. This sub-tab has two panes that are identical.

RTCP XR Channel Summary

Sender Address: The IP address and port number of the sending RTCP channel.
Receiver Address: The IP address and port number of the receiving RTCP channel.
Extended Reports: The number of RTCP Extended Reports sent.
Loss Rate (%): The fraction of packets lost since the beginning of the call.
Discard Rate (%): The fraction of packets discarded since the beginning of the call.
Average Burst Density (%): The fraction of packets within burst periods since the beginning of the call.
Average Gap Density (%): The fraction of packets within gap periods since the beginning of the call.
Average Burst Duration (ms): The mean duration, in milliseconds, of the burst periods since the beginning of the call.
Average Gap Duration (ms): The mean duration, in milliseconds, of the gap periods since the beginning of the call.
Round Trip Delay (ms): The most recently calculated round-trip delay, in milliseconds.
End System Delay (ms): The most recently estimated end system delay, in milliseconds.

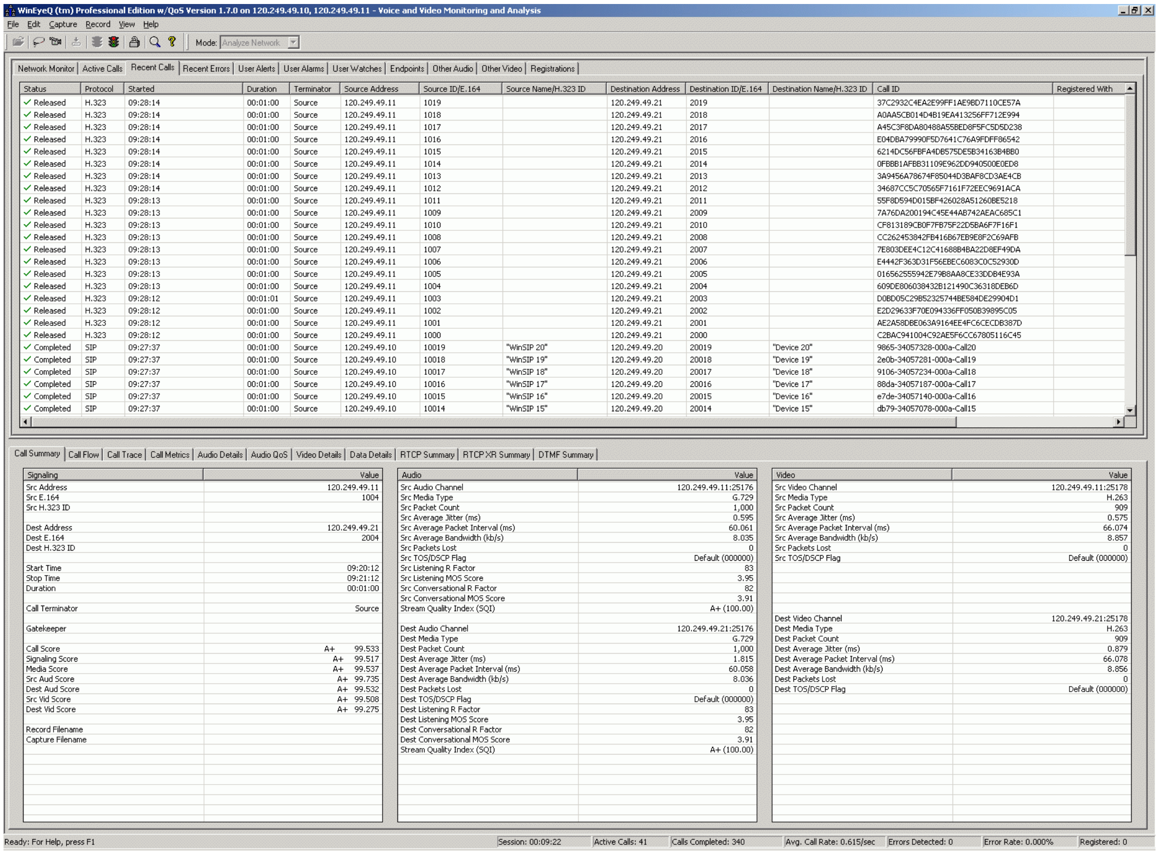
Signal Level (db): The relative speech signal level expressed as the ratio of the signal level to a 0 dBm0 reference.
Noise Level (db): The relative silence period noise level expressed as the ratio of the background noise level to a 0 dBm0 reference.
Residual Echo Return Loss (db): The residual echo return loss as the sum of the measured echo return loss (ERL) and the echo return loss enhanced (ERLE) of the echo canceller, expressed in dB.
Gap Threshold: The gap threshold, in packets.
R Factor: The voice quality metric for the call channel as measured in the monitored network segment.
External R Factor: The voice quality metric for the call channel as measured in an external monitored network segment.
Listening MOS: The estimated mean opinion listening quality score for the call channel.
Conversational MOS: The estimated mean opinion conversational quality score for the call channel.
Packet Loss Concealment: The packet loss concealment capabilities.
Jitter Buffer Adaptive: Adaptive or non-adaptive.
Jitter Buffer Rate: This represents the implementation specific adjustment rate of a jitter buffer in adaptive mode.
Jitter Buffer Nominal Delay (ms): The current nominal jitter buffer delay, in milliseconds.
Jitter Buffer Max Delay (ms): The maximum jitter buffer delay, in milliseconds, recorded for the call.
Jitter Buffer Absolute Max Delay (ms): The absolute maximum delay, in milliseconds, the jitter buffer can ever introduce to the call channel packet stream.

DTMF Summary



This sub-view provides a detailed and organized tabular display for the active DTMF transmissions that occur during a call for both the source and destination side of the calls.

Recent Calls View



The recent calls view is designed to provide an in-depth view of each recent VoIP call and its status. Each call is represented by an entry in the topmost report; the list is updated as the calls are removed from the active calls view.

This view contains the following columns:

Call Status: The current status of the call. These may be things such as connecting, ringing, connected, error, etc.

Protocol: The values for this field are SIP or H.323.

Started: This is the time (local time) that the call was started.

Duration: The length of time the call is (or was) active.

Terminator: Which side of the call (Source or Destination) terminated the call.

Source Address: The address of the call initiator (caller).

<u>Source ID/E.164</u>: The SIP user ID or H.323 E.164 alias of the caller.

<u>Source Name/H.323 ID</u>: The SIP display name or H.323 ID of the caller.

<u>Destination Address</u>: The address of the call receiver (party called).

<u>Destination ID/E.164</u>: The SIP user ID or H.323 E.164 alias of the party called.

<u>Destination Name/H.323 ID</u>: The SIP display name or H.323 ID of the party called.

<u>Call ID</u>: The SIP or H.323 call ID associated with this call.

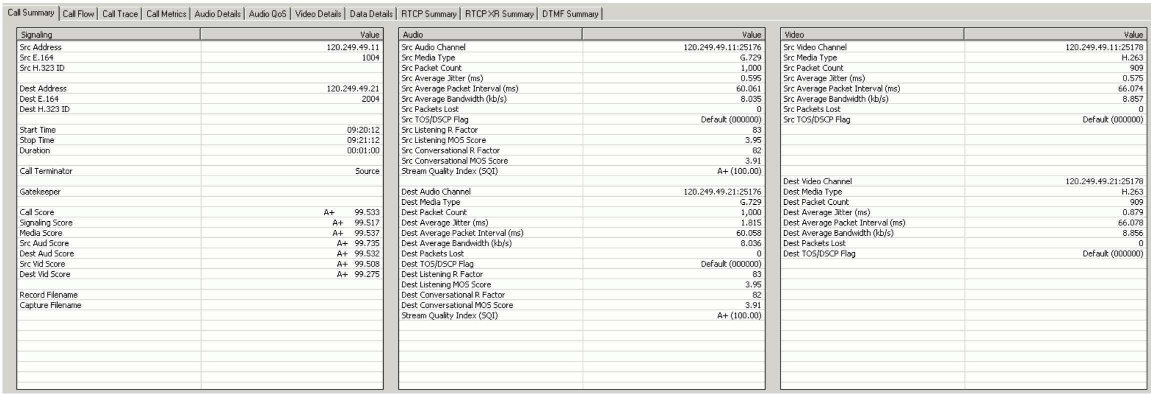
<u>Registered With</u>: The gatekeeper's IP address for H.323 calls, or the Proxy's IP address for SIP calls.

<u>Conference ID</u>: The conference ID (H.323 calls only).

Each individual call has the following sub-views.

- Call Summary
- Call Flow (ladder diagram)
- Call Trace
- Call Metrics
- Audio Details
- Audio QoS
- Video Details
- Data Details
- RTCP Summary
- RTCP XR Summary
- DTMF Summary

Call Summary



This sub-view provides a summary of the call elements including source and destination addresses for signaling and media. There are three panes on this sub-view.

Signaling Pane

<u>Source Address</u>: The IP address of the calling endpoint.
<u>Source ID/Source E.164</u>: The source ID (SIP) or E.164 (H.323) of the calling endpoint.
<u>Source Name/Source H.323 ID</u>: The source name (SIP) or H.323 ID (H.323) of the calling endpoint.
<u>Destination Address</u>: The IP address of the called endpoint.
<u>Destination ID/E.164</u>: The source ID (SIP) or E.164 (H.323) of the called endpoint.
<u>Destination Name/H.323 ID</u>: The source name (SIP) or H.323 ID (H.323) of the called endpoint.
<u>Start Time</u>: The time the first packet was seen on the network.
<u>Stop Time</u>: The time the last packet was seen on the network.
<u>Duration</u>: The difference between the start and stop time.
<u>Call Terminator</u>: The endpoint that terminated the call.
<u>Proxy/Gatekeeper</u>: The address of the proxy (SIP) or gatekeeper (H.323) that participated in the call.
<u>Call Score</u>: Please see Appendix C for scoring details.
<u>Signal Score</u>: Please see Appendix C for scoring details.
<u>Media Score</u>: Please see Appendix C for scoring details.
<u>Source Audio Score</u>: Please see Appendix C for scoring details.
<u>Destination Audio Score</u>: Please see Appendix C for scoring details.
<u>Source Video Score</u>: Please see Appendix C for scoring details.
<u>Destination Video Score</u>: Please see Appendix C for scoring details.
<u>Record Filename</u>: The file name of the record file.
<u>Capture Filename</u>: The file name of the capture file.

Audio Pane

Source Audio Channel: The IP address and port of the calling endpoint.
Source Media Type: The type of codec being used to send the audio.
Source Packet Count: The number of packets sent on this channel.
Source Average Jitter (ms): The average jitter value (as calculated from RFC 3550) for this channel.
Source Average Packet Interval (ms): The average inter-arrival time of packets on this channel.
Source Average Bandwidth (kb/s): The average bandwidth, in kilobits per second, calculated for this channel.
Source Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received.
Source TOS/DSCP Flag: The value of the Type of Service (TOS) / Differentiated Services Code Point (DSCP) flag in the IP header field.
Source Listening R Factor: The current Listening R factor for this media stream.
Source Listening MOS Score: The current Listening MOS Score for this media stream.
Source Conversational R Factor: The current Conversational R factor for this media stream.
Source Conversational MOS Score: The current Conversational MOS Score for this media stream.
Stream Quality Index: The ratio of the current R Factor and MOS score to there optimal values.

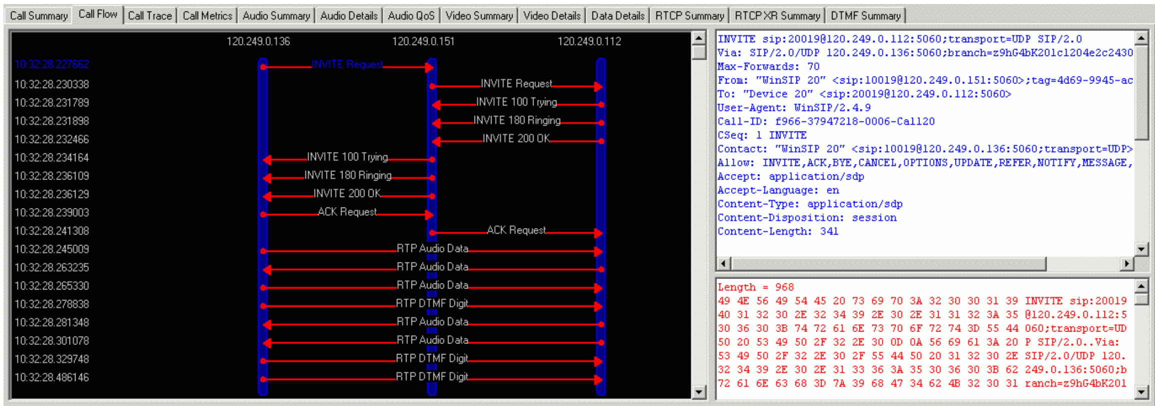
Destination Audio Channel: The IP address and port of the called endpoint.
Destination Media Type: The type of codec being used to send the audio.
Destination Packet Count: The number of packets sent on this channel.
Destination Average Jitter (ms): The average jitter value (as calculated from RFC 3550) for this channel.
Destination Average Packet Interval (ms): The average inter-arrival time of packets on this channel.
Destination Average Bandwidth (kb/s): The average bandwidth, in kilobits per second, calculated for this channel.
Destination Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received.
Destination TOS/DSCP Flag: The value of the Type of Service (TOS) / Differentiated Services Code Point (DSCP) flag in the IP header field.
Destination Listening R Factor: The current Listening R factor for this media stream.

Destination Listening MOS Score: The current Listening MOS Score for this media stream.
Destination Conversational R Factor: The current Conversational R factor for this media stream.
Destination Conversational MOS Score: The current Conversational MOS Score for this media stream.
Stream Quality Index: The ratio of the current R Factor and MOS score to there optimal values.

Video Pane

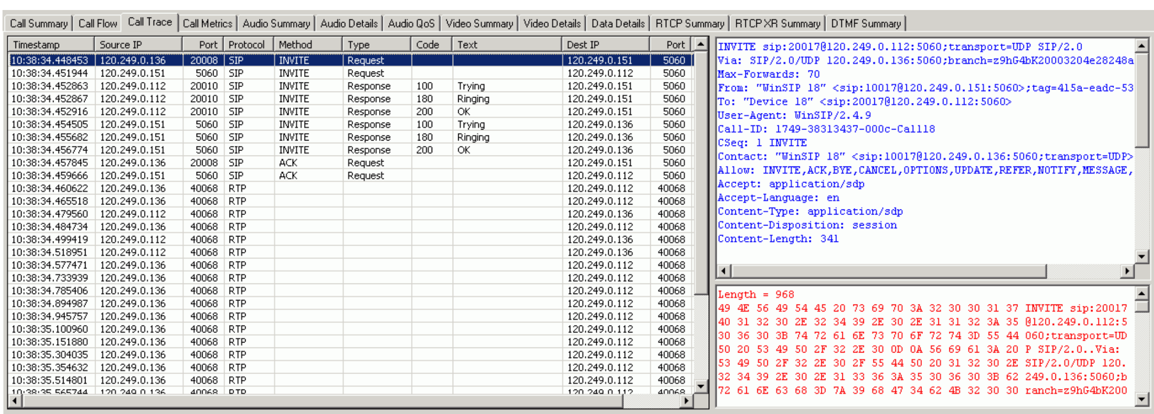
Source Video Channel: The IP address and port of the calling endpoint.
Source Media Type: The type of codec being used to send the Video.
Source Packet Count: The number of packets sent on this channel.
Source Average Jitter (ms): The average jitter value (as calculated from RFC 3550) for this channel.
Source Average Packet Interval (ms): The average inter-arrival time of packets on this channel.
Source Average Bandwidth (kb/s): The average bandwidth, in kilobits per second, calculated for this channel.
Source Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received.
Source TOS/DSCP Flag: The value of the Type of Service (TOS) / Differentiated Services Code Point (DSCP) flag in the IP header field.
Destination Video Channel: The IP address and port of the called endpoint.
Destination Media Type: The type of codec being used to send the Video.
Destination Packet Count: The number of packets sent on this channel.
Destination Average Jitter (ms): The average jitter value (as calculated from RFC 3550) for this channel.
Destination Average Packet Interval (ms): The average inter-arrival time of packets on this channel.
Destination Average Bandwidth (kb/s): The average bandwidth, in kilobits per second, calculated for this channel.
Destination Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received.
Destination TOS/DSCP Flag: The value of the Type of Service (TOS) / Differentiated Services Code Point (DSCP) flag in the IP header field.

Call Flow



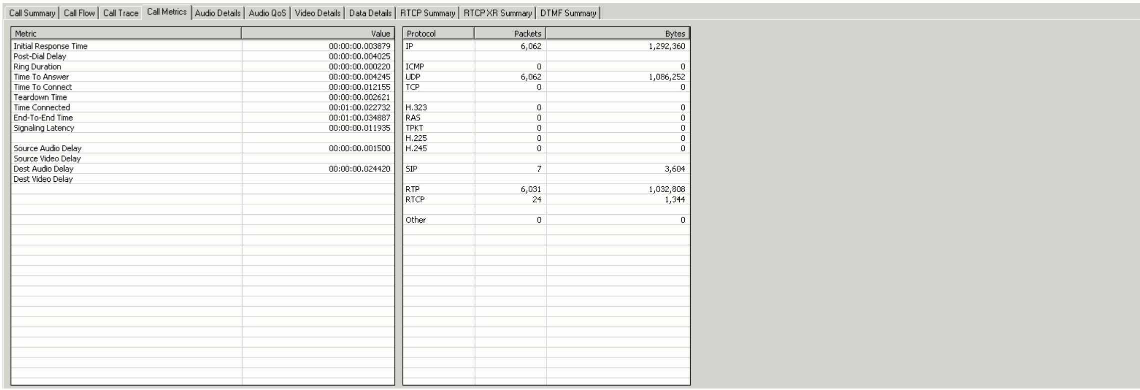
This sub-view provides a time-stamped ladder diagram view of the call flow (signaling, media and media quality packets). Each "rung" in the ladder may be highlighted to display the decoded packet in both ASCII and hexadecimal representations.

Call Trace



This sub-view provides a time stamped protocol specific display of the call flow (signaling, media and media quality packets). Each entry in the report may be highlighted to display the decoded packet in both ASCII and hexadecimal representations.

Call Metrics



This sub-view provides a summary of the call elements including metric measurements for response times and signaling interval and packets and byte counts analyzed by each protocol layer. There are two panes on this sub-view.

Metrics Pane

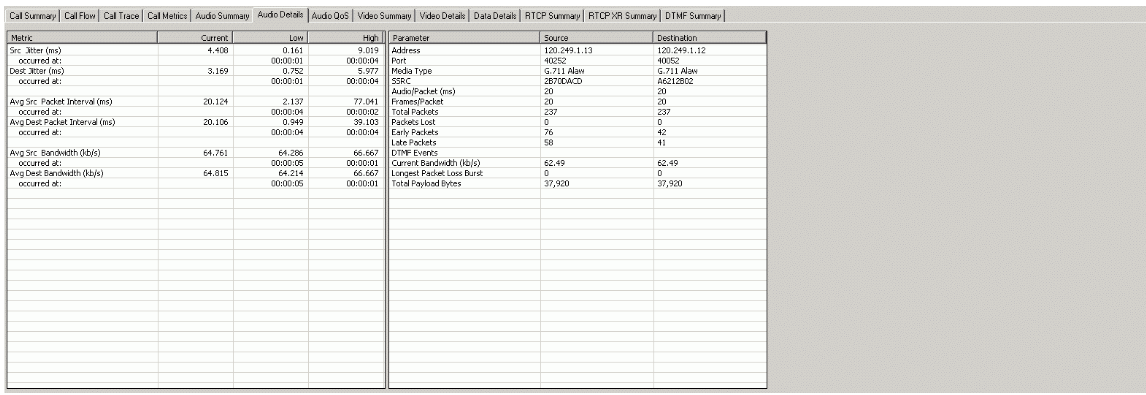
<u>Initial Response Time</u>: The length of time it took for the first message that was sent by the calling endpoint to be acknowledged by the called endpoint or proxy/gatekeeper.
<u>Post-Dial Delay</u>: The length of time from the start of the call until the start of the ring.
<u>Ring Duration</u>: The length of time the call was ringing.
<u>Time to Answer</u>: The length of time from the start of the call until it was answered.
<u>Time to Connect</u>: The length of time it took for the call to be connected.
<u>Teardown Time</u>: The length of time it took for the call close sequence to take place.
<u>Time Connected</u>: The length of time from when the call was connected until the close sequence started.
<u>End to End Time</u>: The length of time from the start of the call until it was completed.
<u>Signal Latency</u>: The length of time it took for the call to connect plus disconnect.
<u>Source Audio Delay</u>: The length of time from when the call was connected until the first source audio packet was sent.
<u>Source Video Delay</u>: The length of time from when the call was connected until the first source video packet was sent.
<u>Destination Audio Delay</u>: The length of time from when the call was connected until the first destination audio packet was sent.

Destination Video Delay: The length of time from when the call was connected until the first destination video packet was sent.

Protocol Pane

Packets and Bytes count, for the selected call, broken down by indicated protocol.

Audio Details



This sub-view provides summary information including jitter and interval measurements for the audio streams. The high, low and current values for each stream as well as the stream type, the sender's IP address and port, the receiver's IP address and port, the number of packets lost and the DTMF sequences if present within the stream (RFC 2833 section 3 Named Telephony Events). This sub-view contains two panes.

Metrics Pane

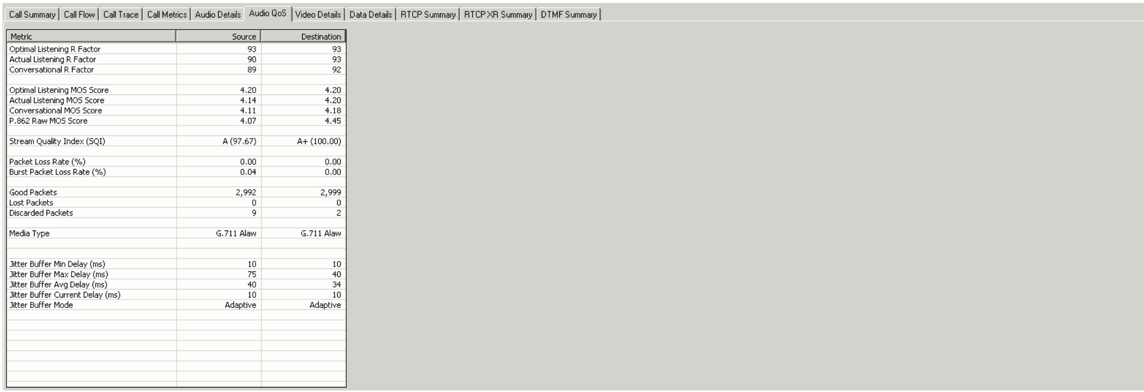
Source Jitter (ms): The average, low, and high jitter measurements calculated for the source audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low source jitter values were calculated.
Destination Jitter (ms): The average, low, and high jitter measurements calculated for the destination audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination jitter values were calculated.
Average Source Packet Interval (ms): The average, low, and high inter-arrival time of packets on the source audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low source packet interval values were calculated.

Average Destination Packet Interval (ms): The average, low, and high inter-arrival time of packets on the destination audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination packet interval values were calculated.
Average Source Bandwidth: The average, low, and high bandwidth, in kilobits per second, calculated for the source audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low source bandwidth values were calculated.
Average Destination Bandwidth: The average, low, and high bandwidth, in kilobits per second, calculated for the destination audio stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination bandwidth values were calculated.

Parameters Pane

Address: The IP addresses for the source and destination channels.
Port: The port numbers for the source and destination channels.
Media Type: The codec type for the source and destination channels.
SSRC: The synchronization source for the source and destination channels.
Audio/Packet (ms): The length of audio time contained in each packet for the source and destination channels.
Frames/Packet: The number of audio frames contained in each packet for the source and destination channels.
Total Packets: The number of packets counted for the source and destination channels.
Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received for the source and destination channels.
Early Packets: The number of packets considered early as configured on the Edit Menu **|** Settings **|** Advanced Tab for the source and destination channels.
Late Packets: The number of packets considered late as configured on the Edit Menu **|** Settings **|** Advanced Tab for the source and destination channels.
DTMF Events: The value of the DTMF digits (RFC 2833) for the source and destination channels.
Current Bandwidth (kb/s): The bandwidth, in kilobits per second, calculated during the last second for the source and destination channels.
Longest Packet Loss Burst: The count of the longest sequence of lost packets for the source and destination channels.
Total Payload Bytes: The number of bytes in the payload portion of the packet for the source and destination channels.

Audio QoS



Metric	Source	Destination
Optimal Listening R Factor	93	93
Actual Listening R Factor	90	93
Conversational R Factor	89	92
Optimal Listening MOS Score	4.20	4.20
Actual Listening MOS Score	4.14	4.20
Conversational MOS Score	4.11	4.18
P.862 Raw MOS Score	4.07	4.45
Stream Quality Index (SQI)	A (97.67)	A+ (100.00)
Packet Loss Rate (%)	0.00	0.00
Burst Packet Loss Rate (%)	0.04	0.00
Good Packets	2,992	2,999
Lost Packets	0	0
Discarded Packets	9	2
Media Type	G.711 Alaw	G.711 Alaw
Jitter Buffer Min Delay (ms)	10	10
Jitter Buffer Max Delay (ms)	75	40
Jitter Buffer Avg Delay (ms)	40	34
Jitter Buffer Current Delay (ms)	10	10
Jitter Buffer Mode	Adaptive	Adaptive

This sub-view provides the QoS metrics for each stream. The R-factor/MOS scoring feature is a non-intrusive measurement technique available for the WinEyeQ call monitor. WinEyeQ passively measures the characteristics of live VoIP calls and reports quality scores in real-time. The algorithm used to obtain the R-Factor/MOS quality scores accurately models the way that time-varying impairments, most notably burst packet loss and possible jitter buffer discards, affect perceived speech quality. This sub-view contains a single pane.

Metrics Pane

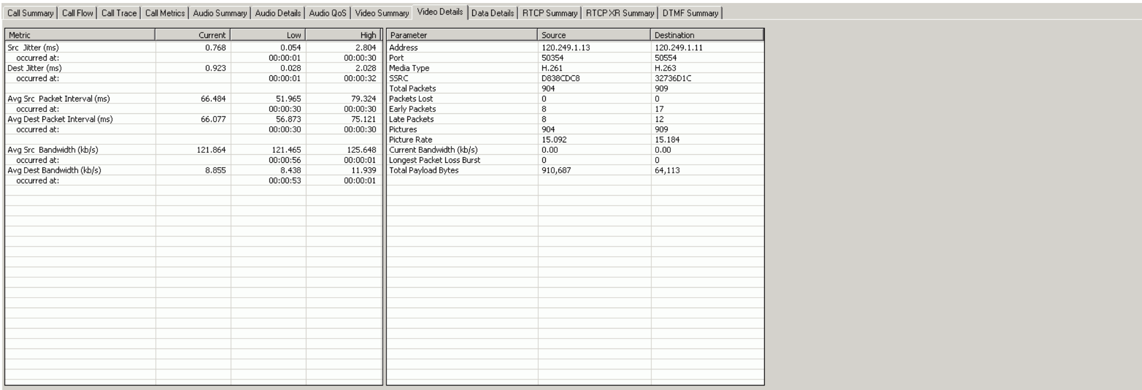
Optimal Listening R Factor: The highest score that is attainable for this codec.
Actual Listening R Factor: The current value of the Listening R Factor for the source and destination audio streams.
Conversational R Factor: The current value of the Conversational R Factor for the source and destination audio streams.
Optimal Listening MOS Score: The highest score that is attainable for this codec.
Actual Listening MOS Score: The current value of the Listening MOS Score for the source and destination audio streams.
Conversational MOS Score: The current value of the Conversational MOS Score for the source and destination audio streams.
P.862 Raw MOS Score: The current value of the P.862 Raw MOS Score for the source and destination audio streams.
Stream Quality Index: The ratio of the current R Factor and MOS score to there optimal values.
Packet Loss Rate (%): The total number packets that were lost divided by the total number of packets that were received.
Burst Packet Loss Rate (%): The packet loss rate encountered for burst conditions for the source and destination audio streams.

Good Packets: The number of packets received for the source and destination audio streams.
Lost Packets: The number of network lost packets for the source and destination audio streams.
Discarded Packets: The number of discarded packets due to excessive delay or extremely early arrival detected for the source and destination audio streams.
Media Type: The codec type for the source and destination audio streams.
Jitter Buffer Minimum Delay (ms): The minimum jitter buffer emulator delay in milliseconds occurring during a call for the source and destination audio streams.
Jitter Buffer Maximum Delay (ms): The maximum jitter buffer emulator delay in milliseconds occurring during a call for the source and destination audio streams.
Jitter Buffer Average Delay (ms): The average jitter buffer emulator delay in milliseconds occurring during a call for the source and destination audio streams.
Jitter Buffer Current Delay (ms): The current jitter buffer emulator delay in milliseconds for the source and destination audio streams.
Jitter Buffer Mode: The type of jitter buffer (adaptive of fixer) being used for the source and destination audio streams. This is configured on the Edit Menu **|** Settings **|** QoS Tab.

The quality scores for MOS range from 0 to 4.5 and the R factor measurements range from 0 to 105 depending on codec type. The guidelines for interpreting the R-factor and MOS scores are shown in the table below for the G.711 codec:

Desirability Scale	**R-factor Range**	**MOS Range**
Desirable	94 - 80	4.4 - 4.0
Acceptable	80 - 70	4.0 - 3.6
Reach Connection	70 - 50	3.6 - 2.6
Not recommended	50 - 0	2.6 - 0

Video Details



Metric	Current	Low	High
Src Jitter (ms)	0.768	0.054	2.804
occurred at:		00:00:01	00:00:30
Dest Jitter (ms)	0.923	0.028	2.028
occurred at:		00:00:01	00:00:32
Avg Src Packet Interval (ms)	66.484	51.965	79.324
occurred at:		00:00:30	00:00:30
Avg Dest Packet Interval (ms)	66.077	56.873	75.121
occurred at:		00:00:30	00:00:30
Avg Src Bandwidth (kb/s)	121.864	121.465	125.648
occurred at:		00:00:56	00:00:01
Avg Dest Bandwidth (kb/s)	8.855	8.438	11.939
occurred at:		00:00:53	00:00:01

Parameter	Source	Destination
Address	120.249.1.13	120.249.1.11
Port	50354	50554
Media Type	H.261	H.263
SSRC	D838CDC8	32736D1C
Total Packets	904	909
Packets Lost	0	0
Early Packets	8	17
Late Packets	8	12
Pictures	904	909
Picture Rate	15.092	15.184
Current Bandwidth (kb/s)	0.00	0.00
Longest Packet Loss Burst	0	0
Total Payload Bytes	910,687	64,113

This sub-view provides summary information including jitter and interval measurements for the video streams. The measurements include high, low, and current values for each stream. As well as the stream type, the sender's IP address and port number, the receiver's IP address and port number, the packets lost, the number of pictures detected, and the picture rate. This sub-view contains two panes.

Metrics Pane

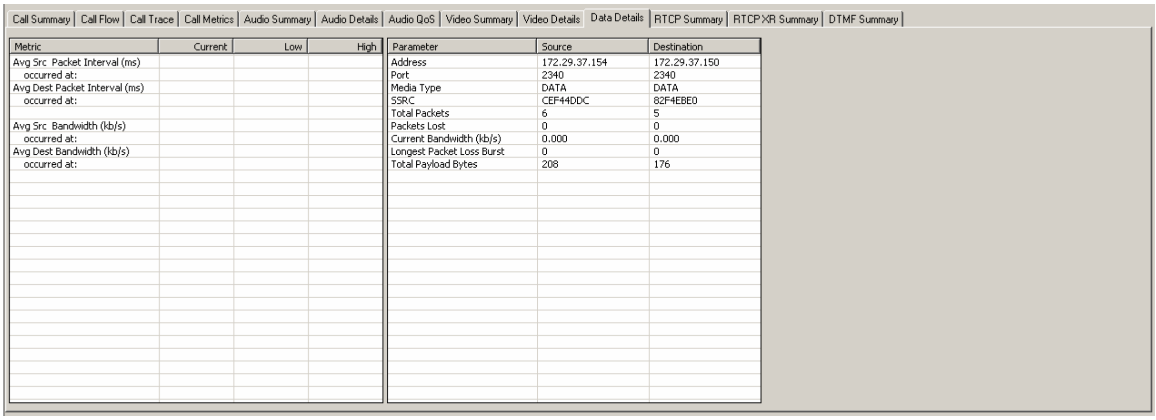
<u>Source Jitter (ms)</u>: The average, low, and high jitter measurements calculated for the source video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low source jitter values were calculated.
<u>Destination Jitter (ms)</u>: The average, low, and high jitter measurements calculated for the destination video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low destination jitter values were calculated.
<u>Average Source Packet Interval (ms)</u>: The average, low, and high inter-arrival time of packets on the source video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low source packet interval values were calculated.
<u>Average Destination Packet Interval (ms)</u>: The average, low, and high inter-arrival time of packets on the destination video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low destination packet interval values were calculated.
<u>Average Source Bandwidth</u>: The average, low, and high bandwidth, in kilobits per second, calculated for the source video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low source bandwidth values were calculated.

Average Destination Bandwidth: The average, low, and high bandwidth, in kilobits per second, calculated for the destination video stream.
Occurred at:: The time, relative to the start of the call, that the high and low destination bandwidth values were calculated.

Parameters Pane

Address: The IP addresses for the source and destination channels.
Port: The port numbers for the source and destination channels.
Media Type: The codec type for the source and destination channels.
SSRC: The synchronization source for the source and destination channels.
Total Packets: The number of packets counted for the source and destination channels.
Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received for the source and destination channels.
Early Packets: The number of packets considered early as configured on the Edit Menu **|** Settings **|** Advanced Tab for the source and destination channels.
Late Packets: The number of packets considered late as configured on the Edit Menu **|** Settings **|** Advanced Tab for the source and destination channels.
Pictures: The number of picture start codes counted for the source and destination channels.
Picture Rate: The number of pictures per second calculated for the source and destination channels.
Current Bandwidth (kb/s): The bandwidth, in kilobits per second, calculated during the last second for the source and destination channels.
Longest Packet Loss Burst: The count of the longest sequence of lost packets for the source and destination channels
Total Payload Bytes: The number of bytes in the payload portion of the packet for the source and destination channels.

Data Details



This sub-view provides summary information including interval measurements for the data streams, the high, low and current values for each stream as well as the stream type, the sender's IP address and port, the receiver's IP address and port, and the number of packets lost. There are two panes on this sub-view.

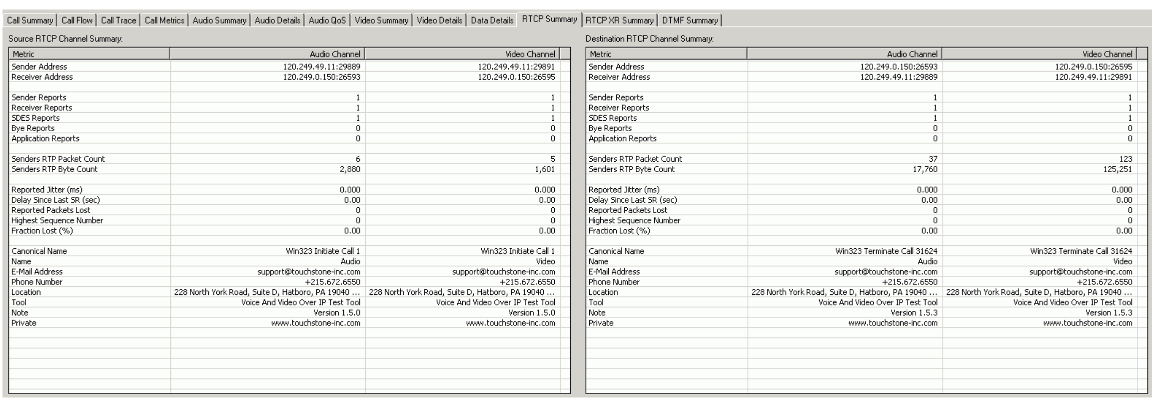
Metrics Pane

<u>Average Source Packet Interval (ms)</u>: The average, low, and high inter-arrival time of packets on the source video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low source packet interval values were calculated.
<u>Average Destination Packet Interval (ms)</u>: The average, low, and high inter-arrival time of packets on the destination video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low destination packet interval values were calculated.
<u>Average Source Bandwidth</u>: The average, low, and high bandwidth, in kilobits per second, calculated for the source video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low source bandwidth values were calculated.
<u>Average Destination Bandwidth</u>: The average, low, and high bandwidth, in kilobits per second, calculated for the destination video stream.
<u>Occurred at</u>:: The time, relative to the start of the call, that the high and low destination bandwidth values were calculated.

Parameters Pane

Address: The IP addresses for the source and destination channels.
Port: The port numbers for the source and destination channels.
Media Type: The codec type for the source and destination channels.
SSRC: The synchronization source for the source and destination channels.
Total Packets: The number of packets counted for the source and destination channels.
Packets Lost: The calculated number of packets lost by subtracting the number of packets expected (using the sequence numbers) minus the number actually received for the source and destination channels.
Current Bandwidth (kb/s): The bandwidth, in kilobits per second, calculated during the last second for the source and destination channels.
Longest Packet Loss Burst: The count of the longest sequence of lost packets for the source and destination channels
Total Payload Bytes: The number of bytes in the payload portion of the packet for the source and destination channels.

RTCP Summary



Source RTCP Channel Summary:

Metric	Audio Channel	Video Channel
Sender Address	120.249.49.11:29889	120.249.49.11:29891
Receiver Address	120.249.0.150:26593	120.249.0.150:26595
Sender Reports	1	1
Receiver Reports	1	1
SDES Reports	1	1
Bye Reports	0	0
Application Reports	0	0
Senders RTP Packet Count	6	5
Senders RTP Byte Count	2,880	1,601
Reported Jitter (ms)	0.000	0.000
Delay Since Last SR (sec)	0.00	0.00
Reported Packets Lost	0	0
Highest Sequence Number	0	0
Fraction Lost (%)	0.00	0.00
Canonical Name	Win323 Initiate Call 1	Win323 Initiate Call 1
Name	Audio	Video
E-Mail Address	support@touchstone-inc.com	support@touchstone-inc.com
Phone Number	+215.672.6550	+215.672.6550
Location	228 North York Road, Suite D, Hatboro, PA 19040 ...	228 North York Road, Suite D, Hatboro, PA 19040 ...
Tool	Voice And Video Over IP Test Tool	Voice And Video Over IP Test Tool
Note	Version 1.5.0	Version 1.5.0
Private	www.touchstone-inc.com	www.touchstone-inc.com

Destination RTCP Channel Summary:

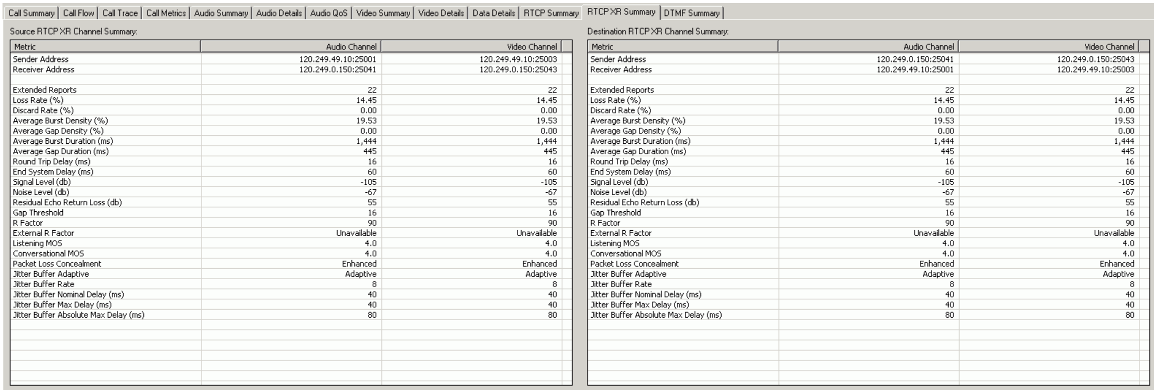
Metric	Audio Channel	Video Channel
Sender Address	120.249.0.150:26593	120.249.0.150:26595
Receiver Address	120.249.49.11:29889	120.249.49.11:29891
Sender Reports	1	1
Receiver Reports	1	1
SDES Reports	1	1
Bye Reports	0	0
Application Reports	0	0
Senders RTP Packet Count	37	123
Senders RTP Byte Count	17,760	125,251
Reported Jitter (ms)	0.000	0.000
Delay Since Last SR (sec)	0.00	0.00
Reported Packets Lost	0	0
Highest Sequence Number	0	0
Fraction Lost (%)	0.00	0.00
Canonical Name	Win323 Terminate Call 31624	Win323 Terminate Call 31624
Name	Audio	Video
E-Mail Address	support@touchstone-inc.com	support@touchstone-inc.com
Phone Number	+215.672.6550	+215.672.6550
Location	228 North York Road, Suite D, Hatboro, PA 19040 ...	228 North York Road, Suite D, Hatboro, PA 19040 ...
Tool	Voice And Video Over IP Test Tool	Voice And Video Over IP Test Tool
Note	Version 1.5.3	Version 1.5.3
Private	www.touchstone-inc.com	www.touchstone-inc.com

This sub-view provides summary information that has been gathered from the RTCP packets that WinEyeQ has analyzed for the audio and video streams that have been sent by both endpoints of the call. This sub-view has two panes that are identical except for source and destination.

RTCP Channel Summary Pane

Sender Address: The IP address and port number of the sending RTCP channel.
Receiver Address: The IP address and port number of the receiving RTCP channel.
Sender Reports: The number of RTCP Sender Reports sent.
Receiver Reports: The number of RTCP Receiver Reports sent.
SDES: The number of RTCP SDES Reports sent.
Bye Reports: The number of RTCP Bye Reports sent.
Application Reports: The number of RTCP Application Reports sent.
Senders Packet Count: The total number of RTP data packets transmitted by the sender since starting transmission.
Senders Byte Count: The total number of payload octets transmitted in RTP data packets by the sender since starting transmission.
Reported Jitter (ms): The jitter measurement calculated on the stream being received from the other endpoint.
Delay Since Last SR (sec): The delay, expressed in units of 1/65536 seconds, between receiving the last SR packet from the remote endpoint and sending this reception report block.
Reported Packets Lost: The total number of RTP data packets from the remote endpoint that have been lost since the beginning of reception.
Highest Sequence Number: The low 16 bits contain the highest sequence number received in an RTP data packet from the remote endpoint, and the most significant 16 bits extend that sequence number with the corresponding count of sequence number cycles.
Fraction Lost (%): The fraction of RTP data packets from the remote endpoint lost since the previous SR or RR packet was sent, expressed as a fixed point number with the binary point at the left edge of the field.
Canonical Name: A unique end-point identifier.
Name: The real name used to describe the source.
E-Mail Address: The email address is formatted according to RFC 2822.
Phone Number: The phone number (should be formatted with the plus sign replacing the international access code).
Location: The geographic user location.
Tool: The application or tool name.
Note: This is intended for transient messages describing the current state of the source.
Private: This item is used to define experimental or application-specific extensions.

RTCP XR Summary



Source RTCP XR Channel Summary:

Metric	Audio Channel	Video Channel
Sender Address	120.249.49.10:25001	120.249.49.10:25003
Receiver Address	120.249.0.150:25041	120.249.0.150:25043
Extended Reports	22	22
Loss Rate (%)	14.45	14.45
Discard Rate (%)	0.00	0.00
Average Burst Density (%)	19.53	19.53
Average Gap Density (%)	0.00	0.00
Average Burst Duration (ms)	1,444	1,444
Average Gap Duration (ms)	445	445
Round Trip Delay (ms)	16	16
End System Delay (ms)	60	60
Signal Level (db)	-105	-105
Noise Level (db)	-67	-67
Residual Echo Return Loss (db)	55	55
Gap Threshold	16	16
R Factor	90	90
External R Factor	Unavailable	Unavailable
Listening MOS	4.0	4.0
Conversational MOS	4.0	4.0
Packet Loss Concealment	Enhanced	Enhanced
Jitter Buffer Adaptive	Adaptive	Adaptive
Jitter Buffer Rate	8	8
Jitter Buffer Nominal Delay (ms)	40	40
Jitter Buffer Max Delay (ms)	40	40
Jitter Buffer Absolute Max Delay (ms)	80	80

Destination RTCP XR Channel Summary:

Metric	Audio Channel	Video Channel
Sender Address	120.249.0.150:25041	120.249.0.150:25043
Receiver Address	120.249.49.10:25001	120.249.49.10:25003
Extended Reports	22	22
Loss Rate (%)	14.45	14.45
Discard Rate (%)	0.00	0.00
Average Burst Density (%)	19.53	19.53
Average Gap Density (%)	0.00	0.00
Average Burst Duration (ms)	1,444	1,444
Average Gap Duration (ms)	445	445
Round Trip Delay (ms)	16	16
End System Delay (ms)	60	60
Signal Level (db)	-105	-105
Noise Level (db)	-67	-67
Residual Echo Return Loss (db)	55	55
Gap Threshold	16	16
R Factor	90	90
External R Factor	Unavailable	Unavailable
Listening MOS	4.0	4.0
Conversational MOS	4.0	4.0
Packet Loss Concealment	Enhanced	Enhanced
Jitter Buffer Adaptive	Adaptive	Adaptive
Jitter Buffer Rate	8	8
Jitter Buffer Nominal Delay (ms)	40	40
Jitter Buffer Max Delay (ms)	40	40
Jitter Buffer Absolute Max Delay (ms)	80	80

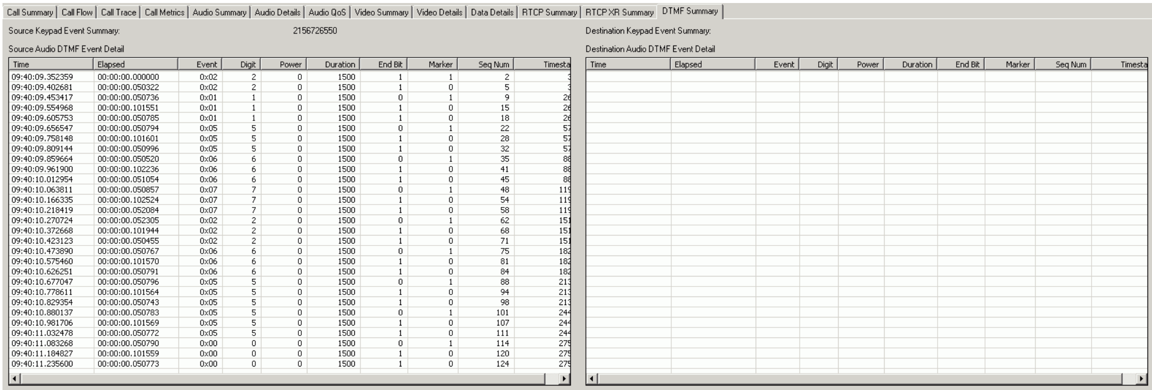
This sub-view provides summary information that has been gathered from the RTCP XR packets that WinEyeQ has analyzed for the audio and video streams that have been sent by both endpoints of the call. This sub-view has two panes that are identical.

RTCP XR Channel Summary

Sender Address: The IP address and port number of the sending RTCP channel.
Receiver Address: The IP address and port number of the receiving RTCP channel.
Extended Reports: The number of RTCP Extended Reports sent.
Loss Rate (%): The fraction of packets lost since the beginning of the call.
Discard Rate (%): The fraction of packets discarded since the beginning of the call.
Average Burst Density (%): The fraction of packets within burst periods since the beginning of the call.
Average Gap Density (%): The fraction of packets within gap periods since the beginning of the call.
Average Burst Duration (ms): The mean duration, in milliseconds, of the burst periods since the beginning of the call.
Average Gap Duration (ms): The mean duration, in milliseconds, of the gap periods since the beginning of the call.
Round Trip Delay (ms): The most recently calculated round-trip delay, in milliseconds.
End System Delay (ms): The most recently estimated end system delay, in milliseconds.

Signal Level (db): The relative speech signal level expressed as the ratio of the signal level to a 0 dBm0 reference.
Noise Level (db): The relative silence period noise level expressed as the ratio of the background noise level to a 0 dBm0 reference.
Residual Echo Return Loss (db): The residual echo return loss as the sum of the measured echo return loss (ERL) and the echo return loss enhanced (ERLE) of the echo canceller, expressed in dB.
Gap Threshold: The gap threshold, in packets.
R Factor: The voice quality metric for the call channel as measured in the monitored network segment.
External R Factor: The voice quality metric for the call channel as measured in an external monitored network segment.
Listening MOS: The estimated mean opinion listening quality score for the call channel.
Conversational MOS: The estimated mean opinion conversational quality score for the call channel.
Packet Loss Concealment: The packet loss concealment capabilities.
Jitter Buffer Adaptive: Adaptive or non-adaptive.
Jitter Buffer Rate: This represents the implementation specific adjustment rate of a jitter buffer in adaptive mode.
Jitter Buffer Nominal Delay (ms): The current nominal jitter buffer delay, in milliseconds.
Jitter Buffer Max Delay (ms): The maximum jitter buffer delay, in milliseconds, recorded for the call.
Jitter Buffer Absolute Max Delay (ms): The absolute maximum delay, in milliseconds, the jitter buffer can ever introduce to the call channel packet stream.

DTMF Summary



Call Summary | Call Flow | Call Trace | Call Metrics | Audio Summary | Audio Details | Audio QoS | Video Summary | Video Details | Data Details | RTCP Summary | RTCP XR Summary | DTMF Summary

Source Keypad Event Summary: 2156726550

Source Audio DTMF Event Detail

Time	Elapsed	Event	Digit	Power	Duration	End Bit	Marker	Seq Num	Timesta
09:40:09.352359	00:00:00.000000	0x02	2	0	1500	1	1	2	3
09:40:09.402681	00:00:00.050322	0x02	2	0	1500	1	0	5	3
09:40:09.453417	00:00:00.050736	0x01	1	0	1500	0	1	9	26
09:40:09.554968	00:00:00.101551	0x01	1	0	1500	1	0	15	26
09:40:09.605753	00:00:00.050785	0x01	1	0	1500	1	0	18	26
09:40:09.656547	00:00:00.050794	0x05	5	0	1500	0	1	22	57
09:40:09.758148	00:00:00.101601	0x05	5	0	1500	1	0	28	57
09:40:09.809144	00:00:00.050996	0x05	5	0	1500	1	0	32	57
09:40:09.859664	00:00:00.050520	0x06	6	0	1500	0	1	35	88
09:40:09.961900	00:00:00.102236	0x06	6	0	1500	1	0	41	88
09:40:10.012954	00:00:00.051054	0x06	6	0	1500	1	0	45	88
09:40:10.063811	00:00:00.050857	0x07	7	0	1500	0	1	48	119
09:40:10.166335	00:00:00.102524	0x07	7	0	1500	1	0	54	119
09:40:10.218419	00:00:00.052084	0x07	7	0	1500	1	0	58	119
09:40:10.270724	00:00:00.052305	0x02	2	0	1500	0	1	62	151
09:40:10.372668	00:00:00.101944	0x02	2	0	1500	1	0	68	151
09:40:10.423123	00:00:00.050455	0x02	2	0	1500	1	0	71	151
09:40:10.473890	00:00:00.050767	0x06	6	0	1500	0	1	75	182
09:40:10.575460	00:00:00.101570	0x06	6	0	1500	1	0	81	182
09:40:10.626251	00:00:00.050791	0x06	6	0	1500	1	0	84	182
09:40:10.677047	00:00:00.050796	0x05	5	0	1500	0	1	88	213
09:40:10.778611	00:00:00.101564	0x05	5	0	1500	1	0	94	213
09:40:10.829354	00:00:00.050743	0x05	5	0	1500	1	0	98	213
09:40:10.880137	00:00:00.050783	0x05	5	0	1500	0	1	101	244
09:40:10.981706	00:00:00.101569	0x05	5	0	1500	1	0	107	244
09:40:11.032478	00:00:00.050772	0x05	5	0	1500	1	0	111	244
09:40:11.083268	00:00:00.050790	0x00	0	0	1500	0	1	114	275
09:40:11.184827	00:00:00.101559	0x00	0	0	1500	1	0	120	275
09:40:11.235600	00:00:00.050773	0x00	0	0	1500	1	0	124	275

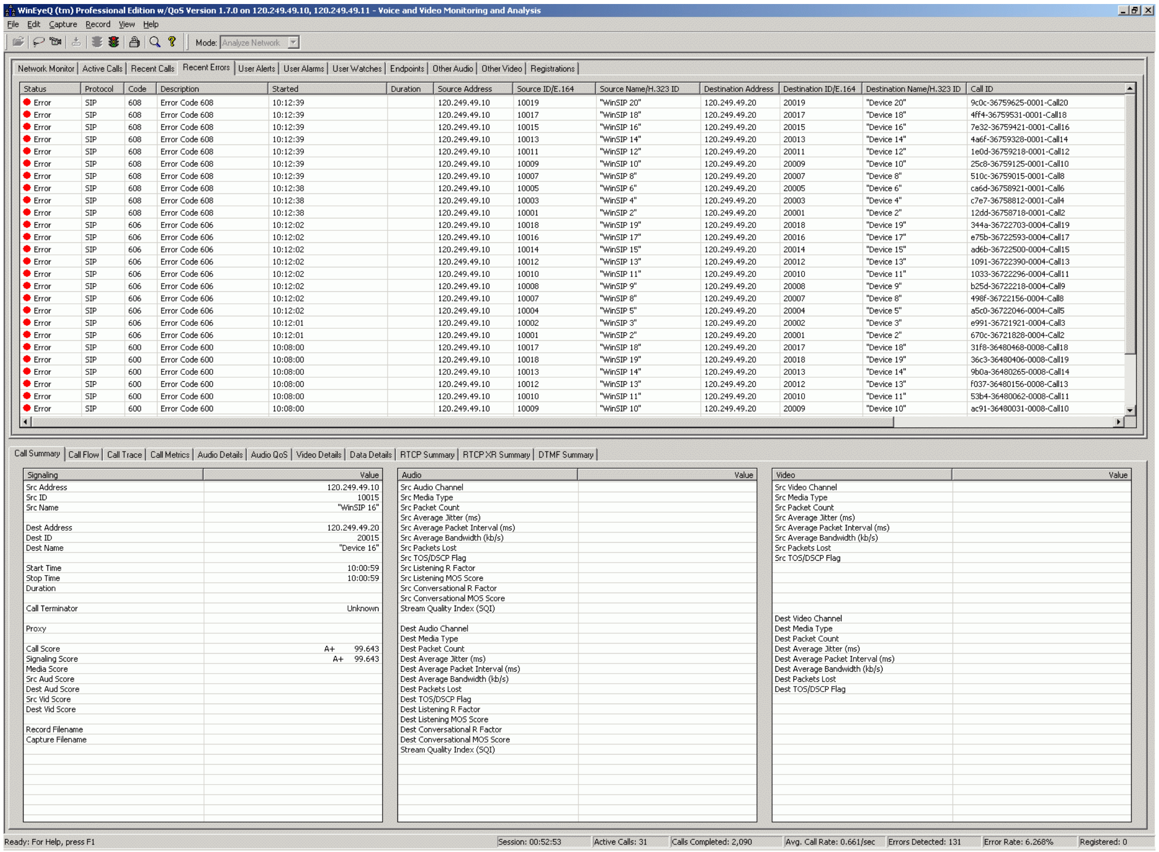
Destination Keypad Event Summary:

Destination Audio DTMF Event Detail

Time	Elapsed	Event	Digit	Power	Duration	End Bit	Marker	Seq Num	Timesta

This sub-view provides a detailed and organized tabular display for the active DTMF transmissions that occur during a call for both the source and destination side of the calls.

Recent Errors View



The recent errors view is designed to provide an in-depth view of each VoIP call for which an error was detected. Each call is represented by an entry, which is updated once every second, in the topmost report. This report contains the following columns:

Status: The current status of the call. These may be things such as connecting, ringing, connected, error, etc.

Protocol: The values for this field are SIP or H.323.

Code: The numeric code for this error (if applicable).

Description: A text description of this error.

Started: This is the time (local time) that the call was started.

Duration: The length of time the call is (or was) active.

Source Address: The address of the call initiator (caller).

Source ID/E.164: The SIP user ID or H.323 E.164 alias of the caller.

Source Name/H.323 ID: The SIP display name or H.323 ID of the caller.

Destination Address: The address of the call receiver (party called).

Destination ID/E.164: The SIP user ID or H.323 E.164 alias of the party called.

Destination Name/H.323 ID: The SIP display name or H.323 ID of the party called.

Call ID: The SIP or H.323 call ID associated with this call.

Registered With: The gatekeeper's IP address, for H.323 calls, or the Proxy's IP address, for SIP calls.

Conference ID: The conference ID (H.323 calls only).

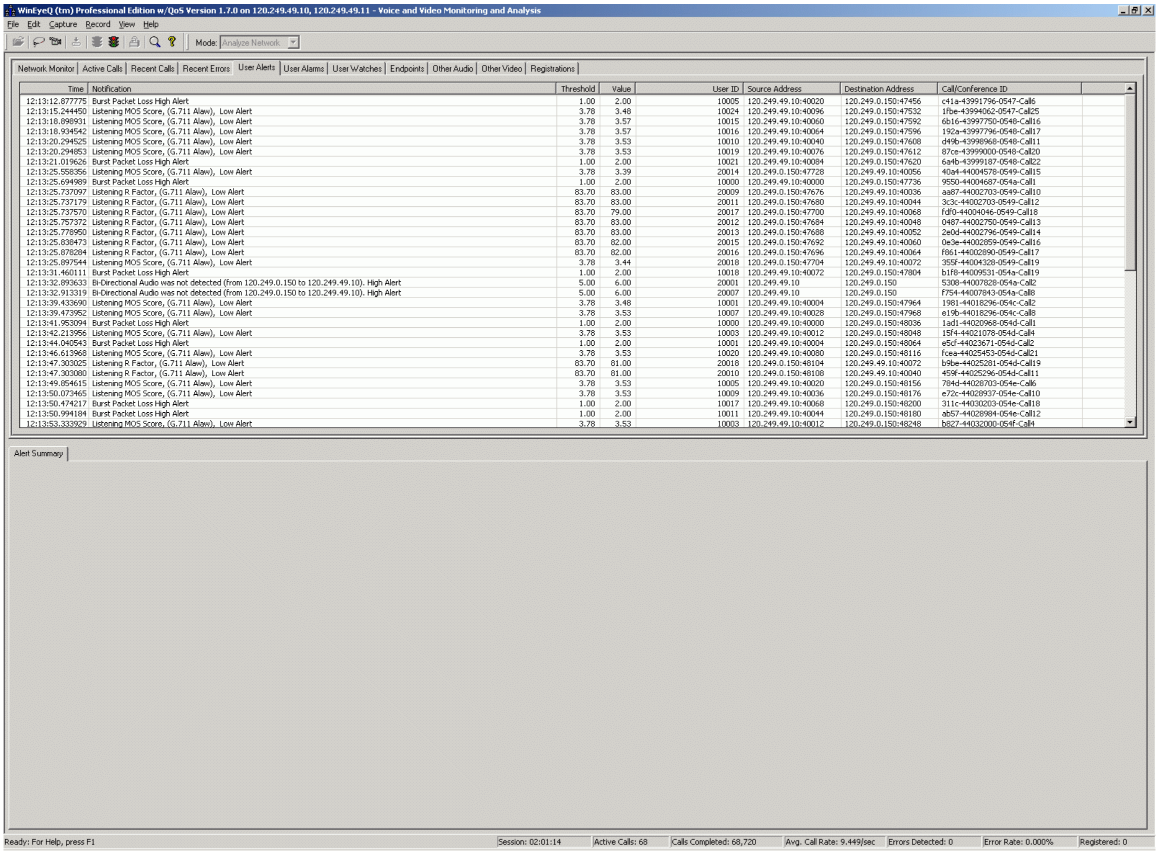
Each individual call has the following sub-views.

- Call Summary
- Call Flow (ladder diagram)
- Call Trace
- Call Metrics
- Audio Details
- Audio QoS
- Video Details
- Data Details
- RTCP Summary
- RTCP XR Summary
- DTMF Summary

To display information about a particular call, select it (click the call line) in the call list. Whenever a call is selected, it will remain "locked" in the view for as long as you wish to view its details.

Note: For a detailed description of these sub-views please refer back to the 'Recent Calls View' section of the manual.

User Alerts View



This view provides an active list of the alerts that have occurred during the test session. The notification list for the events that triggered the alerts is displayed in tabular form. Each alert is represented by an entry in the topmost report. This report contains the following columns:

Time: This is the time the Alert was detected.

Notification: An explanation of the Alert.

Threshold: The threshold value set by the user.

Value: The value that triggered the Alert

User ID: The SIP user ID or H.323 alias of the caller.

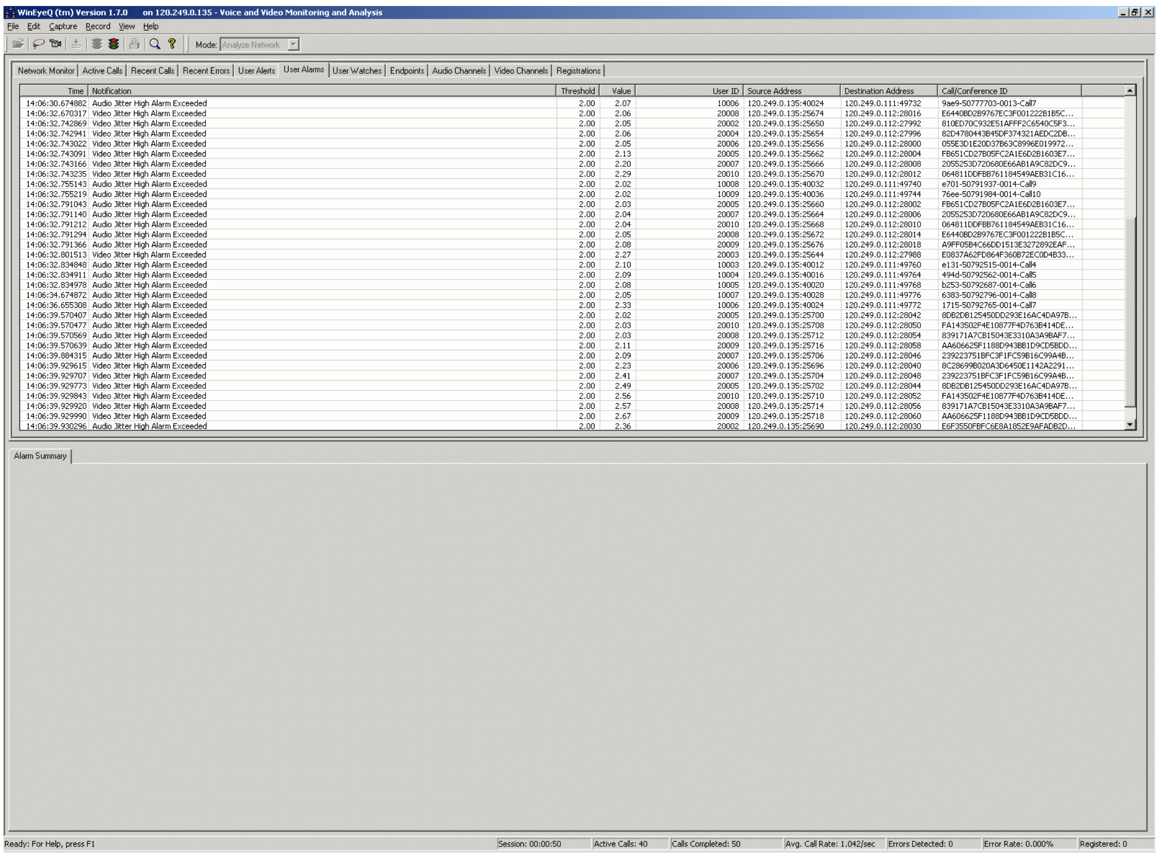
Source Address: The address of the call initiator (caller).

Destination Address: The address of the call receiver (party called).

Call/Conference ID: The SIP or H.323 call ID associated with this call.

Various alert thresholds are set by the user for audio/video jitter, interval, packet loss, and R-Factor/MOS score measurements

User Alarms View



This view provides an active list of the alarms that have occurred during the test session. The notification list for the events that triggered the alarms is displayed in tabular form. Each alert is represented by an entry in the topmost report. This report contains the following columns:

Time: This is the time the Alarm was detected.

Notification: An explanation of the Alarm.

Threshold: The threshold value set by the user.

Value: The value that triggered the Alarm

User ID: The SIP user ID or H.323 alias of the caller.

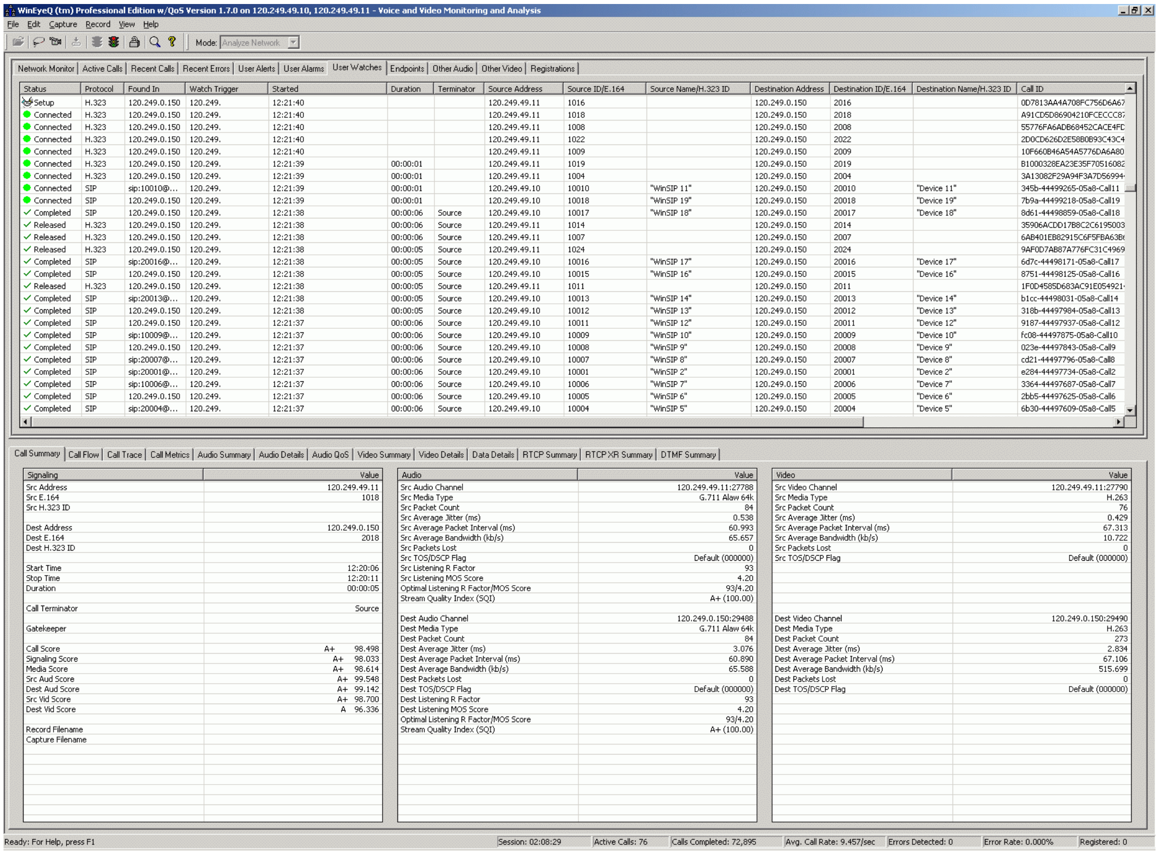
Source Address: The address of the call initiator (caller).

Destination Address: The address of the call receiver (party called).

Call/Conference ID: The SIP or H.323 call ID associated with this call.

Various alarm thresholds are set by the user for audio/video jitter, interval, packet loss, and R-Factor/MOS score measurements

User Watches View



The watch view is designed to provide an in-depth view of each VoIP call and that has been associated with a user-defined "watch" trigger. Each call is represented by an entry, which is updated once every second, in the topmost report. This report contains the following columns:

Call status: The current status of the call. These may be things such as connecting, ringing, connected, error, etc.

Protocol: The values for this field are SIP or H.323.

Found in: This field specifies which call element the value was found in.

Watch trigger: This field specifies what value caused the watch to be triggered.

Started: This is the time (local time) that the call was started.

Duration: The length of time the call is (or was) active.

Terminator: The side that terminated the call (source or destination).

Source Address: The address of the call initiator (caller).

Source ID/E.164: The SIP user ID or H.323 E.164 alias of the caller.

Source Name/H.323 ID: The SIP display name or H.323 ID of the caller.

Destination Address: The address of the call receiver (party called).

Destination ID/E.164: The SIP user ID or H.323 E.164 alias of the party called.

Destination Name/H.323 ID: The SIP display name or H.323 ID of the party called.

Call ID: The SIP or H.323 call ID associated with this call.

Registered With: The gatekeeper's IP address for H.323 calls, or the Proxy's IP address for SIP calls.

Conference ID: The conference ID (H.323 calls only).

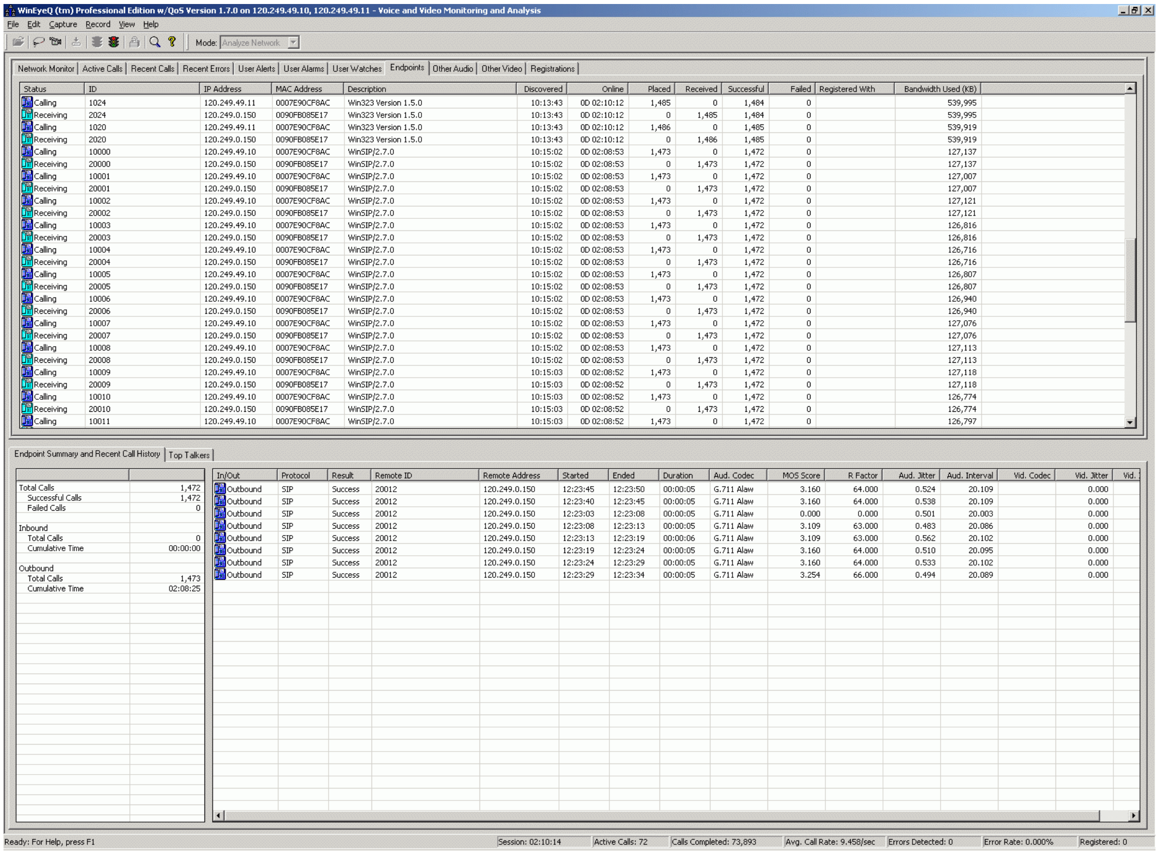
Each individual call has the following sub-views:

- Call Summary
- Call Flow
- Call Trace
- Call Metrics
- Audio Summary
- Audio Details
- Audio QoS
- Video Summary
- Video Details
- Data Details
- RTCP Summary
- RTCP XR Summary
- DTMF Summary

To display information about a particular call, select it in the watch list. Whenever a call is selected, it will remain "locked" in the view for as long as you wish to view its details.

Note: For a detailed description of these sub-views please refer back to the 'Active Calls View' section of the manual.

Endpoints View



The Endpoint View shows a list of each endpoint that has participated in a VoIP call during this WinEyeQ session. This view contains the following columns:

Status: Current status of endpoint, Inactive / Calling / Receiving.

ID: The E.164 alias of the endpoint (H.323) or Call ID (SIP)

IP Address: The IP address of the endpoint.

MAC Address: The MAC address of the endpoint.

Description: A readable text description (if available) of the endpoint.

Discovered: This is the time this endpoint was first observed by WinEyeQ.

Online: The length of time this endpoint has been online.

Placed: The number of calls this endpoint has placed.

Received: The number of calls this endpoint has received.

Successful: The number of calls for this endpoint without errors.

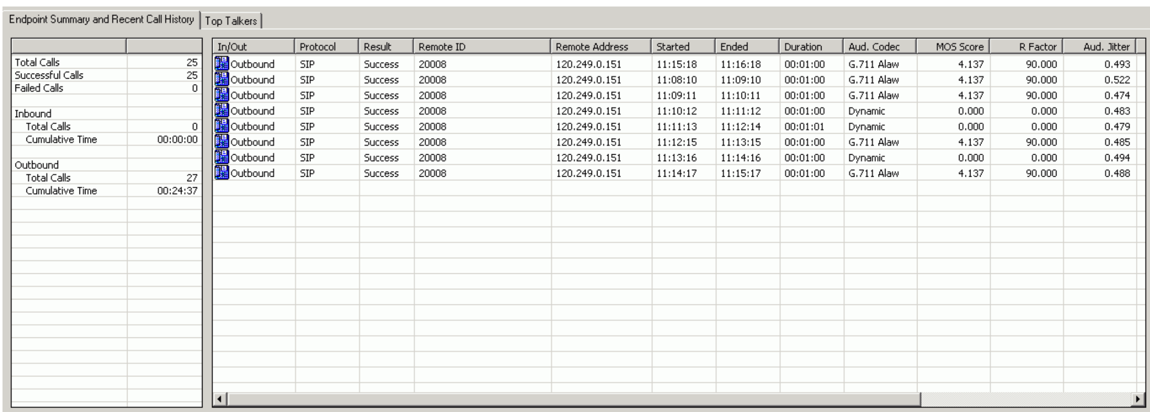
Failed: The number of calls for this endpoint with errors.

Registered With: The gatekeeper's IP address, for H.323 calls, or the Proxy's IP address, for SIP calls.

Bandwidth Used (KB): How many bytes of data has been transferred.

The number of endpoints in the list is user configurable via Edit | Settings | Endpoints.

Endpoint Summary and Recent Call History



The Endpoint Summary and Recent Call History view keeps a list of each call the endpoint has either placed or received.

This view contains the following columns:

In/Out: Whether the call was placed (Outbound) or received (Inbound).

Protocol: The protocol used for the call (H.323 or SIP).

Result: Either Success or Fail.

Remote ID: The E.164 alias (H.323) or Call ID (SIP) of the other endpoint.

Remote Address: The IP address of the endpoint.

Started: The time the call started.

Ended: The time the call ended.

Duration: The call duration.

Audio CODEC: The type of audio codec this endpoint used.

MOS Score: The average MOS score of this endpoint's audio for the call.

R Factor: The average R Factor of this endpoint's audio for the call.

Audio Jitter: The average jitter of this endpoint's audio for the call.

Audio Interval: The average interval of this endpoint's audio for the call.

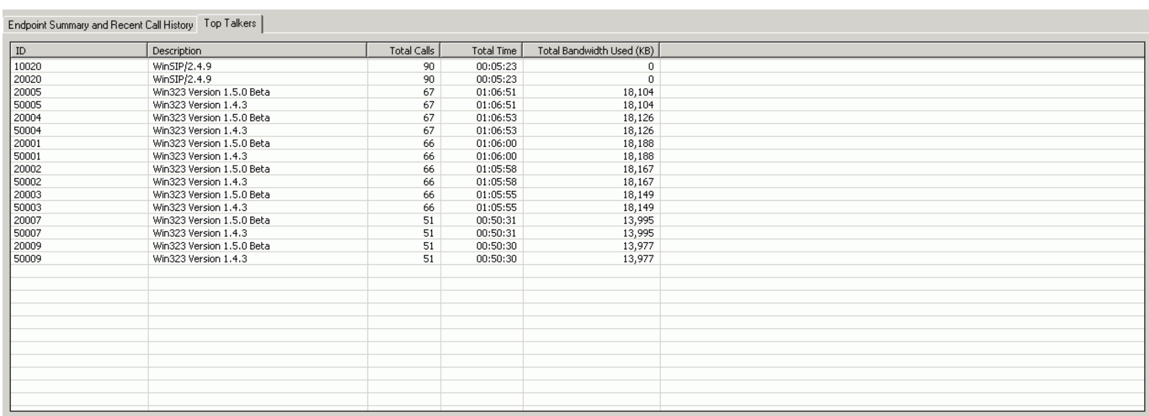
Video CODEC: The type of video codec this endpoint used.

Video Jitter: The average jitter of this endpoint's video for the call.

Video Interval: The average interval of this endpoint's video for the call.

The number of endpoint histories in the list is user configurable via Edit | Settings | Endpoints.

Top Talker


Endpoint Summary and Recent Call History | Top Talkers

ID	Description	Total Calls	Total Time	Total Bandwidth Used (KB)
10020	WinSIP/2.4.9	90	00:05:23	0
20020	WinSIP/2.4.9	90	00:05:23	0
20005	Win323 Version 1.5.0 Beta	67	01:06:51	18,104
50005	Win323 Version 1.4.3	67	01:06:51	18,104
20004	Win323 Version 1.5.0 Beta	67	01:06:53	18,126
50004	Win323 Version 1.4.3	67	01:06:53	18,126
20001	Win323 Version 1.5.0 Beta	66	01:06:00	18,188
50001	Win323 Version 1.4.3	66	01:06:00	18,188
20002	Win323 Version 1.5.0 Beta	66	01:05:58	18,167
50002	Win323 Version 1.4.3	66	01:05:58	18,167
20003	Win323 Version 1.5.0 Beta	66	01:05:55	18,149
50003	Win323 Version 1.4.3	66	01:05:55	18,149
20007	Win323 Version 1.5.0 Beta	51	00:50:31	13,995
50007	Win323 Version 1.4.3	51	00:50:31	13,995
20009	Win323 Version 1.5.0 Beta	51	00:50:30	13,977
50009	Win323 Version 1.4.3	51	00:50:30	13,977

This view contains the following columns:

ID: The E.164 alias of the endpoint (H.323) or Call ID (SIP)

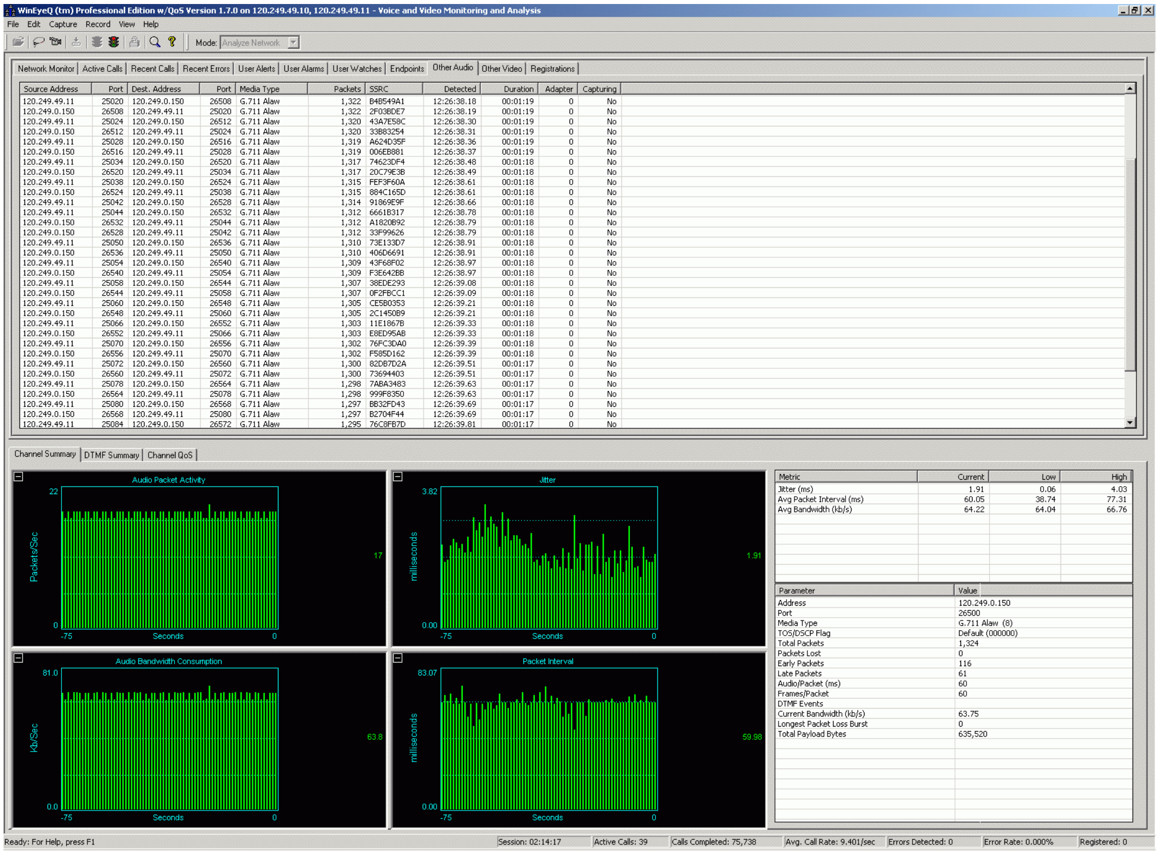
Description: A readable text description (if available) of the endpoint.

Total Calls: The total calls placed and received by this endpoint.

Total Time: The total time the calls lasted.

Total Bandwidth Used (KB): The total bytes transferred.

Other Audio View



This view contains the following columns:

Source Address: The IP address of the call initiator (caller).

Port: The port of the call initiator (caller).

Destination Address: The IP address of the call receiver (party called).

Port: The port of the call receiver (party called).

Media Type: The type of media flowing on this channel.

Packets: The number of packets sent on this channel.

SSRC: The synchronization source from the RTP header.

Detected: The time this stream was detected.

Duration: The length of time the call is (or was) active.

Adapter: The adapter (NIC) that received the packets.

Capturing: Whether or not this stream is being captured to disk.

To start capturing the data from one of these streams right-click the mouse on that stream and select 'Start Rogue Stream Capture'. To stop capturing the data from one of these streams right-click the mouse on that stream and select 'Stop Rogue Stream Capture'.

Other Audio Sub-Views

Channel Summary

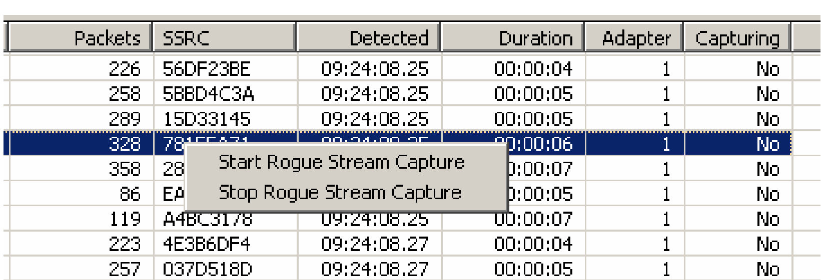
This view provides jitter and latency measurements for an audio stream not identified with a VoIP call. Included with the graphical representations of jitter and latency are the high low and current values for each as well as the stream type, the sender's IP address and port, the receiver's IP address and port, the number of packets lost and the DTMF sequences if present within the stream (RFC 2833 section 3 Named Telephony Events).

DTMF Summary

This sub-view provides a detailed and organized tabular display for the active DTMF transmissions that occurs during an audio stream that was not identified with a VoIP call.

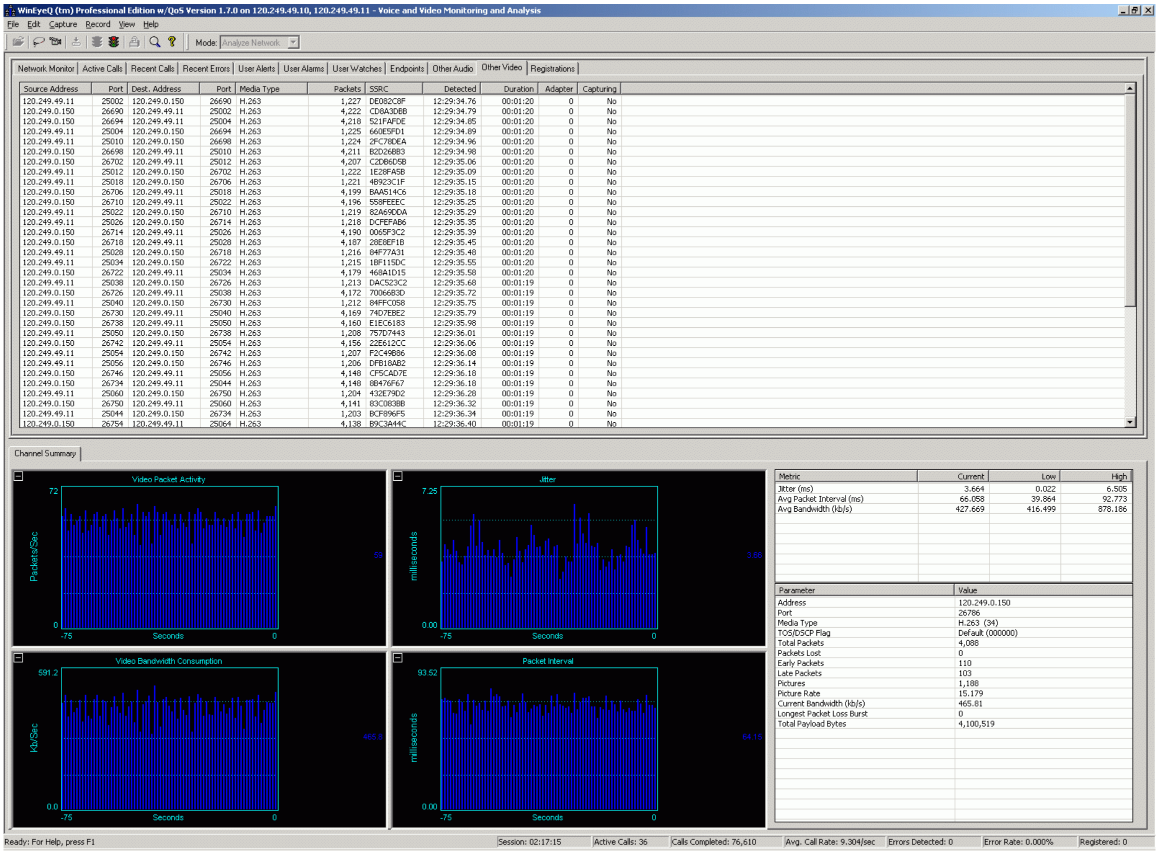
Channel QoS

This sub-view provides the QoS metrics for the stream. The R-factor/MOS scoring feature is a non-intrusive measurement technique available for the WinEyeQ call monitor. WinEyeQ passively measures the characteristics of live audio stream and reports quality scores in real-time. The algorithm used to obtain the R-Factor/MOS quality scores accurately models the way that time-varying impairments, most notably burst packet loss and possible jitter buffer discards, affect perceived speech quality.



The 'Capturing' column reflects the status of the capture.

Other Video View



This view contains the following columns:

Source Address: The IP address of the call initiator (caller).

Port: The port of the call initiator (caller).

Destination Address: The IP address of the call receiver (party called).

Port: The port of the call receiver (party called).

Media Type: The type of media flowing on this channel.

Packets: The number of packets sent on this channel.

SSRC: The synchronization source from the RTP header.

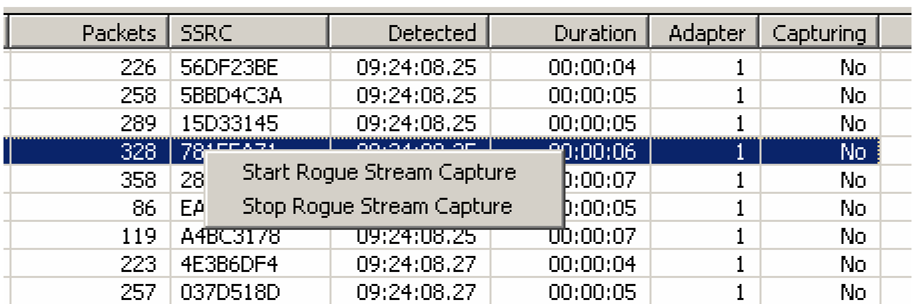
Detected: The time this stream was detected.

Duration: The length of time the call is (or was) active.

Adapter: The adapter (NIC) that received the packets.

Capturing: Whether or not this stream is being captured to disk

To start capturing the data from one of these streams, right-click the mouse on that stream and select 'Start Rogue Stream Capture'. To stop capturing the data from one of these streams, right-click the mouse on that stream and select 'Stop Rogue Stream Capture'.



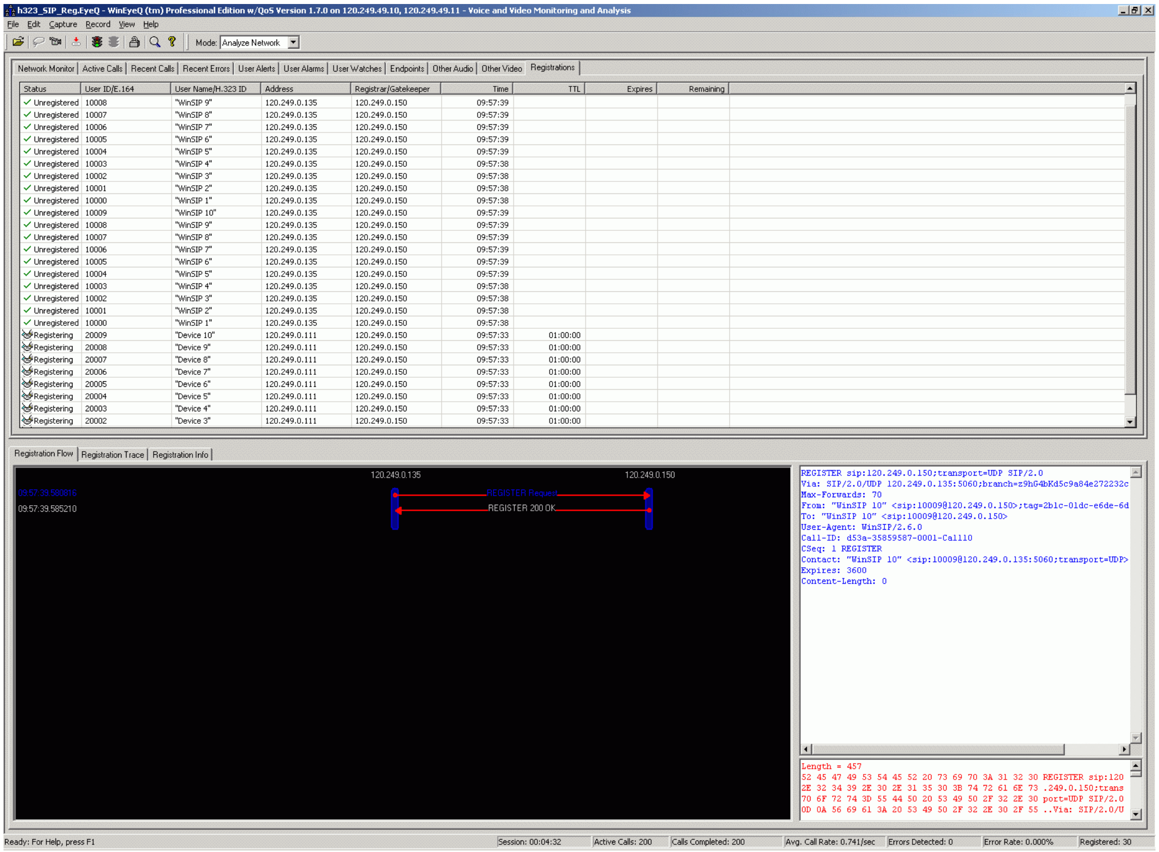
The 'Capturing' column reflects the status of the capture.

Other Video Sub-View

Channel Summary

This view provides jitter and latency measurements for a video stream not identified with a VoIP call. Included with the graphical representations of jitter and latency are the high low and current values for each as well as the stream type, the sender's IP address and port, the receiver's IP address and port, the number of packets lost and the DTMF sequences if present within the stream (RFC 2833 section 3 Named Telephony Events).

Registrations View



The registrations view is designed to provide an in-depth view of each VoIP call registration and its status. Each call is represented by an entry, which is updated once every second, in the topmost report. This report contains the following columns:

<u>Status</u>: The current status of the entry. These may be things such as registering, registered, unregistered, etc.

<u>User ID/E.164</u>: The SIP user ID or H.323 E.164 alias of the registered party.

<u>User Name/H.323 ID</u>: The SIP display name or H.323 ID of the registered party.

<u>Address</u>: The address of the registered party.

<u>Registrar/Gatekeeper</u>: The address of the registrar to which the party is registered.

Time: This is the time of the most recent registration for this party.

TTL: The registration’s time-to-live value.

Expires: The time at which this binding expires.

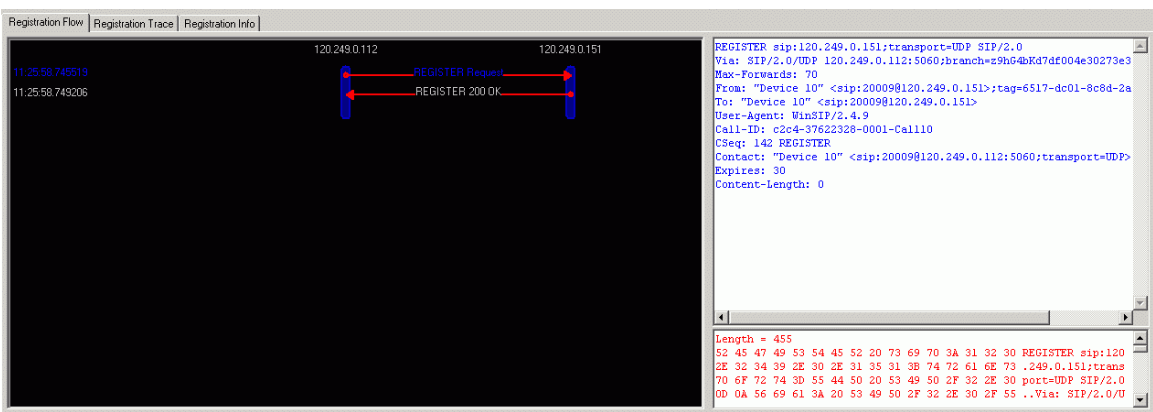
Remaining: The time until this binding expires.

Each individual registration has the following three sub-views:

- Registration Flow
- Registration Trace
- Registration Info

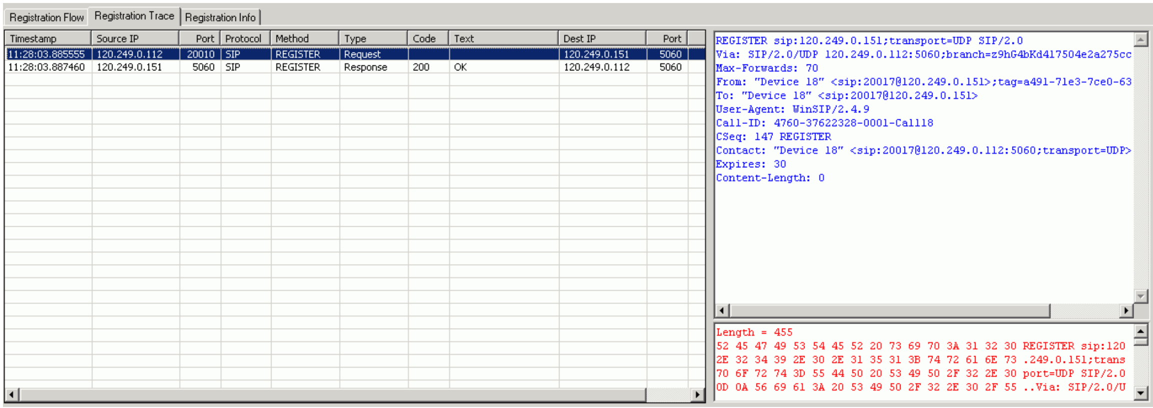
To display information about a particular registration, select it in the registration list. Whenever a registration entry is selected, it will remain “locked” in the view for as long as you wish to view its details.

Registration Flow



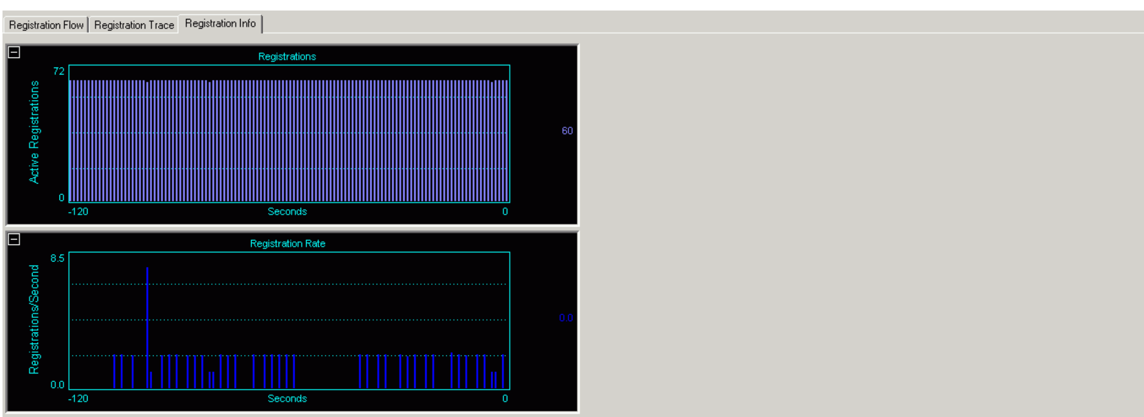
This view provides a time-stamped ladder diagram view of the registration flow. Each “rung” in the ladder may be highlighted to display the decoded packet in both ASCII and hexadecimal representations.

Registration Trace



This view provides a time-stamped protocol specific report view of the registration flow. Each entry in the report may be highlighted to display the decoded packet in both ASCII and hexadecimal representations.

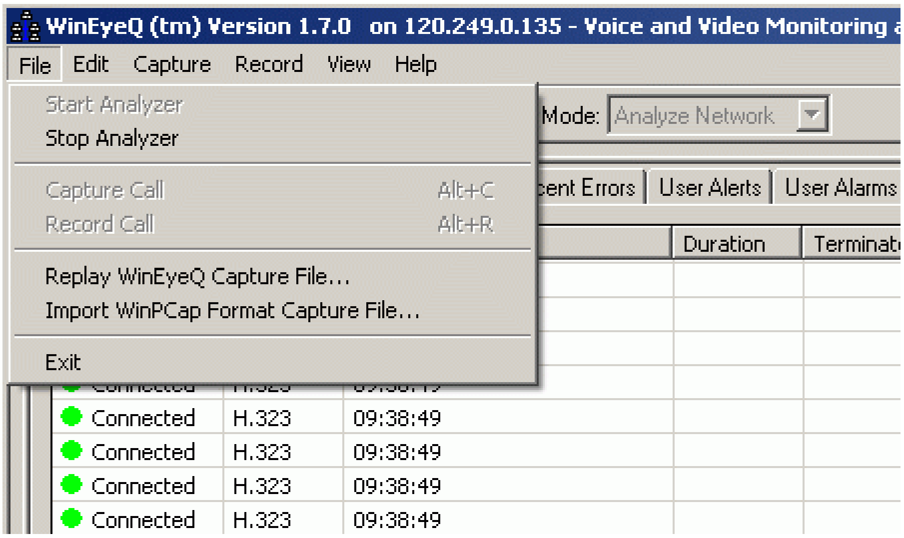
Registration Info



This view provides an overall graphical representation of the number of registrations and the registration rate.

WinEyeQ Menu Commands

File Menu



This menu contains the commands associated with running WinEyeQ.

Start Analyzer: This command starts the analyzer on the currently selected adapter.

Stop Analyzer: This command stops the current analyzer session.

Capture Call: This command is only enabled when a call is in one of the completed states (completed, error, timeout, etc.). When enabled, this command will capture the selected call in WinEyeQ's proprietary format to the specified file.

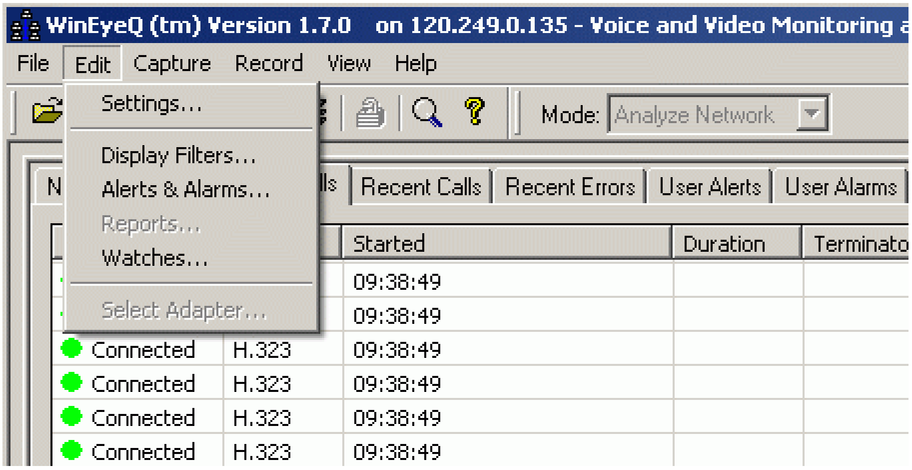
Record Call: This command starts recording the selected call. The signaling and subsequent media will be saved in WinEyeQ's proprietary format to the disk.

Replay WinEyeQ Capture File: This command loads a file captured in WinEyeQ's format and replays it.

Import WinPCap Format Capture File: This command loads a file captured in WinPCap's format and replays it.

Exit: This command ends the WinEyeQ session.

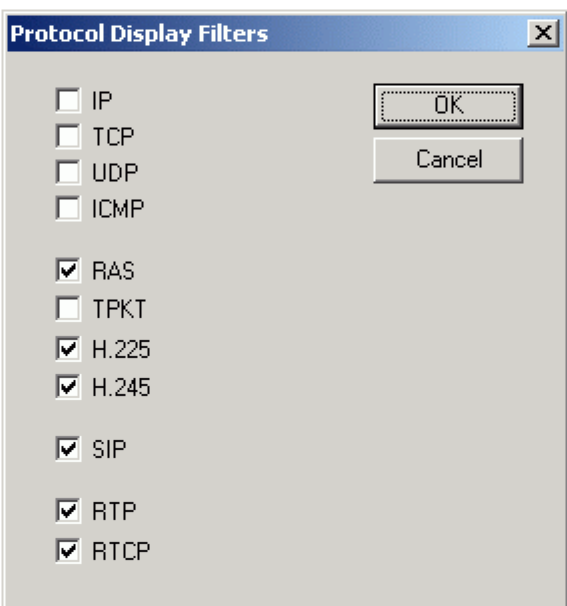
Edit Menu



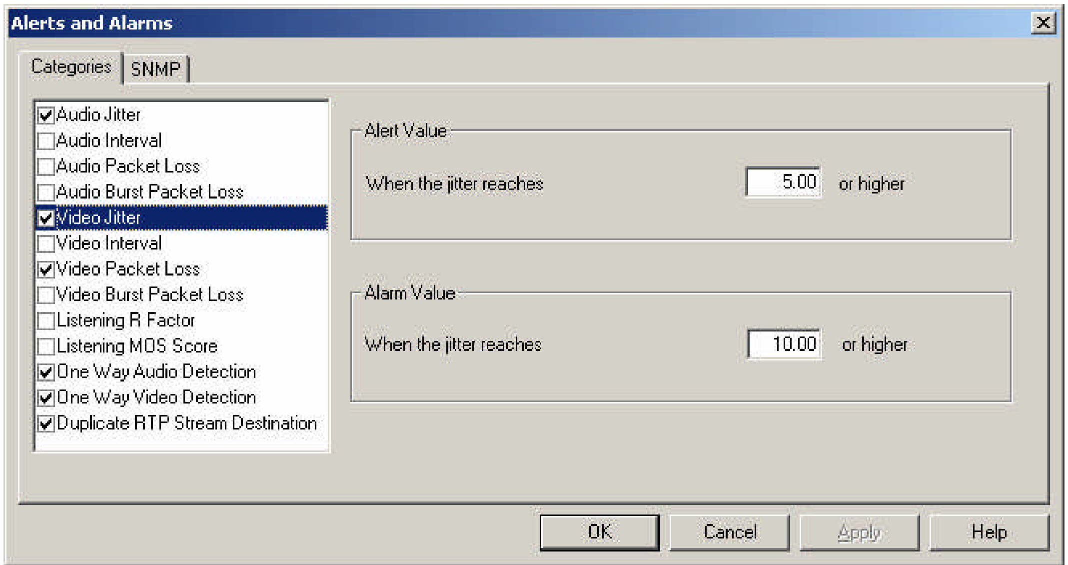
This menu allows you to configure settings, display filters, alerts, alarms, reports, watches, and adapters.

Settings: This command allows you to set the various settings of WinEyeQ so that you can program the tool. See Configuration Settings for a detailed description.

Display Filters: This command allows you to select the protocol displayed.



Alerts and Alarms: This command allows you to set the Alerts and Alarms that WinEyeQ uses.



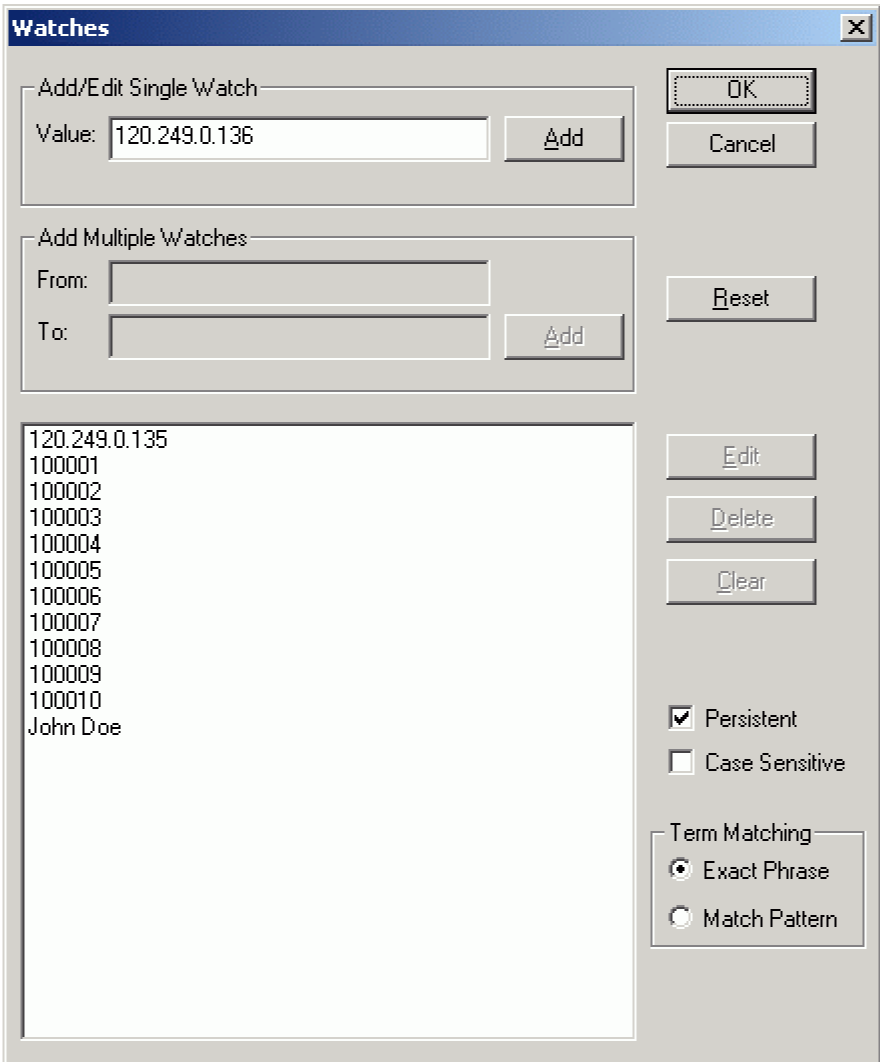
The categories of alerts and alarms are:

- Audio Jitter
- Audio Interval
- Audio Packet Loss
- Audio Burst Packet Loss
- Video Jitter
- Video Interval
- Video Packet Loss
- Video Burst Packet Loss
- Listening R Factor
- Listening MOS Score
- One Way Audio Detection
- One Way Video Detection
- Duplicate RTP Stream Detection

Note: For expanded information on Alerts and Alarms, along with SNMP settings see the Alerts and Alarms section of this manual.

Reports: This command allows you to set logging, call, report and preferences settings. See Configuration Settings for a detailed description.

Watches: From this menu you can add single or multiple watches to WinEyeQ. Watches are a stimulus that triggers WinEyeQ to isolate and analyze any VoIP call that contains that watch. Watches are an extremely simple but powerful way of sifting through a 'haystack' of calls to find the 'needle' call that you are looking for. Calls that are found this way are added to the Watch View.



Add/Edit Single Watch: This is where a watch value is entered. This value can represent any field of any protocol message that WinEyeQ examines. WinEyeQ currently examines the following message fields:

- Source MAC Address, Destination MAC Address
- Source IP Address, Destination IP Address
- Call ID, Conference ID
- Source URI, Destination URI

- Registrar address, Gatekeeper address
- Source User ID, Destination User ID
- Source E.164, Destination E.164, Source H.323 ID, Destination H.323 ID
- Calling Party Number, Called Party Number
- Call Reference Value, Q.931 Display Name

All the user must do is to add the text string of the value of the field he is looking for.

Note: No quotes are needed for strings that contain blanks.

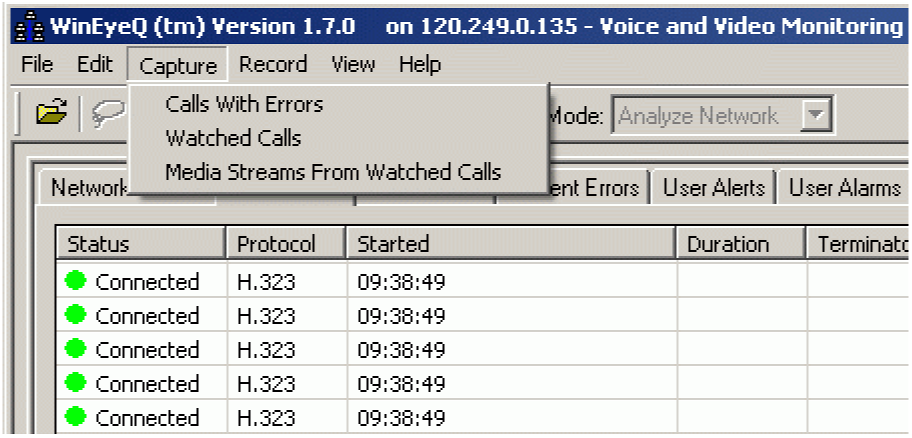
Add Multiple Watches: This is where a range of watches can be added to the program, instead of adding each value separately.

Persistent: If persistent is selected, the watches that have been entered will be written to a file and reloaded the next time that WinEyeQ is run. Otherwise they will be discarded when the program terminates.

Case Sensitive: If case sensitive is selected, the case (upper / lower) of alphabetic characters is considered in the compare. If case sensitive is true then the string "Joe" is not equal "joe".

Term Matching: Exact Phrase or Match Pattern. This offers the user a 'wild card' method of comparing strings. For example, if you add "192.168.10." and have selected Exact Phrase', all fields examined must contain that string exactly. If you have selected Pattern Match, any field that contains "***192.168.10.***" (where * can be any character) will match.

Capture Menu



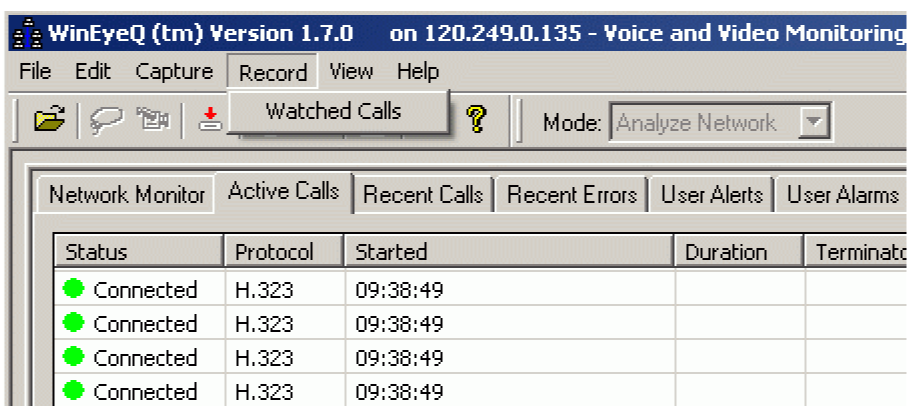
This menu toggles on and off the various capture options.

<u>Calls with errors</u>: Enables/disables capturing calls with errors.

<u>Watched calls</u>: Enables/disables capturing watched calls.

<u>Media streams from watched calls</u>: Enables/disables capturing media streams from the watched calls.

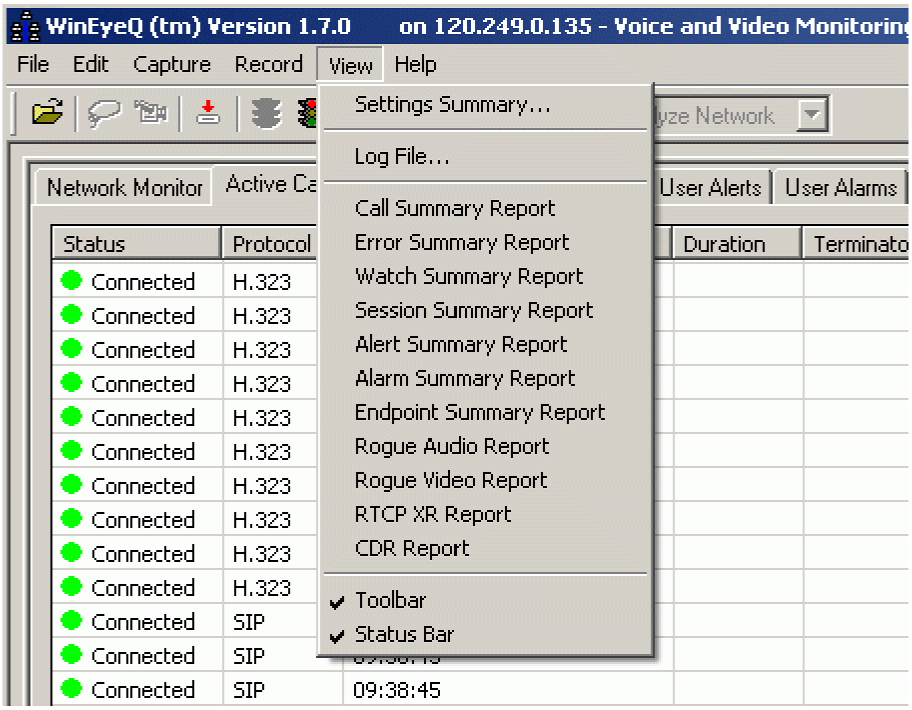
Record Menu



This menu toggles on and off the various record options.

<u>Watched Calls</u>: Enables/disables recording watched calls.

View Menu



This menu allows you to view the settings summary, text based log file and the various reports that are available. It also allows the user to hide the toolbars and status bars.

Settings Summary: Shows the active settings for WinEyeQ.

Log File: Text based data file of the results from the previous test.

Call Summary Report: The call summary report provides a single line entry for each call. Summary information including start time, end time, duration, ID's, addresses, packet counts, QoS metrics, etc. are displayed for each line item.

Error Summary Report: Shows the errors that have occurred during the test session.

Watch Summary Report: Shows the summary information that pertains only to the calls in the watch list.

Session Summary Report: Shows the high level summary information about the test session.

<u>Alert Summary Report</u>: Shows the active alert messages, programmed threshold and measured values.

<u>Alarm Summary Report</u>: Shows the active alarm messages, programmed threshold and measured values.

<u>Endpoint Summary Report</u>: This report contains the information that is removed from the Endpoint View when the number of endpoints in the view exceeds the number of endpoints the user has elected to observe (via Edit | Settings | Endpoints).

<u>Rogue Audio Summary</u>: This report details the start time, end time, duration, QoS measurements, etc. of audio streams that WinEyeQ has detected that are not associated with any VoIP call.

<u>Rogue Video Summary</u>: This report details the start time, end time, duration, QoS measurements, etc. of audio streams that WinEyeQ has detected that are not associated with any VoIP call.

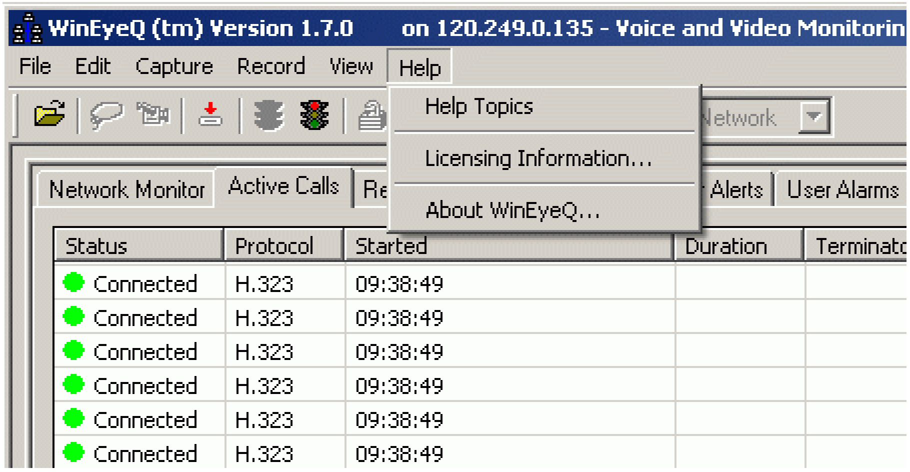
<u>RTCP XR Report</u>: This report captures the information from RTCP XR reports that are sent on the RTCP channel (if any).

<u>CDR Report</u>: Shows the call data records for all the monitored calls.

<u>Toolbar</u>: Shows or hides the toolbar.

<u>Status bar</u>: Shows or hides the status bar.

Help Menu



This menu displays licensing and help information.

Help Topics: Provides user with on line assistance for operating procedures, configuration information and guidance.

Licensing information: Displays information about your WinEyeQ license status. This is also where you can upgrade your license with optional features as they become available.

About WinEyeQ: Displays information about this version of WinEyeQ.

Toolbar Shortcuts

The toolbar contains shortcuts to the most commonly used application commands. The following commands are available:

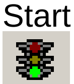
Replay

Capture

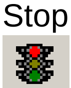
Record

Import WinPCap Capture File

Start Analysis



Stop Analysis

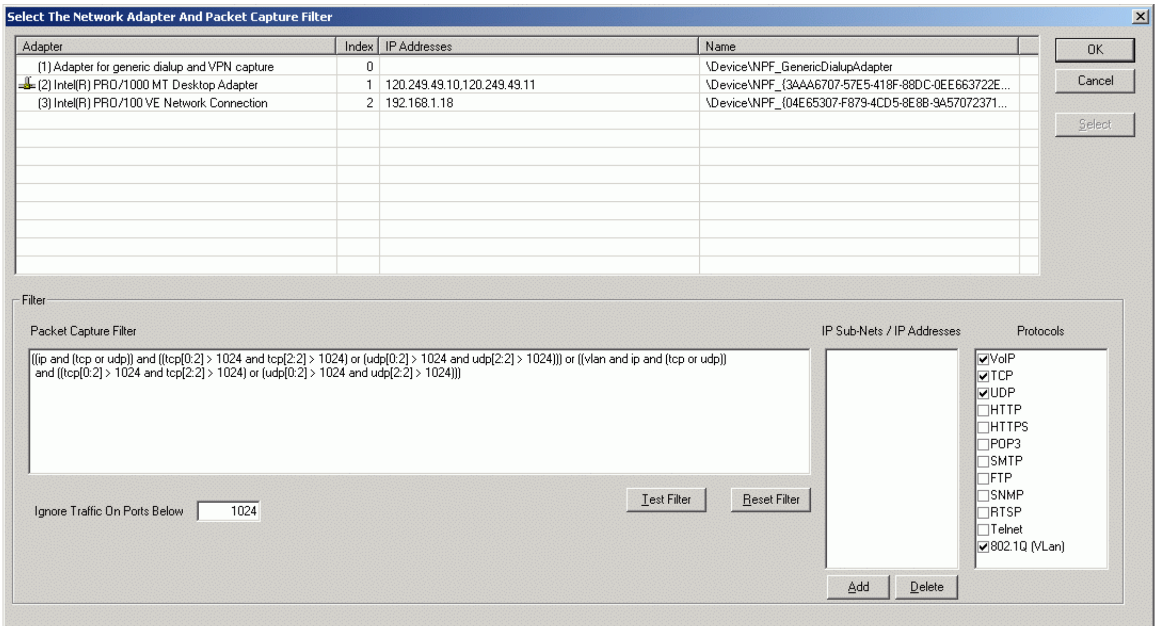


Unlock display (de-select currently selected item)

Manage Watches

Help/About

Selecting the Network Adapter and Packet Capture Filter



The first step in preparing to run WinEyeQ is to select the network adapter you wish to monitor. WinEyeQ will automatically display the Select Adapter screen immediately after starting it for the first time. You may also access this dialog from the Edit | Select Adapter menu item.

The Adapter

On the top part of the screen is a list of the Network Adapters that WinEyeQ has discovered on your PC. Select the adapter you want to monitor by clicking the adapter line and then pressing ‘Select’ or by just double clicking the adapter line.

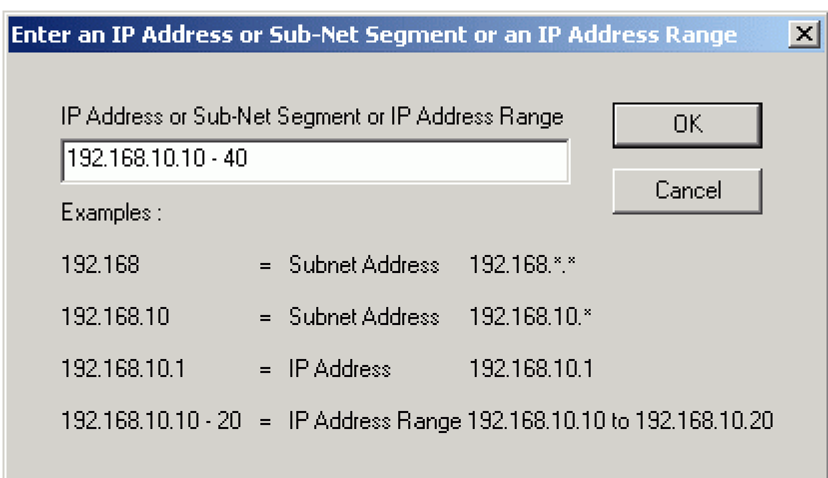
The Filter

The bottom part of the screen is for the Filter. The Filter is used by the network driver (WinPCap) to decide which packets to send to WinEyeQ and which ones to discard. There are four areas that are used set the Filter, The Packet Capture Filter textbox, The Sub-Nets / Addresses textbox, the Protocols box and the Ports textbox.

The Packet Capture Filter textbox is the actual Packet Capture Filter. It has been predefined to capture IP, TCP, and UDP packets from all IP addresses with port numbers greater than 1024 on normal and VLAN networks. You may change the Packet Capture Filter by editing the Filter textbox directly, or in combination with the other three textboxes. In case of an error, simply press the ‘Reset Filter’ button to start over.

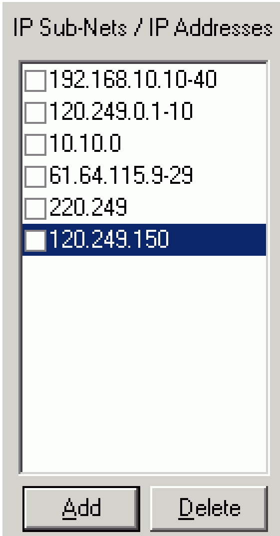
The Sub-Nets / Addresses textbox allows the user to filter on selected IP Addresses or IP Subnets. Subnets / IP Addresses are added or removed from the filter from here.

If you click the 'Add' button, the following dialog is displayed:

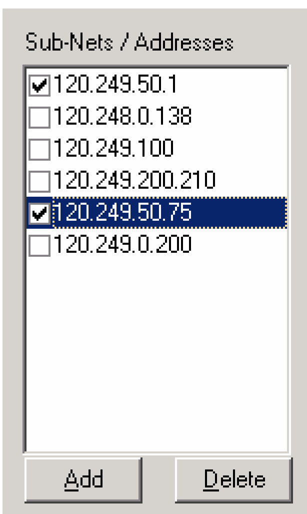


Then enter an IP subnet address, or enter an IP address (or range of addresses), then click OK.

The new value is added to the list.

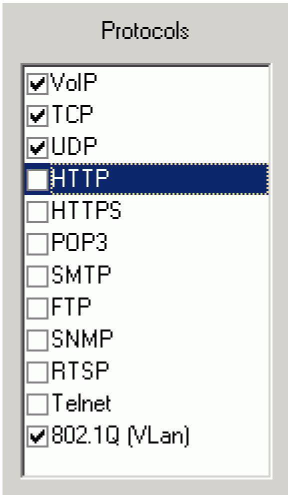


You may the use the check boxes to select / deselect the IP addresses you want WinEyeQ to monitor:



The Subnets / IP Addresses will be added to or removed from the Packet Capture Filter.

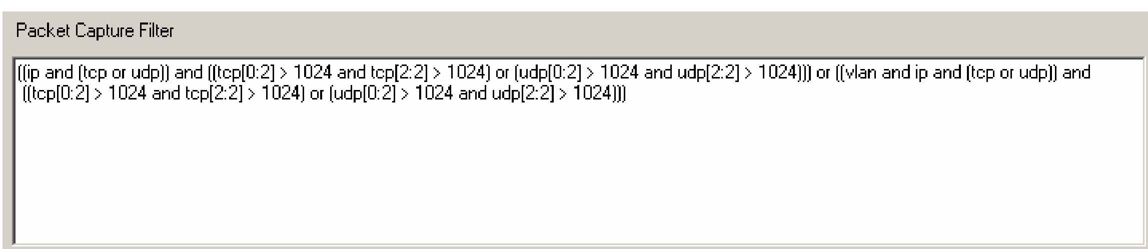
The Protocols textbox allows the user to selectively monitor VoIP and other network protocols.



By checking or un-checking these boxes, the indicated protocols are added or removed from the Packet Capture Filter.

The Ports textbox allows the user to selectively exclude packets from a range of port numbers.

The Packet Capture Filter textbox shows the combination of the Subnet / Addresses textbox, the Protocols textbox and the Ports textbox.



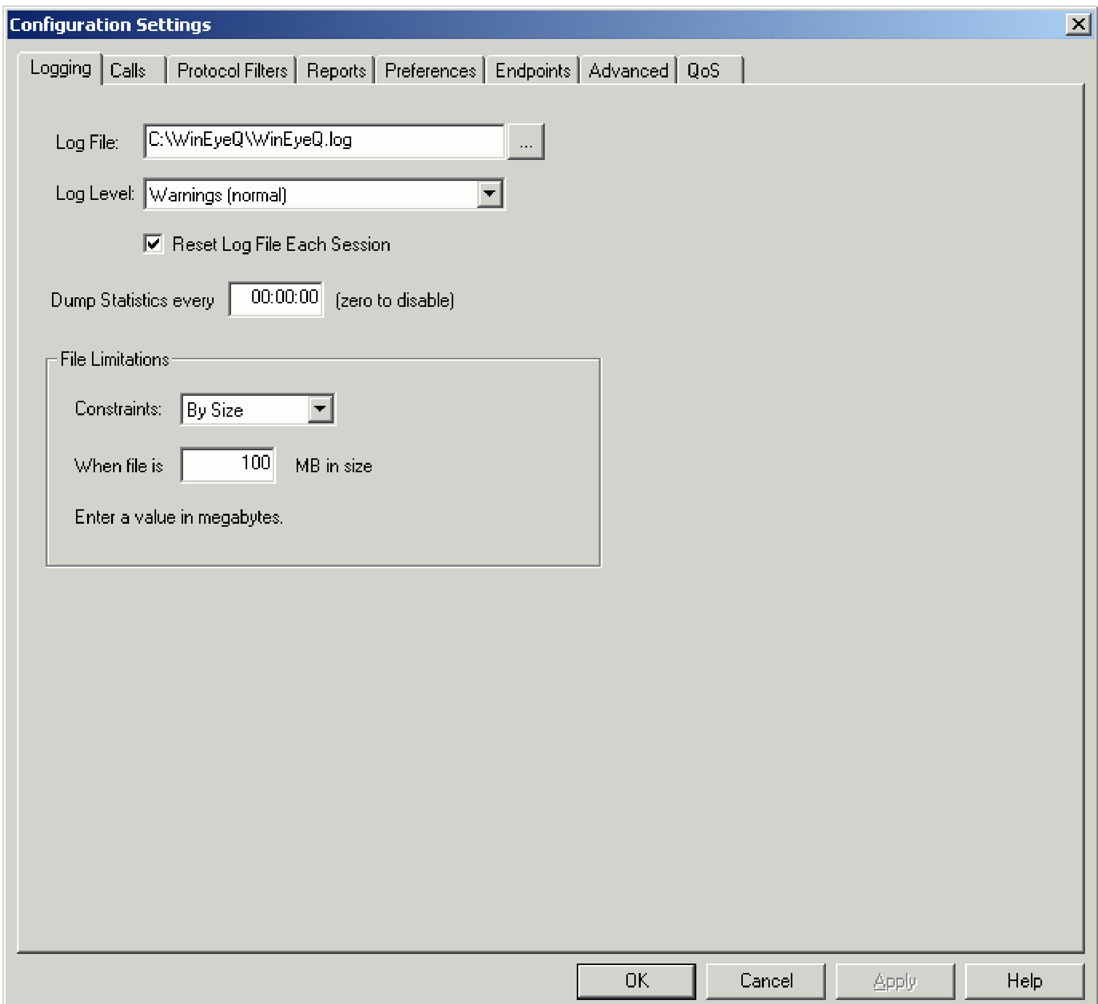
When you make changes to the Subnet /Addresses textbox, the Protocol textbox, or the Ports textbox, the Packet Capture Filter is automatically recalculated. To ensure that the filter has the correct syntax, you may press the Test Filter to check it.

Note: When you press the OK button on the Select Network Adapters dialog, the filter is always checked to ensure it is syntactically correct. If it is not correct, an error message is displayed.

Configuration Settings

The second step in preparing to run WinEyeQ is to review the settings. WinEyeQ will display the following screen(s) when the Edit | Settings menu item is chosen.

Logging



The following options are available to control the application's logging:

Log file: Enter the name and location of the log file you wish to use.

Log level: Select the level of verbosity you wish. The values are:

All: The slowest and most verbose level.
Trace: An extremely high level of detail.
Debug: Standard troubleshooting level.
Information: Medium verbosity.
Warnings: Only warnings and errors.
Errors: Errors messages only.

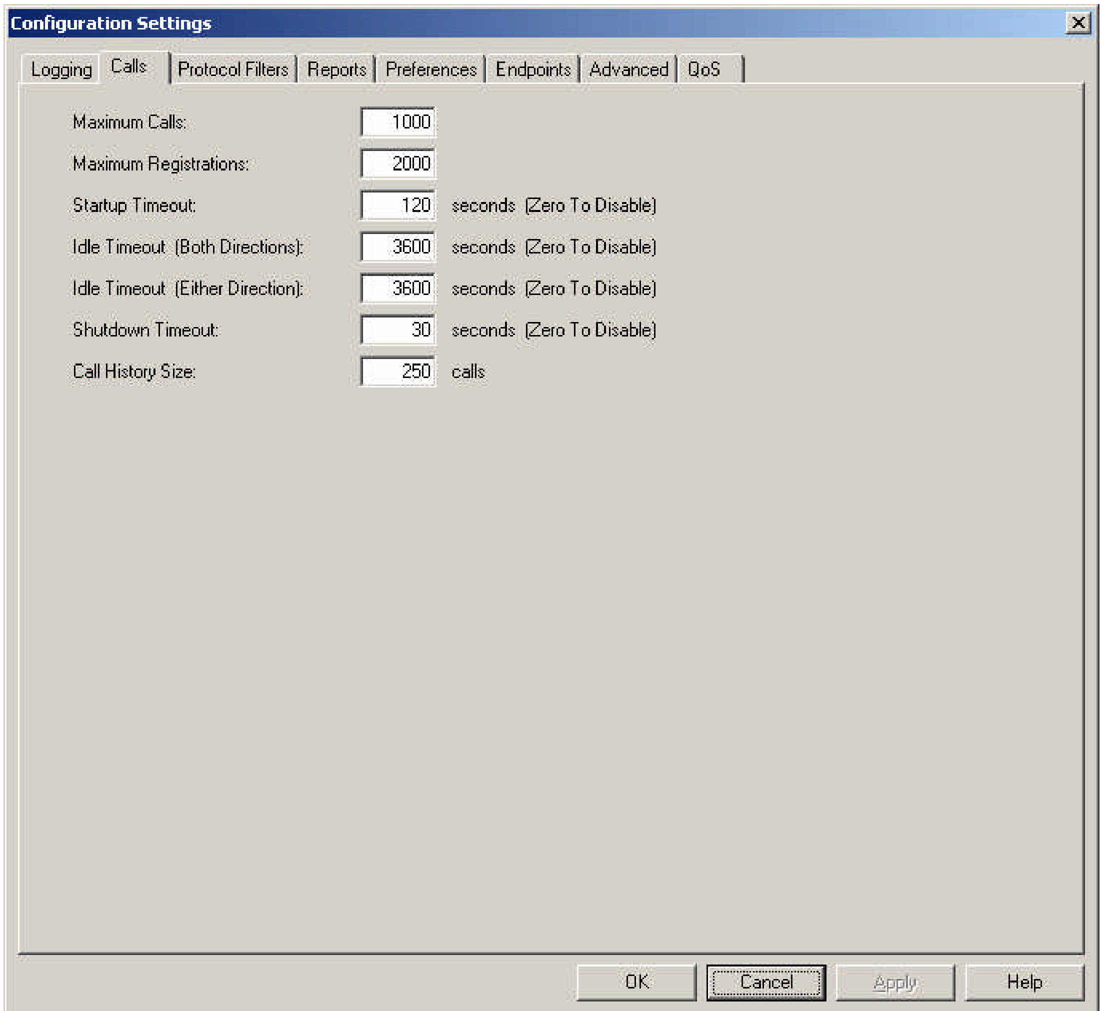
Reset log file each session: This feature keeps the log file constrained by resetting it after each clean exit. If the previous exit was not clean, the contents of the previous session are preserved.

Dump statistics: Sets a timer interval to dump the current statistics to the log file. If this value is zero, the function is disabled.

File Limitations:

Constraints: Sets how the log file is separated. At a certain point the program will close one log file and open a new one and start recording there. The trigger for this event can be set to Size, Interval, Time of Day, or None (which, if selected will hold all information in only one log file).
Constraint Range: Based on the log file constraints, the range sets the event trigger for when the file obtains the value specified in this field.

Calls



The following settings govern the way calls are handled:

Maximum Calls: The maximum number of calls that WinEyeQ will follow (lower values allow for more in-depth media tracing).

Maximum Registrations: The maximum number of registrations that WinEyeQ will follow (lower values allow for more in-depth media tracing).

Startup Timeout: The maximum time after a call is discovered that WinEyeQ will wait for the other endpoint to respond.

Idle Timeout (Both Directions): The maximum time between packets from both the source and destination that WinEyeQ will wait before timing out the call.

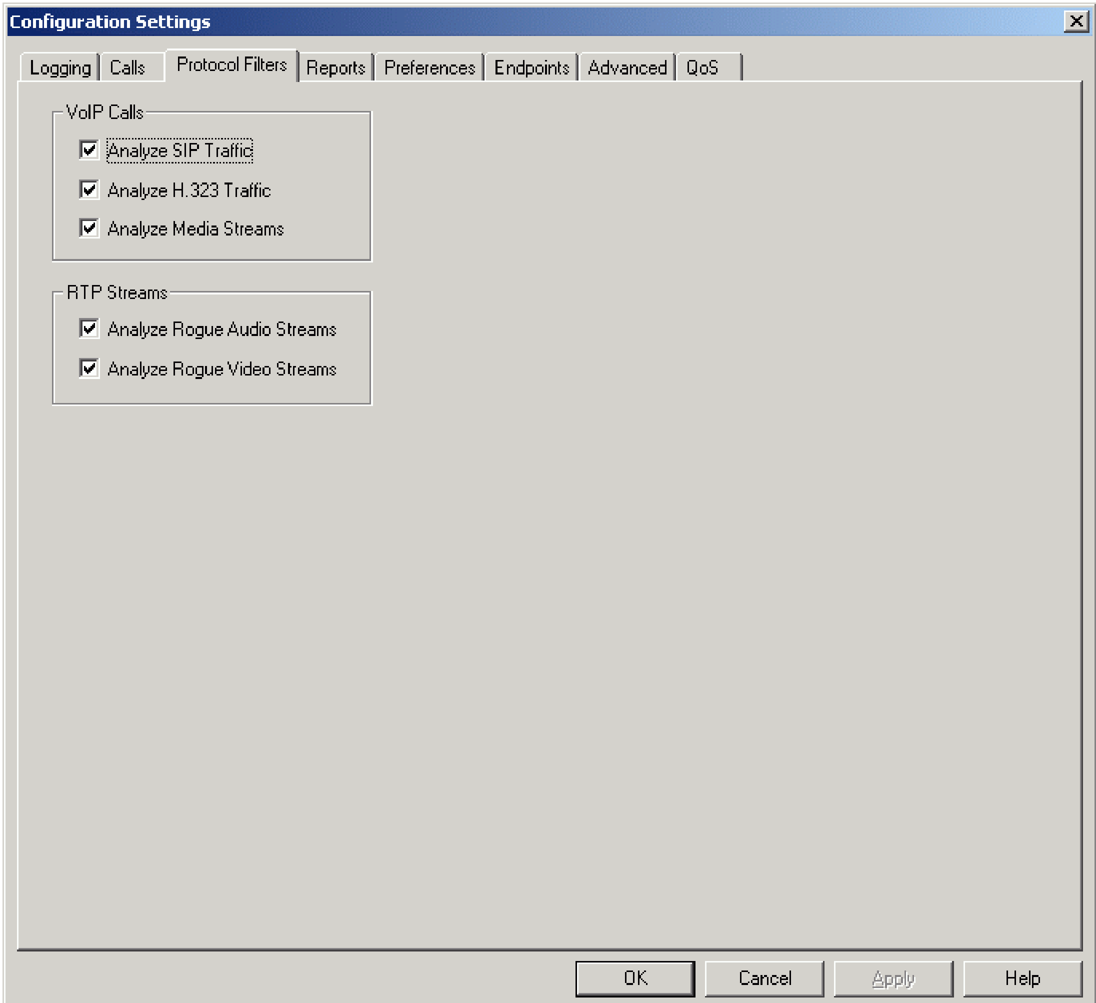
Idle Timeout (Either Direction): The maximum time between packets from either the source or destination that WinEyeQ will wait before timing out the call.

Shutdown Timeout: The maximum time after a call termination attempt is made that WinEyeQ will wait for the other endpoint to respond.

Display time: The time, in seconds, that the call will be displayed on the screen. The amount of memory required by WinEyeQ is proportional to the number of active calls and the length of their display time. Typical values are from 1 to 30 seconds.

Call History Size: The number of calls that will be added to the Recent Calls screen or the Recent Errors screen.

Protocol Filters



The following settings govern the kind of calls are handled:

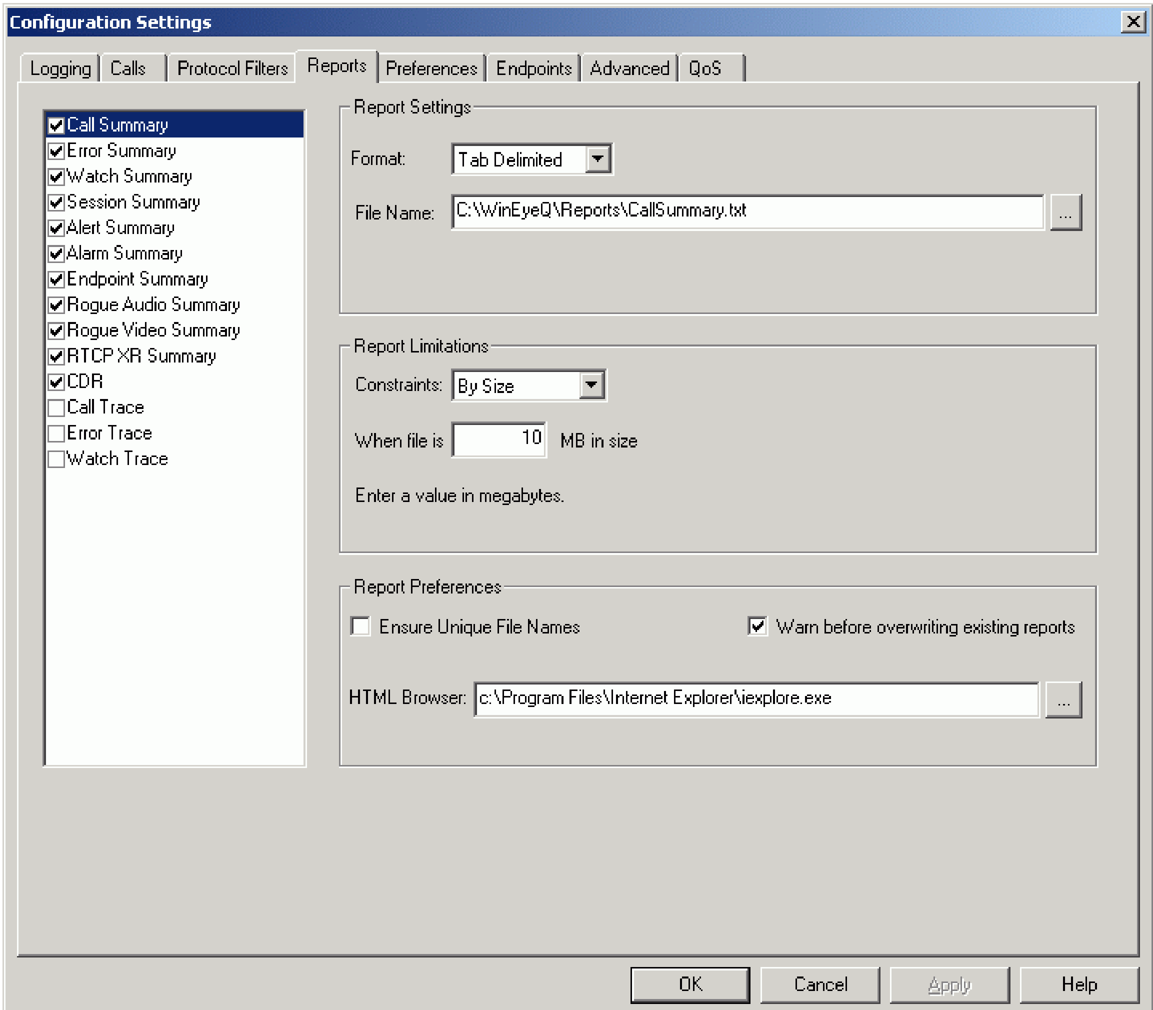
VoIP Calls:

Analyze SIP Traffic: If checked, WinEyeQ will analyze SIP calls.
Analyze H.323 Traffic: If checked, WinEyeQ will analyze H.323 calls.
Analyze Media Streams: If checked, WinEyeQ will analyze audio and video streams.

RTP Streams:

Analyze Rogue Audio Streams: If checked, WinEyeQ will analyze audio streams that are not associated with VoIP calls that WinEyeQ is tracking.
Analyze Rogue Video Streams: If checked, WinEyeQ will analyze video streams that are not associated with VoIP calls that WinEyeQ is tracking.

Reports



The following reports are currently available in WinEyeQ:

Call Summary Report: This report has a one-line-per-call format that details the call parameters, start time, end time, duration, QoS measurements, etc. Call Summary reports are saved in the "Reports' folder.

Error Summary Report: This report has a one-line-per-failed-call format that details the call parameters, start time, end time, duration, QoS measurements, etc. Error Summary reports are saved in the "Reports' folder.

Watch Summary Report: This report has a one-line-per-watched-call format that details the call parameters, start time, end time, duration, QoS measurements, etc. Watch Summary reports are saved in the "Reports' folder.

<u>Session Summary Report</u>: This report generates one-line-per-time-interval that details the number of calls passed / failed, network statistics, etc. The ‘Time Interval’ is set by the user. Session Summary reports are saved in the “Reports’ folder.

<u>Alert Summary Report</u>: This report has a one-line-per-alert format that details the call metric, the alert threshold, and the actual value that triggered the alert. Alert Summary reports are saved in the “Reports’ folder.

<u>Alarm Summary Report</u>: This report has a one-line-per-alarm format that details the call metric, the alarm threshold, and the actual value that triggered the alarm. Alarm Summary reports are saved in the “Reports’ folder.

<u>Endpoint Summary Report</u>: This report contains the information that is removed from the Endpoint View when the number of endpoints in the view exceeds the number of endpoints the user has elected to observe (via Edit **|** Settings **|** Endpoints). Endpoint Summary reports are saved in the “Reports’ folder.

<u>Rogue Audio Summary Report</u>: This report details the start time, end time, duration, QoS measurements, etc. of audio streams that WinEyeQ has detected that are not associated with any VoIP call. Rogue Audio Summary reports are saved in the “Reports’ folder.

<u>Rogue Video Summary Report</u>: This report details the start time, end time, duration, QoS measurements, etc. of video streams that WinEyeQ has detected that are not associated with any VoIP call. Rogue Video Summary reports are saved in the “Reports’ folder.

<u>CDR Report</u>: This report has a one line per call format that summarizes the call information. Start time, end time, duration, IP addresses and ID’s. CDR Summary reports are saved in the “Reports’ folder.

<u>Call, Error and Watch Traces</u>: These reports provide a summary and packet-by-packet trace of the calls. Call, Error and Watch Traces are saved in the “Traces’ folder.

<u>Report Settings</u>:

> <u>Format</u>: Sets the file format that the report will be rendered in such as ASCII, HTML, or XML.
> <u>File Name</u>: Sets the name of the file when it is saved as well as the directory in which it can be found.

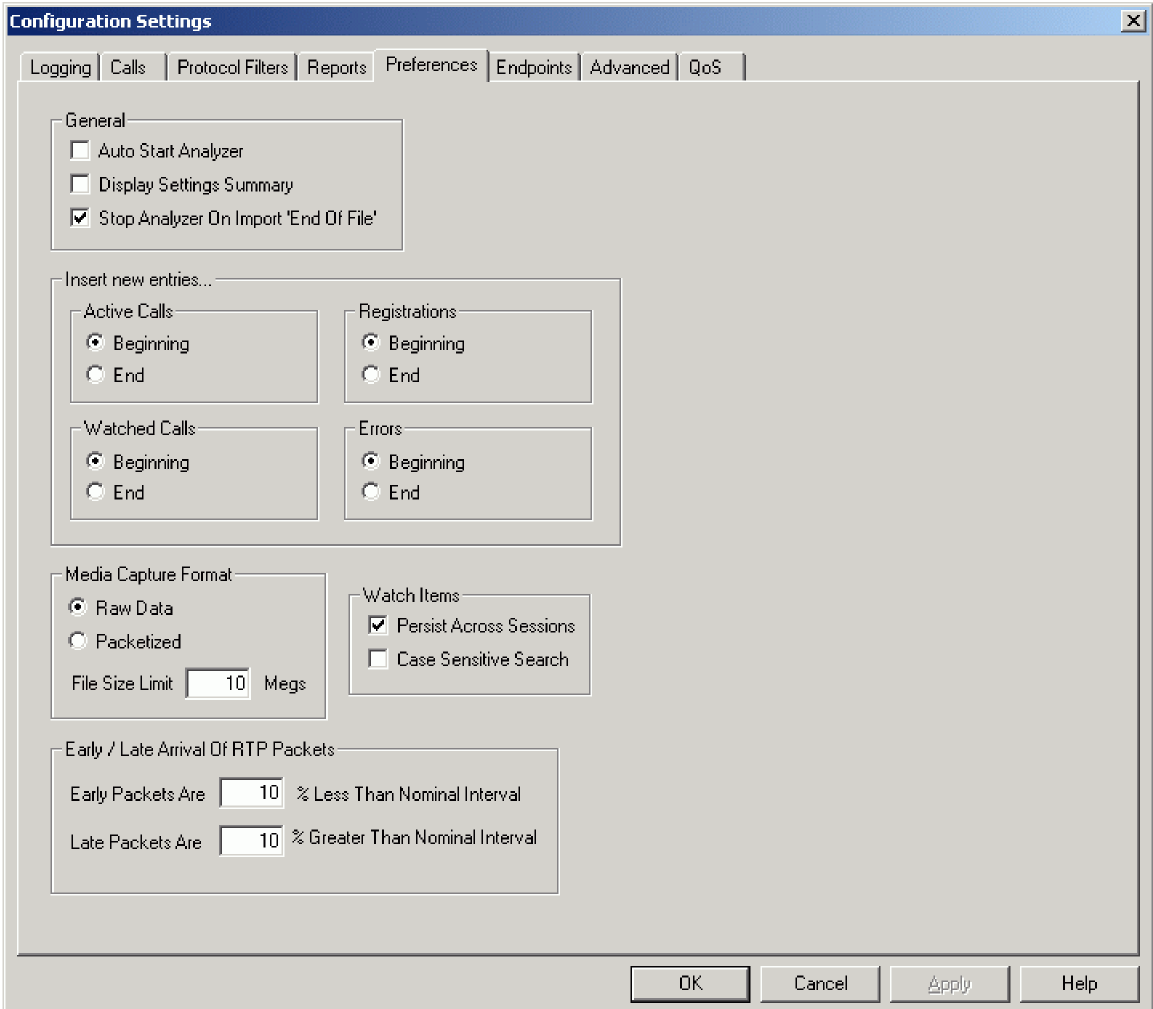
Report Limitations:

Constraints: Sets how each report is separated. At a certain point the program will close one report and open a new one and start recording there. The trigger for this event can be set to Size, Interval, Time of Day, or None (which, if selected will hold all information in only one report file).
Constraint Range: Based on the report constraints, the range sets the event trigger for when the file obtains the value specified in this field.

Report Preferences:

Ensure Unique File Names: If this check box is selected, a timestamp will be appended to the file name when it is created.
Warn before overwriting existing reports: If this check box is selected, the user will be prompted if an existing file is about to be overwritten.
HTML Browser: Specifies the location of an HTML browser application to be used to open reports created in HTML format.

Preferences



The following preferences are available in WinEyeQ:

General:

Auto start analyzer: This feature starts the analysis as soon as WinEyeQ is launched.

Display Settings Summary: If checked, WinEyeQ displays a summary of all the program settings in effect when the program is started.

Stop Analyzer on Import 'End Of File': If selected, WinEyeQ will stop analyzing when an 'end of file' condition is detected while reading an imported file (WinEyeQ or WinPCap format).

Insert new entries:

Active Calls: This option determines where new entries will be added to the active call list.

Watched Calls: This option determines where new entries will be added to the watched call list.

Registrations: This option determines where new entries will be added to the registration list.

Errors: This option determines where new entries will be added to the error list.

Media Capture Format:

Raw or Packetized Data: Choose the media capture format.

File Size Limit: Constraint placed on file size

Watch Items:

Persist Across Sessions: This option automatically reloads the previous session's watches when WinEyeQ is started.

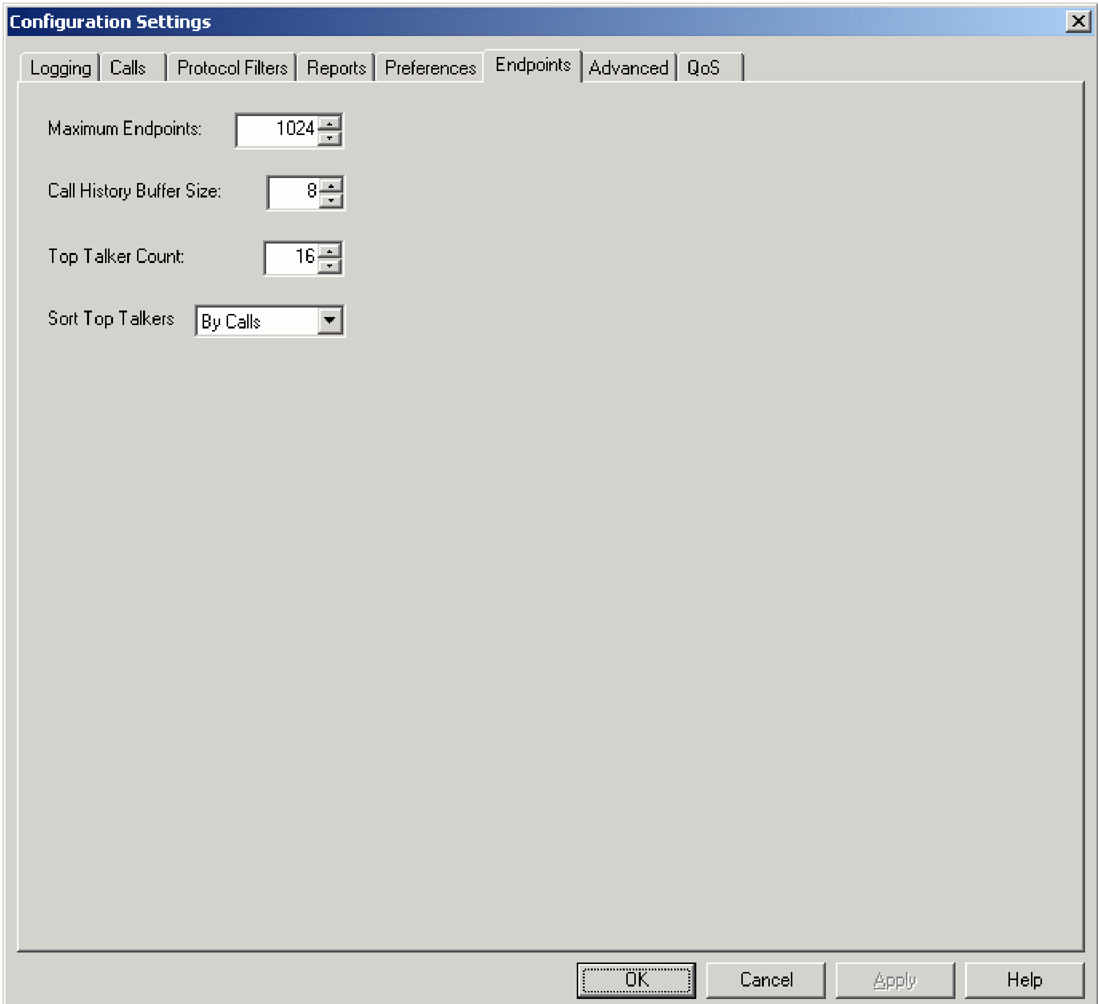
Case Sensitive Searches: This option makes watch item searches sensitive to case.

Early / Late Arrival of RTP Packets:

Early Packets Are XX % Less Than Nominal Interval: Choose a percentage value of the perfect packet interval such that if the interval falls below this value the packet will be considered early. For example, if an RTP stream is sending packets every 20 milliseconds and the early value is 10 %, then if the interval between packets is less than 18 milliseconds, the packet will be considered early.

Late Packets Are XX % Greater Than Nominal Interval: Choose a percentage value of the perfect packet interval such that if the interval falls above this value the packet will be considered late. For example, if an RTP stream is sending packets every 20 milliseconds and the late value is 10 %, then if the interval between packets is greater than 22 milliseconds, the packet will be considered late.

Endpoints



The following endpoint options are available in WinEyeQ:

Maximum Endpoints: The maximum number of endpoints that will be monitored on the Endpoint View.

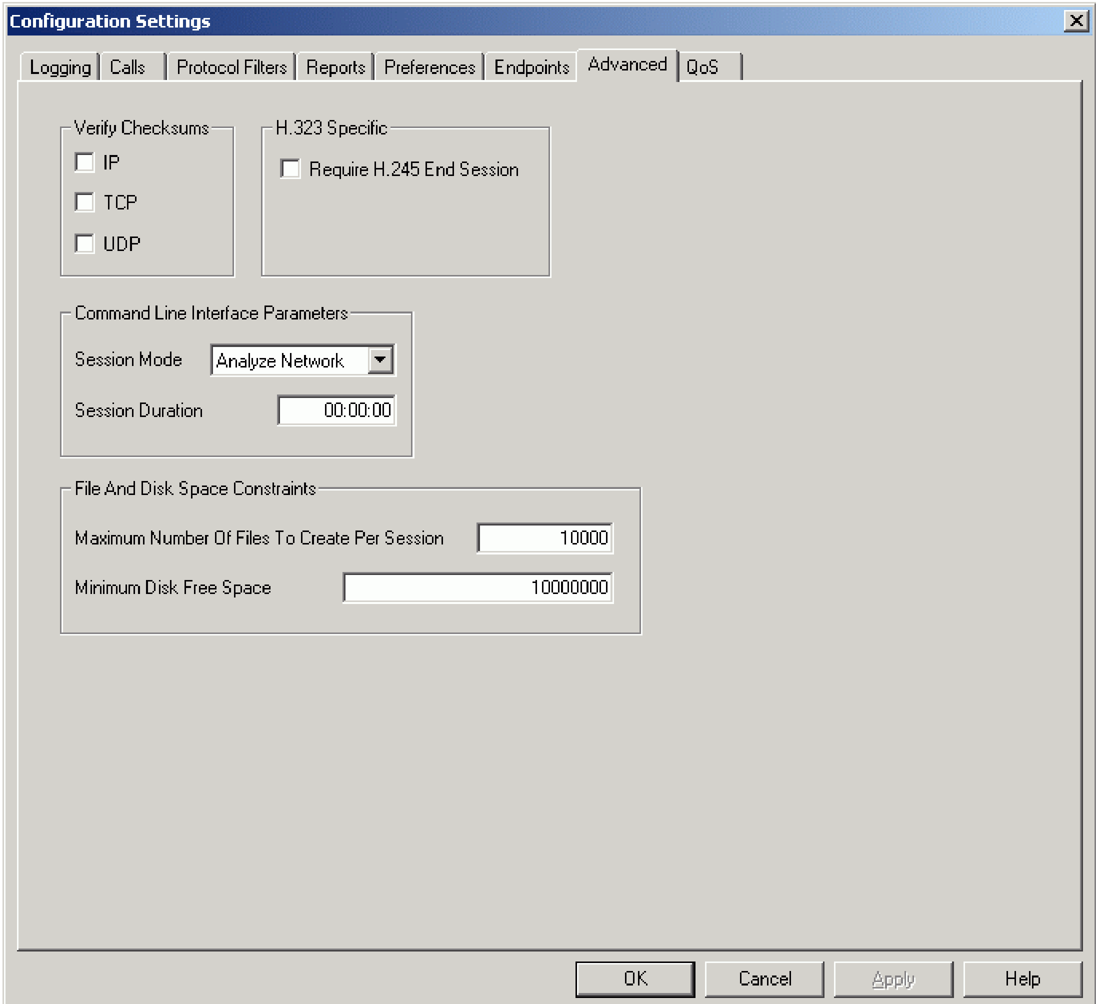
Call History Buffer Size: The maximum number of calls each endpoint has placed / received that will be monitored in the Endpoint Summary and Recent Call History view.

Top Talker Count: The number of Top Talkers that will be added to the Top Talker screen.

Sort Top Talkers: The way that the Top Talkers will be sorted:

By the number of calls
By the time those calls were connected
By the amount of bandwidth used in those calls

Advanced



The following advanced options are available in WinEyeQ:

Verify Checksums:

IP, TCP, and UDP: The respective checksum will be calculated and verified for each of the listed protocols.

H.323 Specific:

Require H.245 End Session: If selected WinEyeQ will require both endpoints to send the End Session message to close the H.245 channel. If not selected, the H.225 Release Complete message will be considered the equivalent.

Command Line Interface Parameters:

Session Mode: Select WinEyeQ mode when program is run by command line.

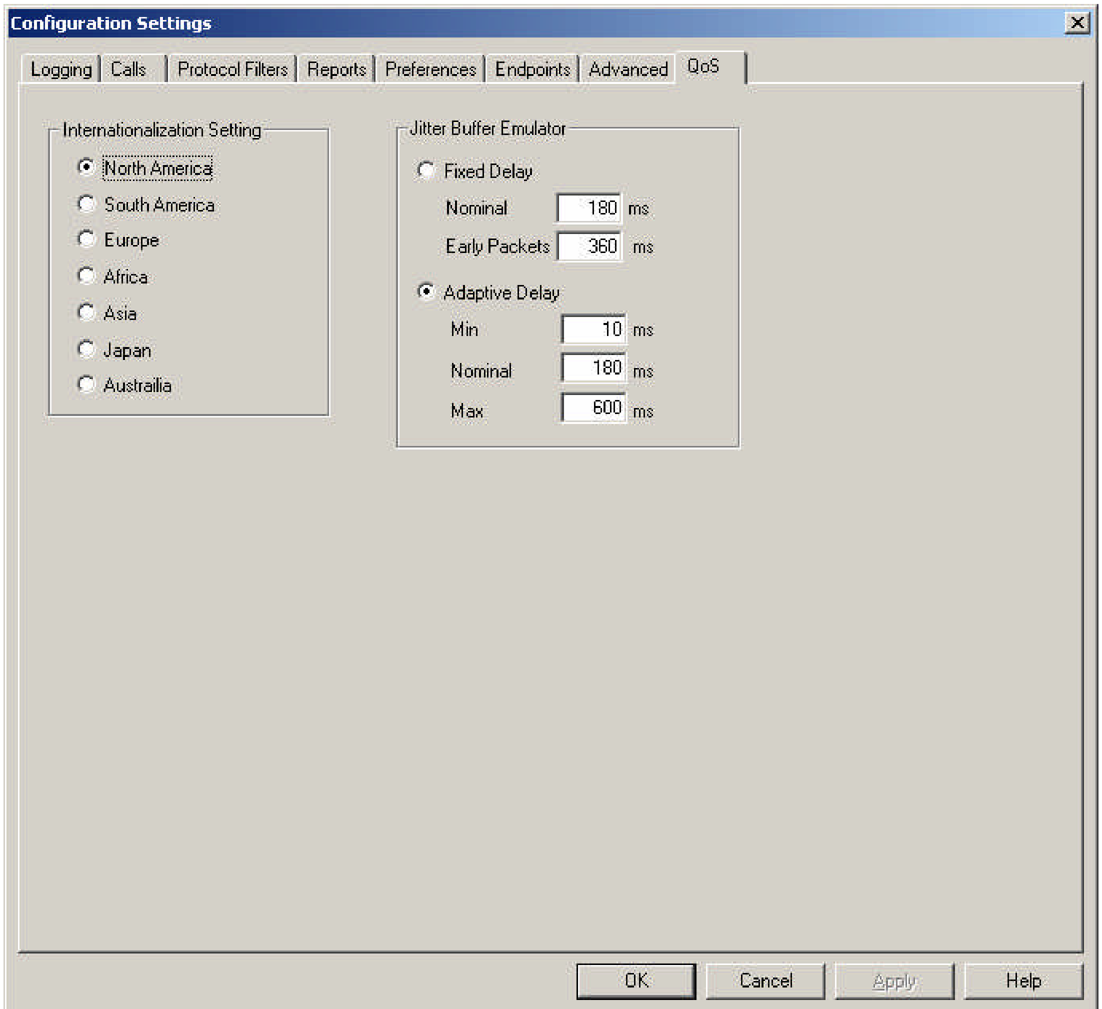
Session Duration: Enter the duration of a command line test. HH:MM:SS

File and Disk Space Constraints:

Maximum Number of Files to Create per Session: This is the maximum number of files (reports, traces, recordings) that WinEyeQ will create during one session.

Minimum Disk Free Space: If the free space on the hard disk that WinEyeQ is running from falls below this amount, WinEyeQ will stop writing to that disk.

QoS



The following QoS options are available for WinEyeQ:

Internationalization Setting: Sets WinEyeQ to generate quality metrics suitable for scales used in different countries.

Jitter Buffer Emulator: simulates the parameters of a jitter buffer. This allows WinEyeQ to have greater accuracy when collecting and analyzing information on packet loss and call quality.

Fixed Delay: Configured Nominal delay does not change.

Nominal Delay: This is the largest "late" delay for a packet beyond which it would be discarded. It is the delay applied to packets that arrives on time or within an "early window".
Early Packets: This is used to determine whether, a packet that is "early", can be accommodated in the emulated jitter buffer. It is the maximum delay that will be applied to a packet that is accommodated by the jitter buffer emulator. IP phones and gateways generally have a maximum buffer that limits the total number of packets that can be stored.

The default values for the fixed settings are 60 ms for the Nominal Delay and 80 ms for the Early Packets.

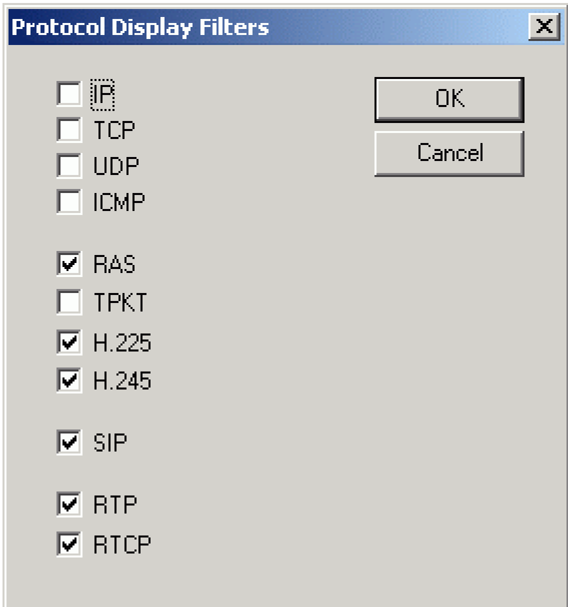
Adaptive Delay: Configured Nominal delay adapts over time.

Min Delay: This is the smallest delay that will be applied to a packet in the Jitter Buffer emulator. The configured nominal delay will not adapt to below this delay.
Nominal Delay: This is used as above. Based on the observed jitter, it adapts and is bounded by the Max and Min delays
Max Delay: This is the upper bound for the Nominal delay, and is also used in estimating the "early window" as mentioned above.

The default values for the adaptive settings are 10 ms for the Minimum Delay, 60 ms for the Nominal Delay and 240 ms for the Maximum Delay.

Note: If these values are chosen such that a jitter buffer cannot be constructed, N/C will be displayed in the QoS tables.

Display Filters

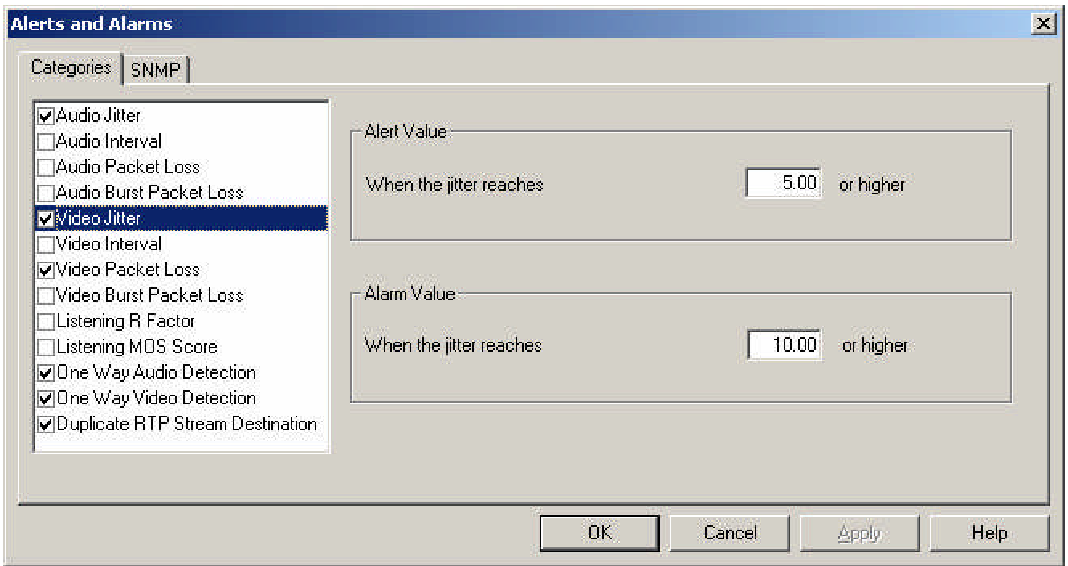


The last step in preparing to run WinEyeQ is to review the filters. WinEyeQ will display the following screen when the Edit | Display Filters menu item is chosen. Select the protocols you want WinEyeQ to display.

Note: Due to memory constraints, only the first few RTP and RTCP packets are displayed for each call.

Alerts and Alarms

Categories



Configurable alerts and alarms are available for the audio and video metric measurements that WinEyeQ performs in real-time. The alert and alarm values are thresholds that are set by the user. The alert and alarm mechanism provides for a two stage detection of user settable limits. Alerts may be set for the following events:

Audio Jitter: When the jitter of an audio stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Audio Interval: When the time between receiving two successive packets (the interval) of an audio stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Audio Packet Loss: When the total number of packets lost of an audio stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Audio Burst Packet Loss: When the number of consecutive packets lost of an audio stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Video Jitter: When the jitter of a video stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Video Interval: When the time between receiving two successive packets (the interval) of a video stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Video Packet Loss: When the total number of packets lost of a video stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Video Burst Packet Loss: When the number of consecutive packets lost of a video stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Listening R Factor: When the listening R factor of an audio stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

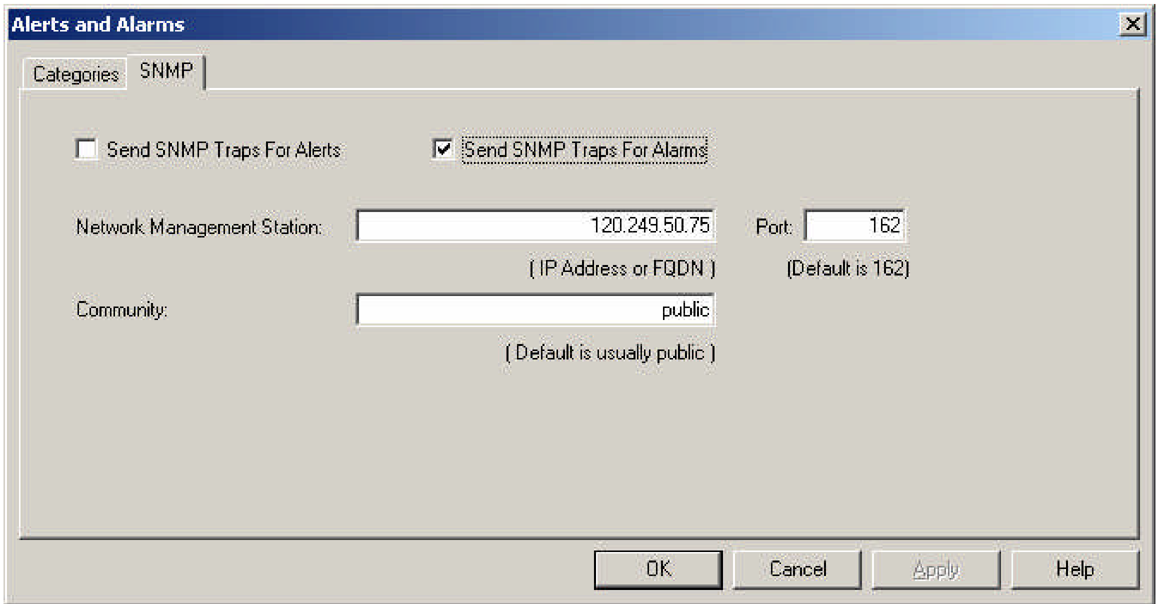
Listening MOS Score: When the listening MOS score of an audio stream exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

One Way Audio Detection: When a call that has audio flowing in only one direction exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

One Way Video Detection: When a call that has video flowing in only one direction exceeds the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

Duplicate RTP Stream Destination: When two media streams that have the same destination IP address and port number are detected and exceed the alert/alarm threshold, a message will be sent to the Alert/Alarm screen.

SNMP



Alerts and alarms may optionally send SNMP traps to an SNMP Network Management Station.

Send SNMP Traps For Alerts: If checked an SNMP trap will be sent to the NMS for all Alerts that have been generated by WinEyeQ.

Send SNMP Traps For Alarms: If checked an SNMP trap will be sent to the NMS for all Alarms that have been generated by WinEyeQ.

Network Management Station: This is the IP Address or Fully Qualified Domain Name of the Network Management Station.

Port: This is the port number where the Network Management Station is listening for SNMP traps. The well known port is 162.

Community: This is the community name used by the Network Management Station. The default community name for most SNMP agents is public.

The following information is provided in each SNMP trap that is sent:

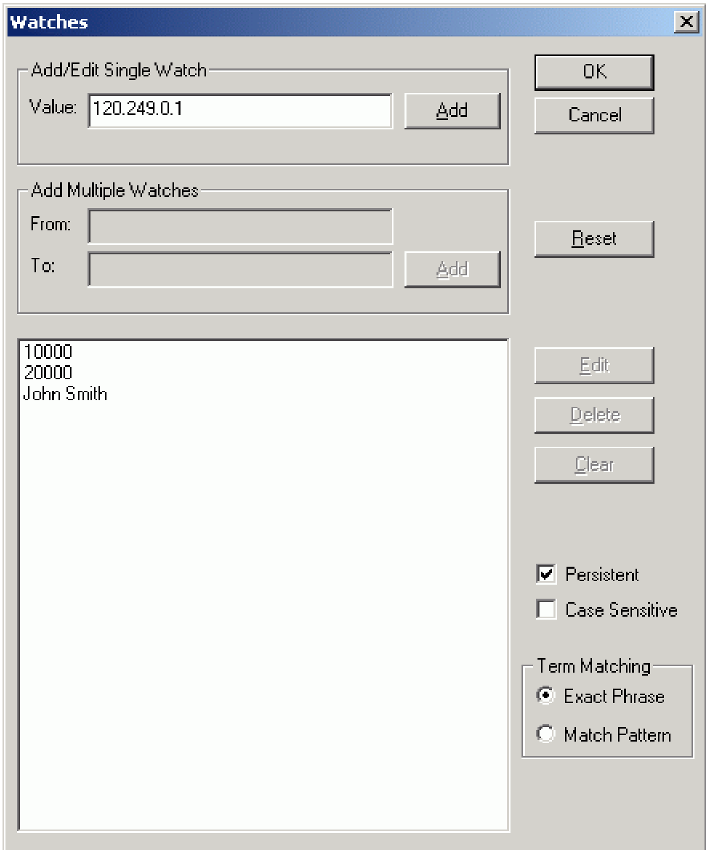
The name of the application generating the trap - WinEyeQ
Whether the trap was an alert or an alarm
The type of trap - audio, video, or signaling
The description of the trap
The source IP address and port of the call
The destination IP address and port of the call
The threshold value that was set for the trap
The actual value that triggered the trap
The date and time the trap was generated
The ID and User name from the call

Note: Each field of the trap is generated as a character string.

The following is an example of an SNMP trap generated by WinEyeQ:

1.3.6.1.4.1.27631.1 WinEyeQ
1.3.6.1.4.1.27631.1.2 Alarm
1.3.6.1.4.1.27631.1.2.2 Video
1.3.6.1.4.1.27631.1.2.2.2 Jitter
1.3.6.1.4.1.27631.1.2.2.2.1 Jitter High Alarm
1.3.6.1.4.1.27631.1.2.2.2.2 Source 120.249.50.100:50354
1.3.6.1.4.1.27631.1.2.2.2.3 Dest 120.249.50.75:25008
1.3.6.1.4.1.27631.1.2.2.2.4 Threshold 1.10
1.3.6.1.4.1.27631.1.2.2.2.5 Value 3.09
1.3.6.1.4.1.27631.1.2.2.2.6 Time 05/08/2007 17:43:16.697
1.3.6.1.4.1.27631.1.2.2.2.7 ID = BB94C810992CEE9D58731FB3D16753F2 - User = 500095

Watches



The watch mechanism allows you to filter out specific calls based upon the value of various call elements or fields within a call. This powerful mechanism allows you to trap calls based upon call ID, IP address, E.164 alias, H.323 ID and most other fields where values are known ahead of time. You may add, edit and delete values associated with watches.

Watches may be designated as persistent (lasting across sessions) and case-sensitive by selecting the appropriate settings on the Edit | Preferences page from the options menu item. Also, you can specify the watch to match the value exactly or match a subset of the value. For example, if 'Exact' were selected, the watch 'Joe' would match the value 'Joe' but not the value 'Joey'. If 'Match Pattern' were selected, 'Joe' would match both 'Joe' and 'Joey'.

Capturing Calls

Overview

WinEyeQ allows you to capture the protocol signaling and initial RTP and RTCP packets from each stream. You may capture the calls manually or associate watches with known call elements and automatically capture the calls as the watches are triggered.

Capturing watched calls also allows you to save the individual media streams with or without the RTP header. This feature is enabled by selecting "Media Streams from Watched Calls" from the Capture menu.

When the file is automatically generated via a watch, the file format will be as follows:

Cap [user id] [timestamp].EyeQ:

Where [user id] is the user ID of the source and timestamp is the local time of the call when recording begins. e.g. "Cap 2156726550 01102005090000.EyeQ".

Capture - Calls with Errors

Click Capture menu command then select Capture Calls with Errors. Calls are captured as they move off the active list to the error list. If you don't have Capture Calls With Errors selected, you can still capture the call by right clicking it in the Error list. Only the initial three RTP packets are captured unless the packet contains DTMF. Only the initial three RTCP packets are captured.

The Default file location where captures are saved is:

C:\WinEyeQ\Capture Files*.EYEQ

Capture - Watched Calls

Click Capture menu command then select Capture Watched Calls. If you don't have Capture Watched Calls selected, you can still capture the call by right clicking it in the Error list. Only the initial three RTP packets are captured unless the packet contains DTMF. Only the initial three RTCP packets are captured

The Default file location where captures are saved is:

C:\WinEyeQ\Capture Files*.EYEQ

Capture - Media Streams from Watched Calls

Click the Capture menu command then select Capture Media Streams from Watch Calls. With this option selected the capture file(s) will contain the full number of RTP packets for the watched call.

If enabled while the analyzer is running media streams from calls already on the watch list will not be captured. Only calls added to the watch list after enabling Capture | Watch Calls Media Streams will have their media streams captured.

Default file location:

C:\WinEyeQ\Audio Capture Files*.g711a (for a call running G.711 Alaw)

C:\WinEyeQ\Video Capture Files*.h261 (for a call running H.261)

Capture - Rogue Streams

While viewing media streams in either Other Audio or Other Video right click on the stream of interest and select Start Rogue Stream Capture.

Default file location:

C:\WinEyeQ\Audio Capture Files*.rogue for Other Audio Capture.

C:\WinEyeQ\Video Capture Files*.rogue for Other Video Capture.

The media stream capture will begin immediately after selecting Start Rogue Stream Capture. Media previous to this point will not be included within the capture file.

Recording Calls

Overview

WinEyeQ allows you to record the protocol signaling, RTP and RTCP channels into one singular file for replay. You may record the calls manually or associate watches with known call elements and automatically capture the calls as the watches are triggered.

When the file is automatically generated via a watch, the file format will be as follows:

<u>Rec [user id] [timestamp].EyeQ</u>:

Where [user id] is the user ID of the source and timestamp is the local time of the call when recording begins, e.g. "Rec 2156726550 01102005090000.EyeQ".

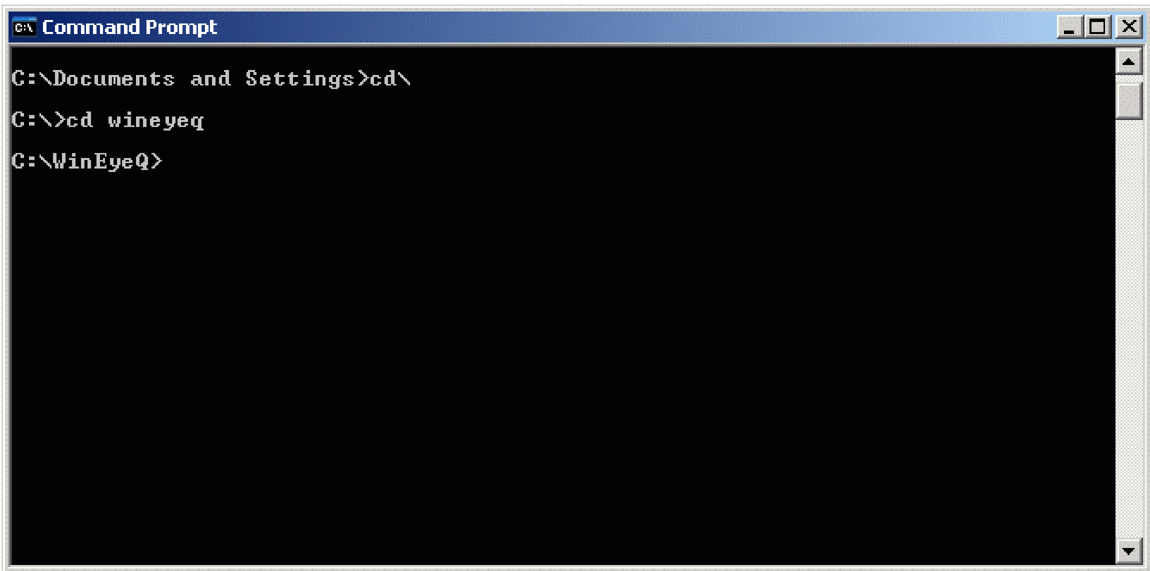
Record - Watch Calls

All of the signaling and media packets are recorded from the watched call to the file.

Command Line Interface

WinEyeQ offers a very basic Command Line Interface (CLI). The application can be started and given all of the information it needs to execute (see Creating Custom Scenarios) but that is the extent of the interaction.

All commands must be entered while in the WinEyeQ directory.



From here you can access all of the WinEyeQ commands and parameters.

To understand how to use the CLI you must first understand the way WinEyeQ retains the parameters the user has entered from one session to the next. WinEyeQ stores these parameters in files located in the WinEyeQ folder on the installed hard drive.

WinEyeQ.cfg

The primary parameter file for WinEyeQ is WinEyeQ.cfg. This file contains the basic parameters required to run WinEyeQ. Normally the values in this file are read and written by the Graphical User Interface (GUI) of the application. If this file is ever deleted, WinEyeQ will rebuild it the next time the application is run.

WinEyeQ.cfg also contains the names of other files that may be used while WinEyeQ is running.

The following parameter files are listed in WinEyeQ.cfg:

- Reports.cfg
- AlertsAlarms.cfg
- Watches.lst
- Addresses.flt

Each of these files contains information that can be altered to affect the WinEyeQ sessions. Again, the values in these files are normally read and written by the Graphical User Interface (GUI) of the application. To find the location of these files in the configuration, open up WinEyeQ.cfg using Notepad.

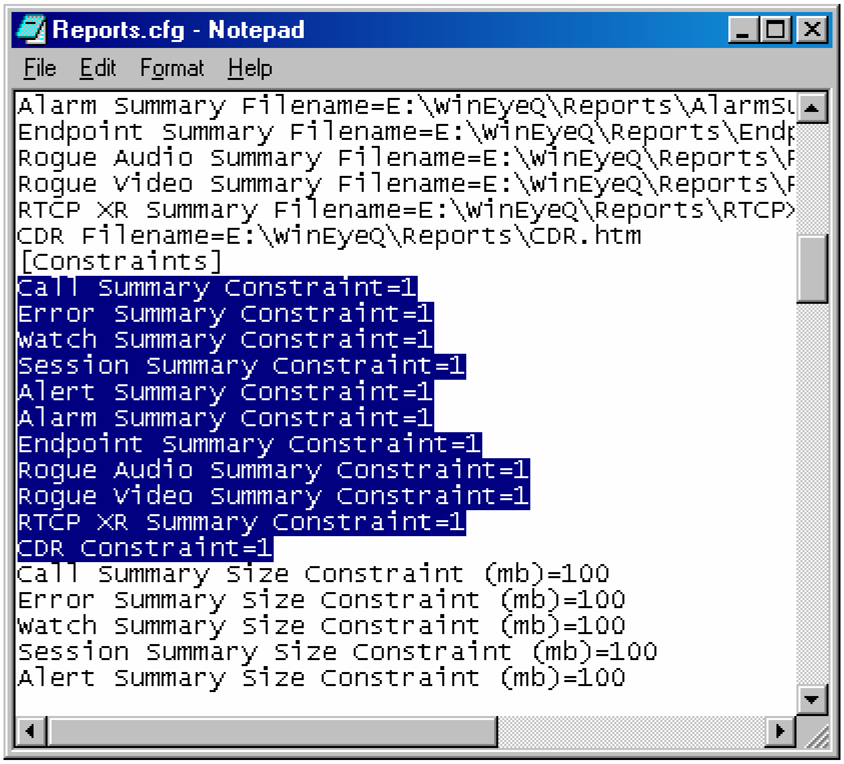
WinEyeQ.cfg - Notepad

File Edit Format Help

```
[Configuration]
LogFile=C:\Projects\WinEyeQ.1.5.X\WinEyeQ.log
ReportsFile=C:\Projects\WinEyeQ.1.5.X\Reports.cfg
AddressFiltersFile=C:\Projects\WinEyeQ.1.5.X\Addresses.flt
Alerts And Alarms File=C:\Projects\WinEyeQ.1.5.X\AlertsAlarms.cfg
Watches File=C:\Projects\WinEyeQ.1.5.X\Watches.lst
Application Window Pos=0,0,1280,1024
Application Name=Demonstration
Exited Cleanly=FALSE
Session Mode=1
LogLevel=0
Reset LogFile=TRUE
LogFile Contraint=1
LogFile Size Contraint (mb)=100
LogFile Period Contraint=3600000
LogFile Time Contraint=0
Command Port=998
Data Port=999
Database Enabled=FALSE
Network Adapter=1
Call Startup Timeout=10
Call Idle Timeout (Both Directions)=10
Call Idle Timeout (Either Direction)=10
Call Shutdown Timeout=10
Display Time=3
```


Reports.cfg

This contains the parameters for the reports that are generated by WinEyeQ. The active reports can be toggled on and off (a "0" is off, while a "1" is on).

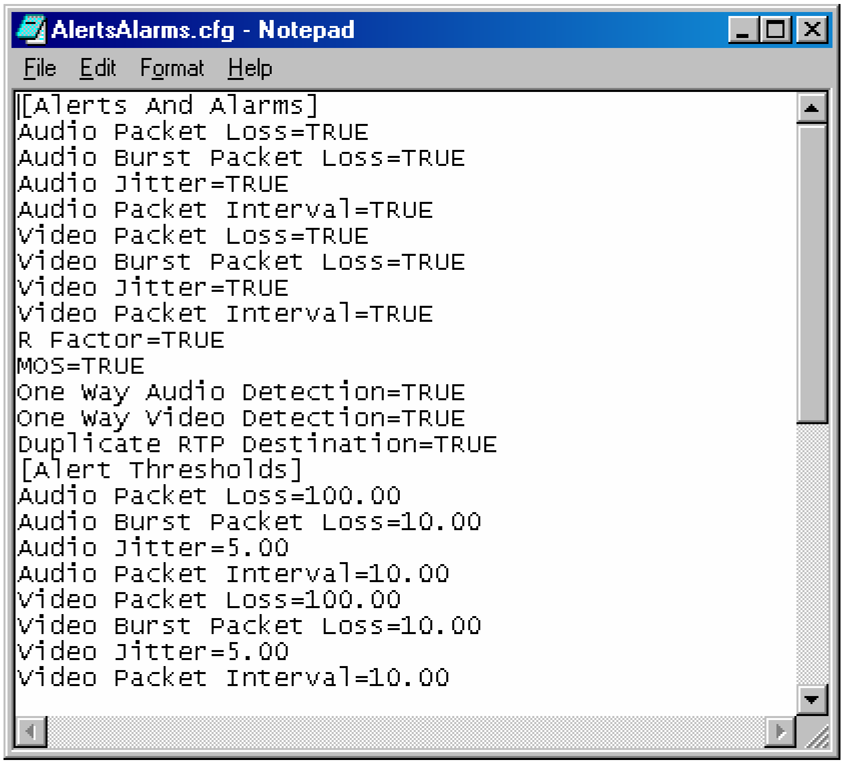



```
Alarm Summary Filename=E:\WinEyeQ\Reports\AlarmSu
Endpoint Summary Filename=E:\WinEyeQ\Reports\Endp
Rogue Audio Summary Filename=E:\WinEyeQ\Reports\R
Rogue Video Summary Filename=E:\WinEyeQ\Reports\R
RTCP XR Summary Filename=E:\WinEyeQ\Reports\RTCPX
CDR Filename=E:\WinEyeQ\Reports\CDR.htm
[Constraints]
Call Summary Constraint=1
Error Summary Constraint=1
Watch Summary Constraint=1
Session Summary Constraint=1
Alert Summary Constraint=1
Alarm Summary Constraint=1
Endpoint Summary Constraint=1
Rogue Audio Summary Constraint=1
Rogue Video Summary Constraint=1
RTCP XR Summary Constraint=1
CDR Constraint=1
Call Summary Size Constraint (mb)=100
Error Summary Size Constraint (mb)=100
Watch Summary Size Constraint (mb)=100
Session Summary Size Constraint (mb)=100
Alert Summary Size Constraint (mb)=100
```

You can also find and change the settings on how often the reports are refreshed (such as time of day, file size, or set intervals) as well as various other report constraints.

AlertsAlarms.cfg

This file controls which alerts and alarms are active, as well as the various thresholds to trigger them.



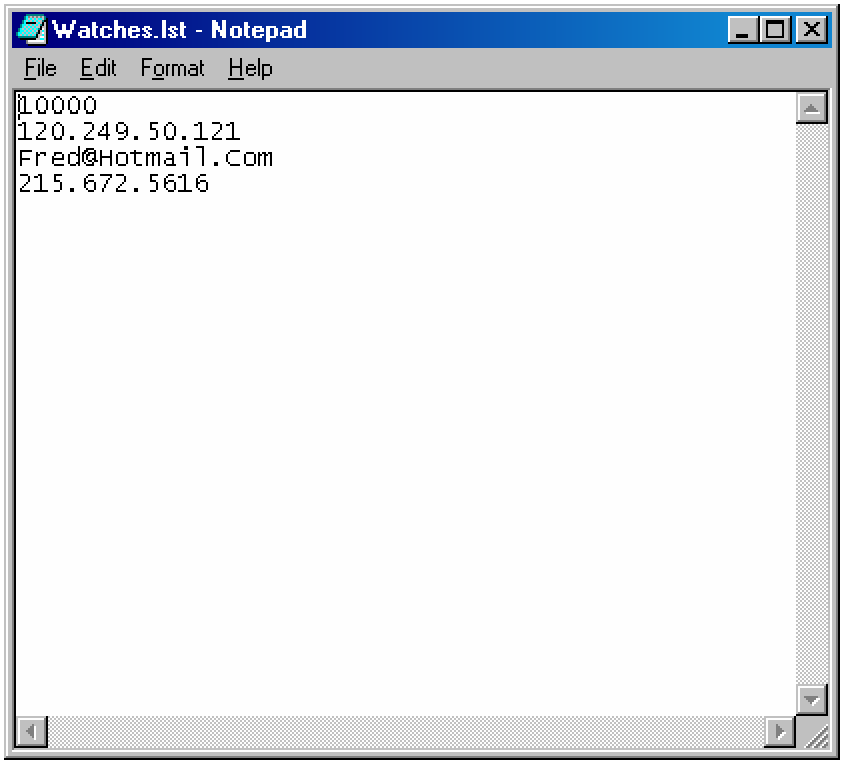
AlertsAlarms.cfg - Notepad

File Edit Format Help

```
[Alerts And Alarms]
Audio Packet Loss=TRUE
Audio Burst Packet Loss=TRUE
Audio Jitter=TRUE
Audio Packet Interval=TRUE
Video Packet Loss=TRUE
Video Burst Packet Loss=TRUE
Video Jitter=TRUE
Video Packet Interval=TRUE
R Factor=TRUE
MOS=TRUE
One Way Audio Detection=TRUE
One Way Video Detection=TRUE
Duplicate RTP Destination=TRUE
[Alert Thresholds]
Audio Packet Loss=100.00
Audio Burst Packet Loss=10.00
Audio Jitter=5.00
Audio Packet Interval=10.00
Video Packet Loss=100.00
Video Burst Packet Loss=10.00
Video Jitter=5.00
Video Packet Interval=10.00
```

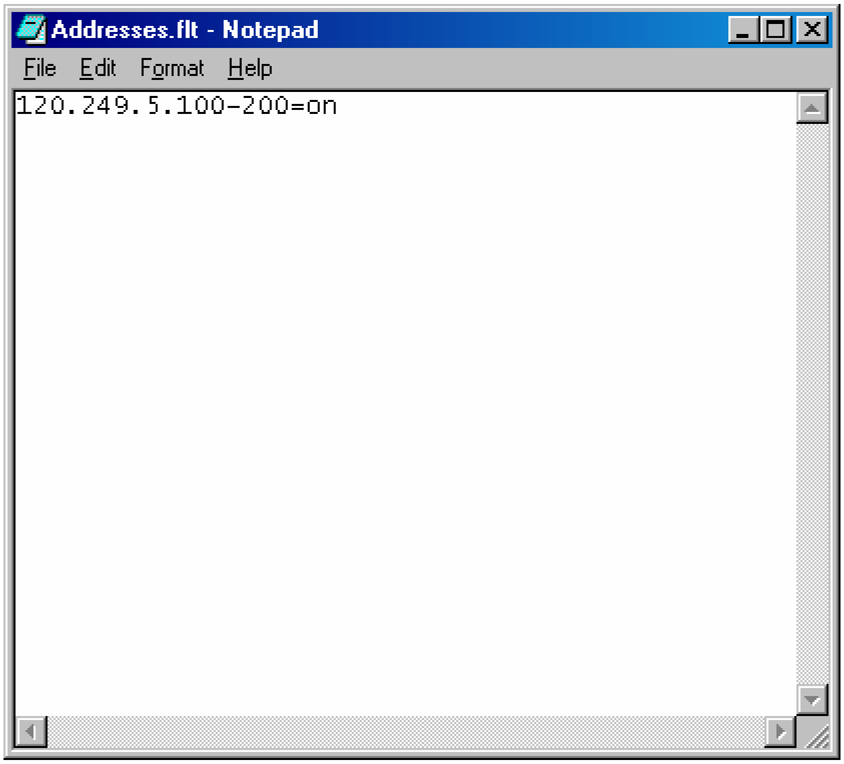
Watches.lst

Sets and controls the watches that are generated.



Addresses.flt

This controls the range of IP addresses that the filter looks at for information to analyze.

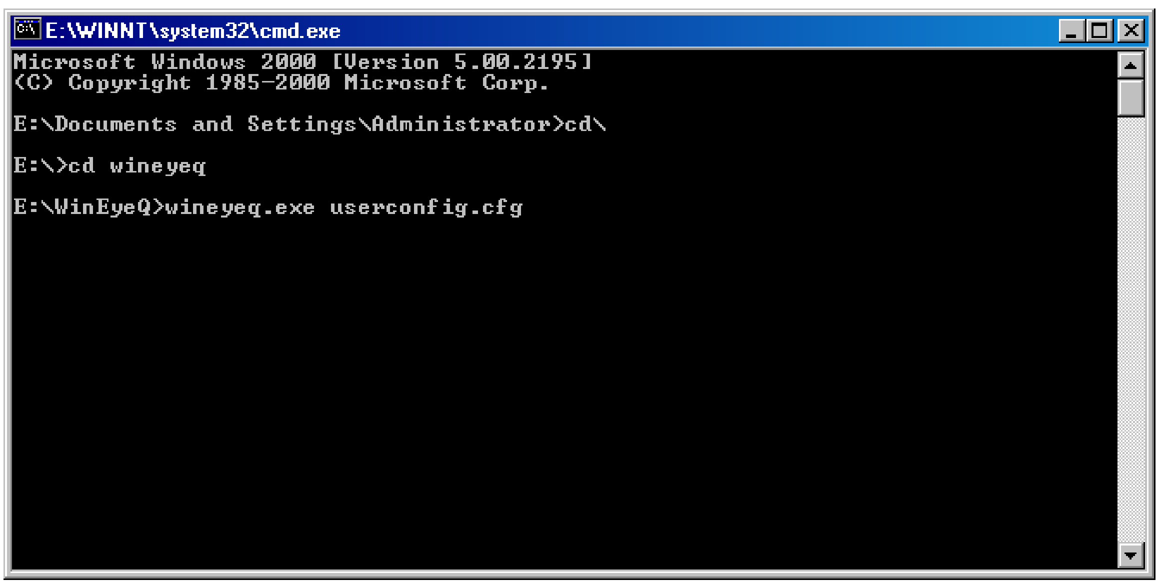


Creating Custom Scenarios

The first step in creating a custom scenario is to save and rename the WinEyeQ.cfg file. Be sure that the new configuration is a .cfg file and not a .txt file. Next, open the parameter files you wish to alter in Notepad, look through the various options available, and alter the parameters as you wish. Be sure to save the files and rename them, again making sure that they are not .txt files. Finally, in your new WinEyeQ configuration file, change the file names so that it points to the appropriate new parameter file(s) you created, and be sure to save the file. Now, you may run your new scenario when you are on the command line in your directory.

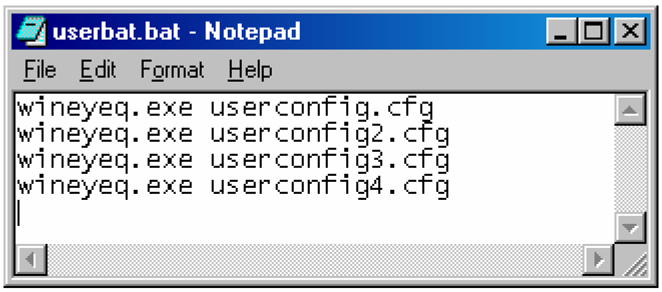
Running Custom Scenarios

In order to run a custom scenario that you created, first make sure that all of the files you made and altered are in the WinEyeQ directory. Next, open up the command prompt, again opening up the WinEyeQ directory. To run your file, type in the command “wineyeq.exe [your replacement for the WinEyeQ.cfg file].cfg and press enter.

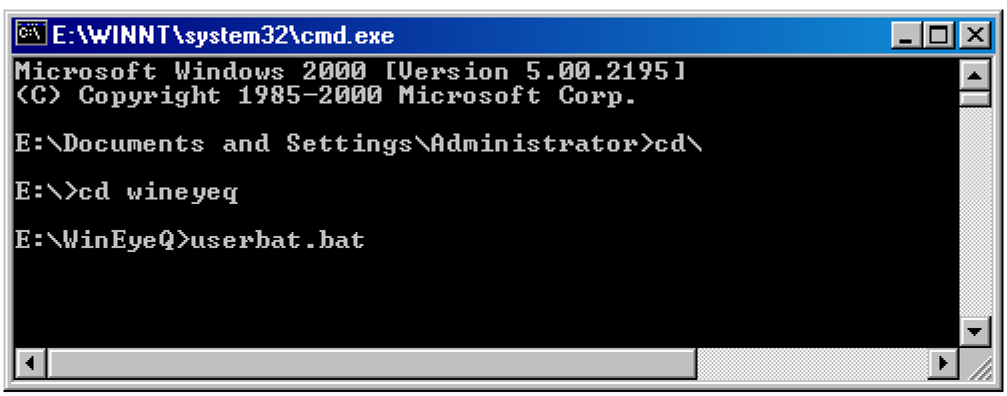


Creating and Running .bat files

You can create files that run several custom configurations in sequence by creating a .bat file. First, you must create each individual configuration you wish to run, using the steps mentioned earlier, and be sure that they are all given unique file names within the WinEyeQ directory. Next, open up a Notebook document, and enter the commands you wish to use in sequence, being sure to press enter after each command. Save the file when you are done as a .bat file in the WinEyeQ directory.



Finally, when you are in the command interface, simply enter the .bat file name and press enter to run the sequence.



WinPcap License

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

Appendix A

Theoretical Maximum MOS Scores and R Factors

The following chart contains the theoretical maximum values for Listening and Conversational MOS and R factor by codec type.

Codec Name	MOS-LQ	MOS-CQ	R-LQ	R-CQ
G.711 u-law	4.2	4.18	93	92
G.711 A-law	4.2	4.18	93	92
G.722 64k	3.88	3.84	94	93
G.722 56k	3.73	3.69	90	89
G.722 48k	3.53	3.48	84	83
G.722.1 32k	4.04	4.01	100	99
G.722.1 24k	3.91	3.91	96	95
G.722.2 23.85k	4.164	4.14	106	105
G.722.2 23.05k	4.16	4.14	106	105
G.722.2 19.85k	4.16	4.14	106	105
G.722.2 18.25k	4.09	4.09	103	102
G.722.2 15.85k	4.09	4.06	102	101
G.722.2 14.25k	4.06	4.04	101	100
G.722.2 12.85k	3.98	3.95	98	97
G.722.2 8.85k	3.73	3.69	90	89
G.722.2 6.6k	3.35	3.3	79	78
G.723.1-5.3k	3.61	3.57	74	73
G.723.1-6.3k	3.77	3.73	78	76
G.726-16k	2.82	2.77	57	56
G.726-24k	3.35	3.3	68	67
G.726-32k	4.04	4.01	86	85
G.726-40k	4.16	4.14	91	90
G.728	4.04	4.01	86	85
G.729/G.729B	3.95	3.91	83	82
G.729A/G.729AB	3.91	3.88	82	81
G.729E 8.0k	3.91	3.88	82	81
G.729E 11.8k	4.11	4.09	89	88
AMR NB 12.2k	4.09	4.06	88	59
AMR NB 10.2k	3.91	3.88	82	81
AMR NB 7.95k	3.69	3.65	76	75
AMR NB 7.4k	3.61	3.57	74	73
AMR NB 6.7k	3.44	3.39	70	69
AMR NB 5.9k	3.25	3.21	66	65
AMR NB 5.15k	3.06	3.02	62	61
AMR NB 4.75k	3.02	2.96	61	60
iLBC 13.3k	3.88	3.84	81	80
iLBC 15.2k	3.95	3.91	83	82
Speex NB 2.15k	2.92	2.87	59	58
Speex NB 5.95k	2.92	2.87	59	58
Speex NB 8k	3.39	3.35	69	68
Speex NB 11k	3.88	3.84	81	77
Speex NB 15k	4.11	4.09	89	88
Speex NB 18.2k	4.11	4.09	89	88
Speex NB 24.6k	4.16	4.14	91	90
Speex NB 3.95k	2.41	2.36	49	48

Appendix B

Sample SNMP traps.

This would be an Alert for an Audio stream that had low packet interval:

1.3.6.1.4.1.27631.1 WinEyeQ
1.3.6.1.4.1.27631.1.1 Alert
1.3.6.1.4.1.27631.1.1.1 Audio
1.3.6.1.4.1.27631.1.1.1.3 Interval
1.3.6.1.4.1.27631.1.1.1.3.1 Packet Interval Low Alert
1.3.6.1.4.1.27631.1.1.1.3.2 Source 120.249.50.100:50354
1.3.6.1.4.1.27631.1.1.1.3.3 Dest 120.249.50.75:25008
1.3.6.1.4.1.27631.1.1.1.3.4 Threshold 58.80
1.3.6.1.4.1.27631.1.1.1.3.5 Value 58.42
1.3.6.1.4.1.27631.1.1.1.3.6 Time 05/08/2007 17:43:15.397
1.3.6.1.4.1.27631.1.1.1.3.7 ID = BB94C810992CEE9D58731FB3D16753F2 - User = 500095

And this would be an Alarm for a Video stream that had high jitter:

1.3.6.1.4.1.27631.1 WinEyeQ
1.3.6.1.4.1.27631.1.2 Alarm
1.3.6.1.4.1.27631.1.2.2 Video
1.3.6.1.4.1.27631.1.2.2.2 Jitter
1.3.6.1.4.1.27631.1.2.2.2.1 Jitter High Alarm
1.3.6.1.4.1.27631.1.2.2.2.2 Source 120.249.50.100:50354
1.3.6.1.4.1.27631.1.2.2.2.3 Dest 120.249.50.75:25008
1.3.6.1.4.1.27631.1.2.2.2.4 Threshold 1.10
1.3.6.1.4.1.27631.1.2.2.2.5 Value 3.09
1.3.6.1.4.1.27631.1.2.2.2.6 Time 05/08/2007 17:43:16.697
1.3.6.1.4.1.27631.1.2.2.2.7 ID = BB94C810992CEE9D58731FB3D16753F2 - User = 500095

Appendix C

Call Scoring - Letter Grades

The letter grades assigned to the various scores associated with signaling and audio and video quality are determined by the following scale:

A+	98 or above
A	92 or above
A-	90 or above
B+	88 or above
B	82 or above
B-	80 or above
C+	78 or above
C	72 or above
C-	70 or above
D+	68 or above
D	62 or above
D-	60 or above
F	Below 60

Audio Scores

This score is designed to provide a comprehensive value which considers all components that contribute the overall QoS/QoE of an audio stream.

The audio score is calculated using Touchstone's proprietary formula which considers the stream's jitter, inter-packet interval, early arrival packets, late arrival packets, listening and conversational MOS scores, listening and conversational R Factor scores and weights these factors against their optimal values.

The audio scores use the scale identified above to determine a corresponding "grade" for the stream.

Video Scores

This score is designed to provide a comprehensive value which considers all components that contribute the overall QoS/QoE of a video stream.

The video score is calculated using Touchstone's proprietary formula which considers the stream's jitter, picture rate, early and late packets to assess the overall stream quality. This score is graded using the scale outline above.

Media Score

This score is designed to provide a comprehensive value which considers all components that contribute the overall QoS/QoE of stream.

The media score is calculated using Touchstone's proprietary formula which considers the weighted values obtained from the scoring of the audio and video components.

The media score uses the scale identified above to determine a corresponding "grade" for the media component.

Signaling Score

This score is designed to provide a comprehensive value which considers all components that contribute the overall QoE of the signaling component of a SIP or H.323-based telephony call or video conference.

The signaling score is calculated using Touchstone's proprietary formula which considers signaling metrics such as initial response time, post-dial delay and call teardown time. These metrics are then compared against industry-accepted values and the score is then calculated based upon the results.

The signaling score uses the scale identified above to determine a corresponding "grade" for the media component.

Overall Score

The overall score is designed to provide a comprehensive value which considers all components that contribute the overall QoE of a SIP or H.323-based telephony call or video conference.

The overall score is calculated using Touchstone's proprietary formula which considers a weighted combination of the signaling and media scores. This score paints a highly accurate portrait of the overall quality of the session.

The overall score uses the scale identified above to determine a corresponding "grade" for the call or conference.

Touchstone Technologies, Inc.
228 North York Road
Suites C & D
Hatboro, PA. 19040

www.touchstone-inc.com