Analyzer User Guide

Version 3.0

March 2014

The information herein is furnished for informational use only, is subject to change by Ixia without notice, and should not be construed as a commitment by Ixia. Ixia assumes no responsibility or liability for any errors or inaccuracies contained in this publication.

Corporate Headquarters	Ixia Worldwide Headquarters 26601 W. Agoura Rd. Calabasas, CA 91302 USA +1 877 FOR IXIA (877 367 4942) +1 818 871 1800 (International) (FAX) +1 818 871 1805 sales@ixiacom.com	Web site: www.ixiacom.com General: info@ixiacom.com Investor Relations: ir@ixiacom.com Training: training@ixiacom.com Support: support@ixiacom.com +1 818 595 2599 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
EMEA	Ixia Technologies Europe Limited Part 2nd floor, Clarion House, Norreys Drive Maidenhead, UK SL6 4FL +44 (1628) 408750 FAX +44 (1628) 639916 salesemea@ixiacom.com	Support: support-emea@ixiacom.com +40 21 301 5699 For the online support form, go to: http://www.ixiacom.com/support/inquiry/?location=emea
Asia Pacific	Ixia Pte Ltd 210 Middle Road #08-01 IOI Plaza Singapore 188994	Support: support-asiapac@ixiacom.com +91 80 4939 6410 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
Japan	Ixia Communications KK Nishi-Shinjuku Mitsui Bldg 11F 6-24-1, Nishi-Shinjuku, Shinjuku-ku Tokyo 160-0023 Japan	Support: support-japan@ixiacom.com +81 3 5326 1980 For the online support form, go to: http://www.ixiacom.com/support/inquiry/
India	Ixia Technologies Pvt Ltd Tower 1, 7th Floor, UMIYA Business Bay Cessna Business Park Survey No. 10/1A, 10/2, 11 & 13/2 Outer Ring Road, Varthur Hobli Kadubeesanahalli Village Bangalore East Taluk Bangalore-560 037, Karnataka, India +91 80 42862600	Support: support-india@ixiacom.com +91 80 4939 6410 For the online support form, go to: http://www.ixiacom.com/support/inquiry/?location=india

China	Ixia Technologies (Shanghai) Company Ltd Unit 3, 11th Floor, Raffles City, Beijing Beijing, 100007 P.R.C.	Support: support-china@ixiacom.com 400 898 0598 (Greater China Region) +86 10 5732 3932 (Hong Kong)

Change: 4150211 *Date:* September 24, 2013

For viewing the FAQs related to the product, go to Ixia Technical Support Online:
https://ebsoprod.ixiacom.com/OA_HTML/jtflogin.jsp

Table of Contents

Chapter 1 About this Guide

Purpose 1-1
Manual Content 1-1
Technical Support 1-2

Chapter 2 Introduction to Analyzer

About Analyzer 2-1

Chapter 3 Analyzer Versions

Analyzer Versions 3-1

Analyzer License Management 3-2

Chapter 4 Analyzer Navigation

Main Window 4-1

Menus and Tool Bars 4-2
Packet Capture Menu 4-2

Application Viewers 4-10
Application Layer Views 4-11
Network Layer Views 4-18
Physical Layer View 4-23
Common View. 4-23
Packet Tree View 4-27
Capture Statistics View 4-27

Actions Performed in Analyzer. 4-29
Opening a Capture in Analyzer. 4-29
Customizing the Main View. 4-29
Applying a Packets Filter 4-32
Saving a Packets Filter 4-34
Loading a Packets Filter 4-35
PRBS Packet Compare 4-35

Chapter 5 SIP Captures

SIP Conversations 5-1
SIP Registration in Analyzer 5-2
SIP Call Control in Analyzer 5-3

SIP Statistics 5-4
SIP Conversation Statistics. 5-4
SIP Endpoint Statistics 5-6

SIP Errors Logged by Analyzer 5-7

Chapter 6 MGCP Captures

MGCP Conversations 6-1

MGCP Statistics. 6-3
Conversation Statistics 6-3
Endpoint Statistics. 6-5

MGCP Errors Logged by Analyzer. 6-5

Chapter 7 MPEG Captures

Chapter 8 RTP Captures

RTP Application Conversations View 8-1
RTP Stream Viewer 8-4

Detailed RTP Viewers 8-6
Packets View 8-6
Wave Form Viewer 8-7
Jitter Chart 8-7
R Factor Chart 8-8
FFT Viewer 8-8
QoS Viewer 8-9

RTP Specific Errors 8-9

Index

1 About this Guide

The information in this section is provided to help you navigate through this manual and make better use of its content. A list of related documentation is also included.

Purpose

This manual introduces Analyzer and provides detailed information about the application's theory, features, functions, and options.

Manual Content

This manual contains the following sections:

Section	Description
Chapter 1, *About this Guide*	Provides information about this manual, including its purpose, content, and related documentation. It also explains how to contact technical support.
Chapter 2, *Introduction to Analyzer*	Provides a short overview of the product regarding its architecture and layout.
Chapter 3, *Analyzer Versions*	Provides information about licensing and the Analyzer license types.
Chapter 4, *Analyzer Navigation*	Provides a description of the Analyzer Graphical User Interface, allowing you to easily navigate through the application.
Chapter 5, *SIP Captures*	Provides a description of the SIP specific measurements and viewers in Analyzer.
Chapter 6, *MGCP Captures*	Provides a description of the MGCP specific measurements and viewers in Analyzer.
Chapter 7, *MPEG Captures*	Provides a description of the video viewer in Analyzer.
Chapter 8, *RTP Captures*	Provides a description of the RTP specific measurements and viewers in Analyzer.
Index	Provides a comprehensive index (listing) for the manual.

Technical Support

You can obtain technical support for any Ixia product by contacting Ixia Technical Support by any of the methods mentioned on the inside cover of this manual. Technical support from Ixia's corporate headquarters is available Monday through Friday from 6 a.m. to 6 p.m., Pacific Standard Time (excluding American holidays). Technical support from Ixia's EMEA and India locations is available Monday through Friday, 8 a.m. to 5 p.m. local time (excluding local holidays).

2 Introduction to Analyzer

The purpose of this chapter is to provide a short overview on the product regarding its architecture and layout.

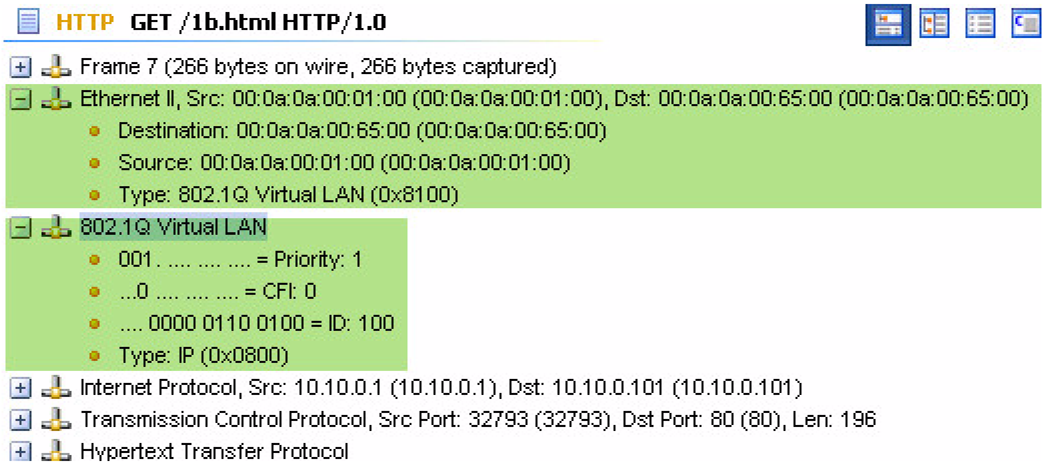
About Analyzer

Analyzer is a powerful Network Traffic Analyzer that captures the traffic on the IXIA ports and provides a lot of statistics, measurements, diagrams, and application viewers to help you debug network problems. It is built as an APTIXIA module and it provides an API to enable other applications to control the network capture.

Analyzer allows you to view the captured packets, network, and application specific statistics, SIP/MGCP call diagrams, RTP Audio waves, MPEG video streams, and so on.

Analyzer can capture L2 Headers with VLAN tags, eliminating the need to use third-party capture tools to view the headers and tags. For example, the following figure shows both the L2 Headers and the 802.1Q VLAN tags:

Figure 2-1.   L2 Headers and VLAN Tags



```
HTTP  GET /1b.html HTTP/1.0

⊞ Frame 7 (266 bytes on wire, 266 bytes captured)
⊟ Ethernet II, Src: 00:0a:0a:00:01:00 (00:0a:0a:00:01:00), Dst: 00:0a:0a:00:65:00 (00:0a:0a:00:65:00)
      ● Destination: 00:0a:0a:00:65:00 (00:0a:0a:00:65:00)
      ● Source: 00:0a:0a:00:01:00 (00:0a:0a:00:01:00)
      ● Type: 802.1Q Virtual LAN (0x8100)
⊟ 802.1Q Virtual LAN
      ● 001. .... .... .... = Priority: 1
      ● ...0 .... .... .... = CFI: 0
      ● .... 0000 0110 0100 = ID: 100
      ● Type: IP (0x0800)
⊞ Internet Protocol, Src: 10.10.0.1 (10.10.0.1), Dst: 10.10.0.101 (10.10.0.101)
⊞ Transmission Control Protocol, Src Port: 32793 (32793), Dst Port: 80 (80), Len: 196
⊞ Hypertext Transfer Protocol
```

3 Analyzer Versions

This chapter covers the license information for Analyzer in the following sections:

- *Analyzer Versions* on page 3-1.
- *Analyzer License Management* on page 3-2.

Analyzer Versions

Analyzer has several variants, each of which is covered by a license. Licenses are of two types:

- for chassis (Analyzer–Chassis Components):
  - Analyzer, Base Software, Packet capture and analysis–performs captures of packets transported over specific protocols, although audio and video decode is not supported;
- for workstations (Analyzer–PC Components):
  - Analyzer, Client, Base Software, Media (audio/video)–decodes and plays audio and video streams;
  - Analyzer Client-Advanced audio–performs in-depth audio analysis;

Analyzer License Management

All Ixia software products are now license-managed. Licensing is managed using the Ixia Registration Utility (IRU). The IRU is automatically installed and run with the installation of licensed Ixia products.

Ixia's license management technique is the means by which Ixia:

- Ensures that its software is licensed and used appropriately.
- Allows Ixia customers to centralize and monitor their software usage.

Licenses are purchased from Ixia and issued to the customer via email. These licenses must be installed onsite in order for the licensed software to operate correctly. License installation for an Ixia software product can occur either:

- At the time of the software installation.
- Sometime after the software installation, but before software usage.

The licensing operation is accomplished with a simple wizard process and can be run from:

- The same computer on which the software was installed, or
- Some other Windows-based PC.

The computer used to perform the licensing process must be connected to the Ixia chassis and workstations in the lab environment. If at all possible, it should also be connected to the Internet. If simultaneous connections to the lab network and Internet are not feasible, it is still possible to complete all licensing operations; the process for offline installation is covered in the *License Management User Guide*.

Depending on the Ixia product, there are two types of licenses that can be purchased:

- A node-locked license – this type of license is locked to a particular chassis or workstation, and allows only certain software functions to run on that chassis or workstation.
- A floating license – this type of license is stored on a License Server, and allows a set number of chassis or workstations to use various software features. All chassis or workstations that use this license must be connected to the License Server, and the server must be running in order for the licensed Ixia product to function. Once the set number of users is reached for a particular license feature, additional users of the product are denied.

Analyzer uses only node-locked licenses. They can be installed either on a License Server or on a chassis/workstation.

Evaluation Licenses

Evaluation licenses are used to evaluate Ixia software products. They can be used for a limited number of days. They act in all respects as a regular license (they must be installed using the IRU), save for the fact that they have a time limit.

Temporary Licenses

Temporary licenses are meant for customer use until receiving a permanent license or in case of licensing software issues on their chassis/workstations. They are time-limited. If licensing software is running on the chassis/workstation, the temporary license is valid for 30 days; if no licensing software is installed/running on the chassis/workstation, the license is limited to two days only.

A temporary license is locked to a particular chassis/workstation. It cannot be updated or registered and can only be issued once per product within a six-month period.

Analyzer temporary licenses operate as described in the following paragraphs.

- Workstation temporary licenses (Analyzer-PC Components, with the next subcomponents):
    - Analyzer, Client, Base Software, Media (audio/video)–is checked when opening a capture, if analyzers are enabled. If there is no such license, a pop-up dialog opens, asking the users if they want a temporary license.

> **NOTE**: When all analyzers are disabled (Options>Preferences>Customization), the Analyzer, Client Base Software, Media (audio) license is not checked.

-
    - Analyzer Client-Advanced audio–To perform in-depth audio analysis, an Analyzer Client-Advanced media license is needed. On attempting to perform such analysis, the Analyzer Client-Advanced media is checked. If the license is not present, a pop-up dialog opens, asking the users if they want a temporary license.
- Chassis temporary licenses (Analyzer-Chassis Components with the Analyzer, Base Software, Packet capture and analysis license) –They are checked when the user applies the configuration and capturing has been enabled. If there is no such license, a temporary license dialog opens, allowing you to choose whether to install a temporary license.

4 Analyzer Navigation

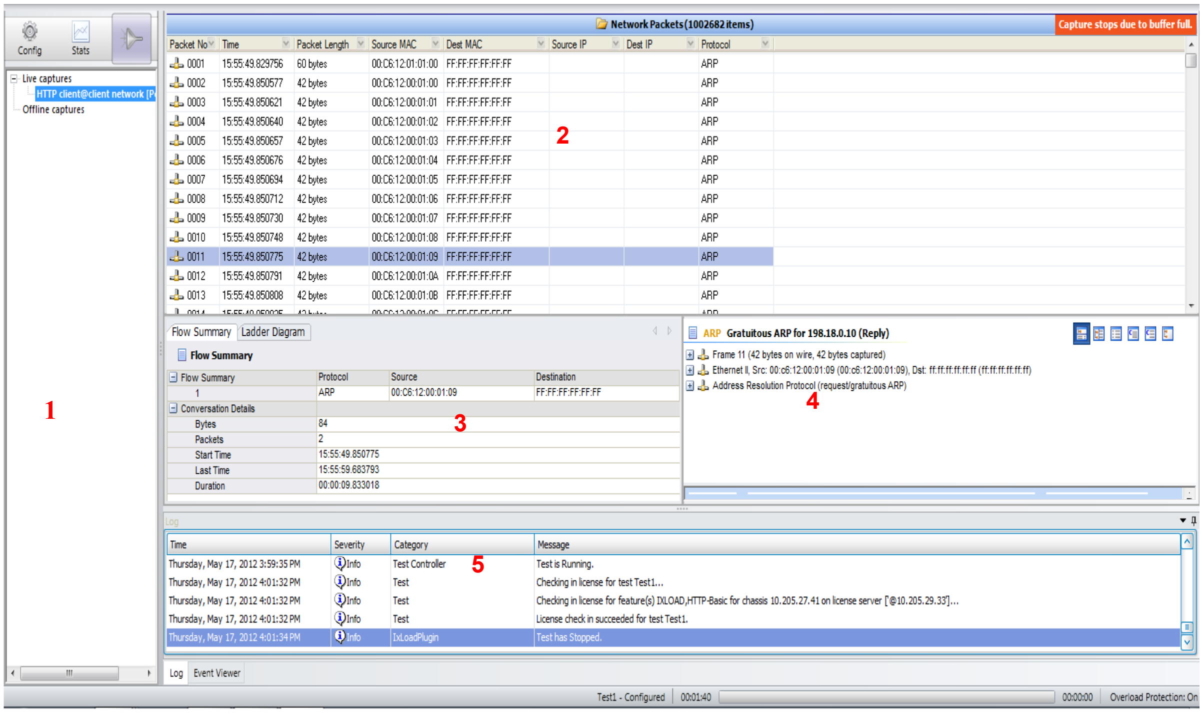
This chapter provides a description of the Analyzer Graphical User Interface, allowing you to easily navigate through the application, by using:

- *Main Window* on page 4-1.
- *Menus and Tool Bars* on page 4-2.
- *Application Viewers* on page 4-10.
- *Actions Performed in Analyzer* on page 4-29.

Main Window

The main window consists of four main panels, as shown in Figure 4-1 on page 4-2:

- *Navigation Toolbox* – Contains navigation links to the *Application, Network*, and *Physical* Layers.
- *Common View* – Contains view specific tabs. It contains more detailed information than the main list, and makes available various statistics related to the main list selection.
- *Packet Tree View* – When available, displays detailed packet information in various forms.
- *Application Viewers* – Lists details related to the selection made in the *Navigation* toolbox.



Network Packets(1002682 items)

Capture stops due to buffer full.

Packet No	Time	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol
0001	15:55:49.829756	60 bytes	00:C6:12:01:01:00	FF:FF:FF:FF:FF:FF			ARP
0002	15:55:49.850577	42 bytes	00:C6:12:00:01:00	FF:FF:FF:FF:FF:FF			ARP
0003	15:55:49.850621	42 bytes	00:C6:12:00:01:01	FF:FF:FF:FF:FF:FF			ARP
0004	15:55:49.850640	42 bytes	00:C6:12:00:01:02	FF:FF:FF:FF:FF:FF			ARP
0005	15:55:49.850657	42 bytes	00:C6:12:00:01:03	FF:FF:FF:FF:FF:FF			ARP
0006	15:55:49.850676	42 bytes	00:C6:12:00:01:04	FF:FF:FF:FF:FF:FF			ARP
0007	15:55:49.850694	42 bytes	00:C6:12:00:01:05	FF:FF:FF:FF:FF:FF			ARP
0008	15:55:49.850712	42 bytes	00:C6:12:00:01:06	FF:FF:FF:FF:FF:FF			ARP
0009	15:55:49.850730	42 bytes	00:C6:12:00:01:07	FF:FF:FF:FF:FF:FF			ARP
0010	15:55:49.850748	42 bytes	00:C6:12:00:01:08	FF:FF:FF:FF:FF:FF			ARP
0011	15:55:49.850775	42 bytes	00:C6:12:00:01:09	FF:FF:FF:FF:FF:FF			ARP
0012	15:55:49.850791	42 bytes	00:C6:12:00:01:0A	FF:FF:FF:FF:FF:FF			ARP
0013	15:55:49.850808	42 bytes	00:C6:12:00:01:0B	FF:FF:FF:FF:FF:FF			ARP

Flow Summary

Flow Summary	Protocol	Source	Destination
1	ARP	00:C6:12:00:01:09	FF:FF:FF:FF:FF:FF
Conversation Details			
Bytes	84		
Packets	2		
Start Time	15:55:49.850775		
Last Time	15:55:59.683793		
Duration	00:00:09.833018		

ARP Gratuitous ARP for 198.18.0.10 (Reply)

- Frame 11 (42 bytes on wire, 42 bytes captured)
- Ethernet II, Src: 00:c6:12:00:01:09 (00:c6:12:00:01:09), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request/gratuitous ARP)

Log

Time	Severity	Category	Message
Thursday, May 17, 2012 3:59:35 PM	Info	Test Controller	Test is Running.
Thursday, May 17, 2012 4:01:32 PM	Info	Test	Checking in license for test Test1...
Thursday, May 17, 2012 4:01:32 PM	Info	Test	Checking in license for feature(s) IXLOAD,HTTP-Basic for chassis 10.205.27.41 on license server ['@10.205.29.33']...
Thursday, May 17, 2012 4:01:32 PM	Info	Test	License check in succeeded for test Test1.
Thursday, May 17, 2012 4:01:34 PM	Info	IxLoadPlugin	Test has Stopped.

Test1 - Configured | 00:01:40 | 00:00:00 | Overload Protection: On

Figure 4-1. Analyzer Main Window

1: Navigation Tool bar

2: Application Viewers

3: Common View

4: Packet Tree View

5: Log View

Menus and Tool Bars

This section describes the Analyzer menu options and tool bar buttons:

Packet Capture Menu

List details related to Open Capture, Grid Operations, Merge Capture etc.

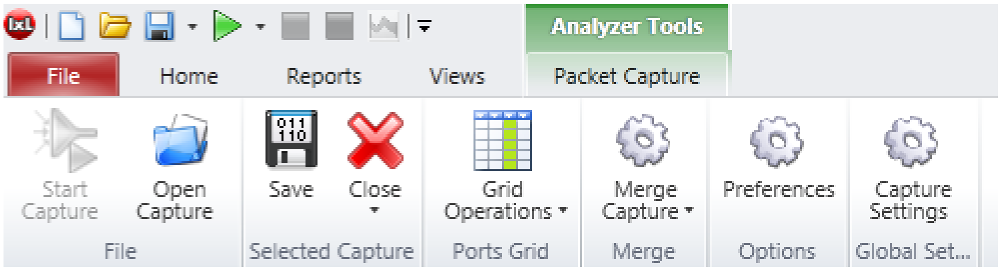


Figure 4-2. Reports Menu

Open Capture

Gives the option to open an existing Capture.

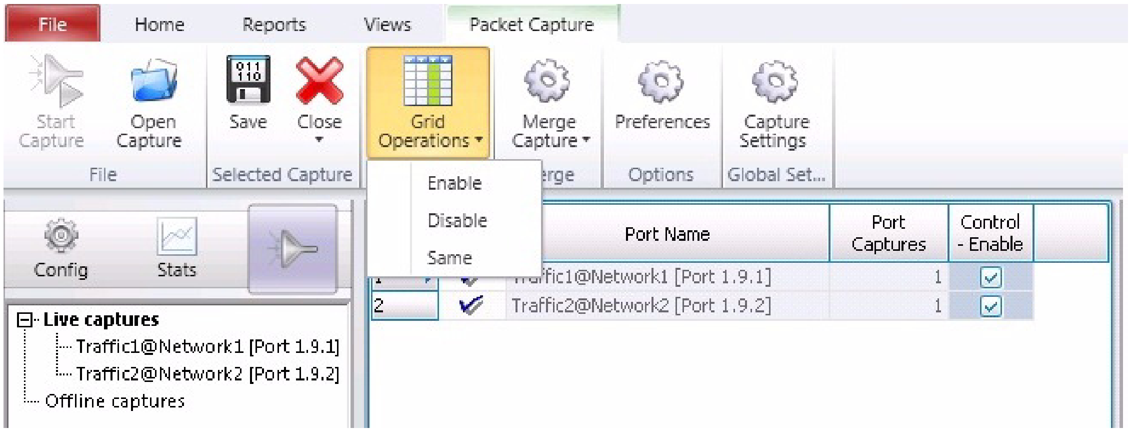
Save and Close

Save button allows you to save the current opened capture(s). Close button allows you to close the selected capture.

Close All allows you to close all displayed captures.

Grid Operations

Grid Operation button allows you to perform one of the defined operations on the entire column. S



		Port Name	Port Captures	Control - Enable
1	✓	raffic1@Network1 [Port 1.9.1]	1	☑
2	✓	Traffic2@Network2 [Port 1.9.2]	1	☑

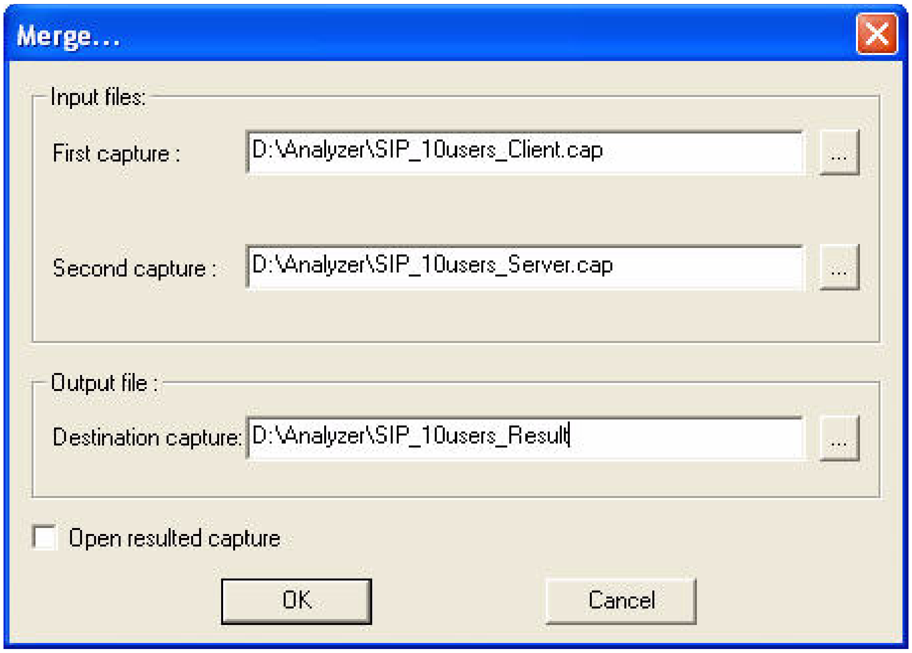
Figure 4-3. Grid Operations Menu

Select the header of Control-Enable column in order to select the entire column.

Grid Operation allows you to perform operations on the selected column as Enable, Disable or Same.

Merge Capture

Analyser has the option of merging two captures. This option will merging two captures.



First capture : D:\Analyzer\SIP_10users_Client.cap

Second capture : D:\Analyzer\SIP_10users_Server.cap

Destination capture: D:\Analyzer\SIP_10users_Result

☐ Open resulted capture

Figure 4-4. Merge Dialog

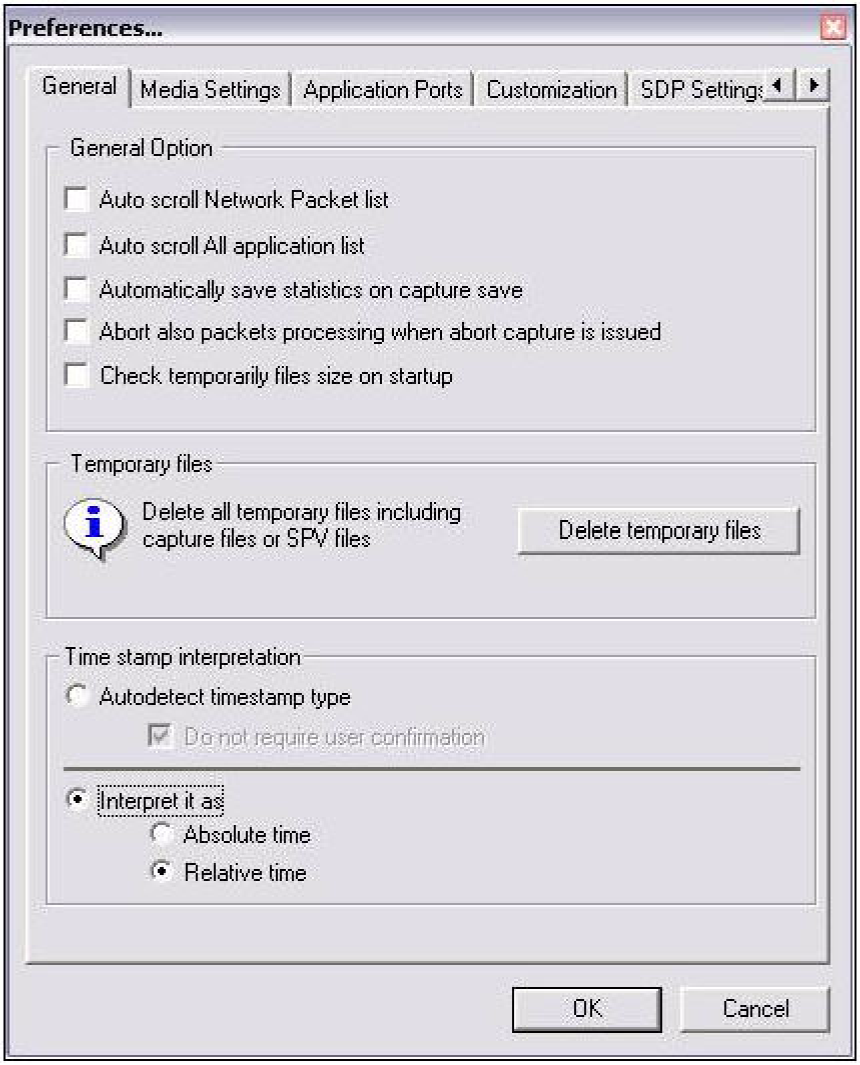
1. Type the path to the first file to merge in the **First capture** field. Alternatively, you can click the ... button to indicate the file's location.
2. Type the path to the second file to merge in the **Second capture** field. Alternatively, you can click the ... button to indicate the file's location.
3. Type the path for the result file in the **Destination Capture** field. Alternatively, you can click the ... button to indicate where you want the file to be saved.
4. Optionally, you can check the Open resulted capture box to automatically open the result file after the merging process is complete.

Click the **OK** button to merge the two files.

> **Note:** Two captures of different types cannot be merged. Both of them must be, for example, Ethernet, or both ATM, and so on. Also, the result file cannot exceed 4 GB.

Preferences

Specify settings for a variety of features.



Preferences...

General | Media Settings | Application Ports | Customization | SDP Setting

General Option

- □ Auto scroll Network Packet list
- □ Auto scroll All application list
- □ Automatically save statistics on capture save
- □ Abort also packets processing when abort capture is issued
- □ Check temporarily files size on startup

Temporary files

Delete all temporary files including capture files or SPV files

Delete temporary files

Time stamp interpretation

- ○ Autodetect timestamp type
  - ☑ Do not require user confirmation
- ● Interpret it as
  - ○ Absolute time
  - ● Relative time

OK Cancel

Figure 4-5. Preferences Window

The following settings are available in the Preferences window:

- *General* – allows you to enable or disable:
    - Auto-scroll for the Network Packets list and for all Application lists – updates packets list as they arrive and are processed by the Analyzer engine;
    - Automatically save statistics on capture save – statistics are saved in .ivu files, saving processing time when captures are subsequently re-opened;
    - Abort also packet processing when abort capture is issued – abort packet processing on the client PC at the same time as capture abort; no further packets are transferred to the Analyzer engine. Capture contains only information up to that moment;
    - Check temporary files size on startup – the temporary files size is verified every time you start the application;
    - Delete temporary files – all .cap files are deleted from the specified location when clicking the **Delete temporary files** button.
    - Time stamp interpretation – has the following options:
        - Autodetect time stamp – Attempts to find out if the capture includes timestamps with an absolute or relative value and interprets them accordingly. The ‘Do not require user confirmation’ checkbox in this section allows you to choose either to be prompted for confirmation of the detected timestamp interpretation (to do this, check the box) or let the application proceed to interpret the timestamps accordingly, without asking for confirmation of the action. By default, the checkbox is selected and no confirmation prompt displays.
        - Interpret it as – Provides two options for interpreting capture time stamps: **Absolute time** and **Relative time**.

> **Note**: *System time* is implemented as a simple count of the number of ticks that have transpired since some arbitrary starting date, called the *epoch*. Usually, systems encode system time as the number of one-second ticks elapsed since the start of the epoch at 1970-01-01 00:00:00.
>
> - *Absolute* time is the representation of time as daylight time.
> - *Relative* time is the time elapsed since an arbitrary starting point. When the capture is done using Analyzer, the starting point is considered to be the moment when the ports timestamps have been last reset, while for other captures that are loaded into Analyzer, the starting point is considered to be at 1970-01-01 00:00:00. For details on resetting ports timestamps, see the corresponding parent application documentation.

- *Media Settings* – allows you to set the **Dejitter** options and modify the **Payload Type Number** for the RTP codecs.
- *Application Ports* – allows you to set the destination ports to be automatically decoded as the specified protocol (for an example of decoding as MPEG, please refer to *MPEG Captures*).

- *Customization* – allows you to enable or disable measurements and protocol analyzers.
    - Measurements checkboxes:
        - Host measurements: enables/disables all measurements in the *Network Hosts* view. When disabled, only the IP, MAC, and Vendor columns have actual values, while the values in all the other columns are 0.
        - Protocol measurements: enables/disables all protocol measurements, both for network and application measurements. When the protocol measurements are disabled, the Network Protocols and the Application Summary views do not display.
        - Statistics: enables/disables the statistics for all the items listed in Table 4-1 on page 4-7.
        - Analyzers – you can enable or disable individual protocol analyzers to conserve resources and speed up packet processing.
- *SDP Settings* – allows you to set the default bit rate for the G.723 codec.

Table 4-1. Columns to which the Statistics checkbox applies

View	Column
Hosts View / Nodes View	Throughput in Throughput out, Packets in per sec Packets out per sec Throughput in medium Throughput in minimum Throughput in maximum Throughput out medium Throughput out minimum Throughput out maximum Bytes sent percent Bytes received percent
Summary View	Endpoints Conversations Control Errors Utilization Failed Successful Connected BHCC BHCA

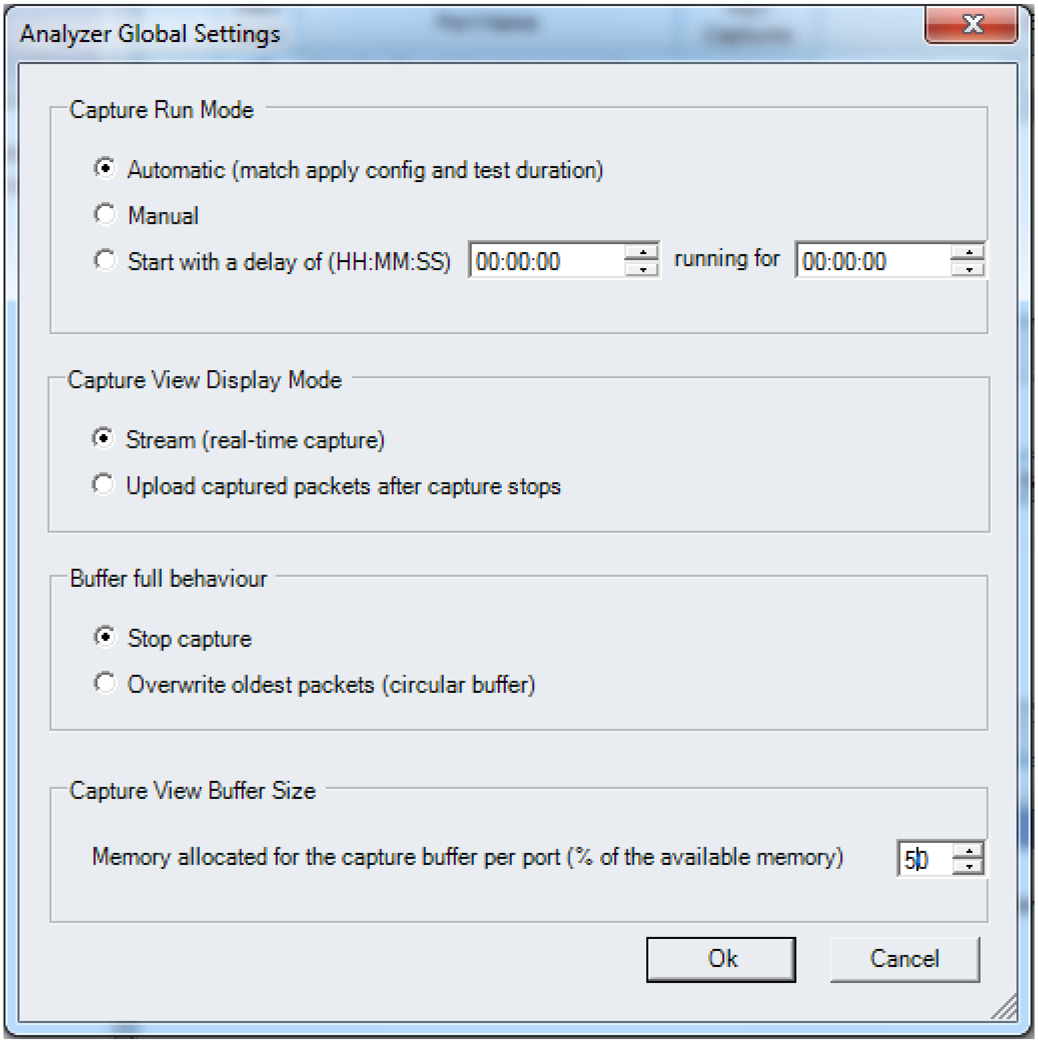
Table 4-1. Columns to which the Statistics checkbox applies

View	Column
Endpoints View secondary list	BHCA BHCC Utilization
Hosts View / Nodes View / Network Protocol View secondary lists	Bytes Send (%) Bytes Rcv (%)

Capture Settings

Capture Settings allows you to configure the following global parameters for Analyzer:

- Capture Run Mode,
- Capture View Display mode,
- Buffer full behavior and
- Capture Buffer Size.



Analyzer Global Settings

Capture Run Mode

● Automatic (match apply config and test duration)

○ Manual

○ Start with a delay of (HH:MM:SS) 00:00:00 running for 00:00:00

Capture View Display Mode

● Stream (real-time capture)

○ Upload captured packets after capture stops

Buffer full behaviour

● Stop capture

○ Overwrite oldest packets (circular buffer)

Capture View Buffer Size

Memory allocated for the capture buffer per port (% of the available memory) 50

Figure 4-6. Capture Settings Window

All these settings can be changed only after the test was stopped and Release Config per port was also complete.

Capture Run Mode: User has the option of tracking the capture in both Automatic or in manual mode. User can also start the capture with a delay. In addition, time duration for capture must also be mentioned.

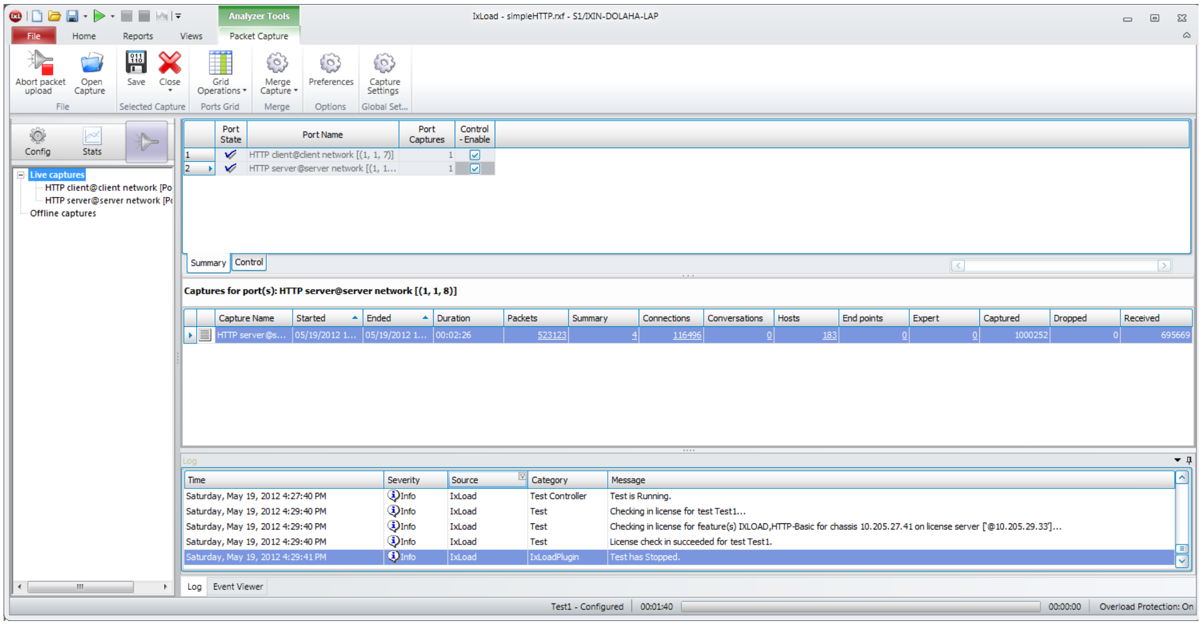
Capture View Display Mode: User has the option to choose how and when the packets should be displayed in the GUI, during real-time or after the capture stops.

Buffer Full Behaviour: When the buffer is full, user can have two options. Either stop the capture or overwrite oldest packets in the buffer.

Capture View Buffer size: User has the option of configuring the memory allocation for the capture buffer per port.

Application Viewers

The application viewers can be easily accessed by using the navigation toolbox links in the left pane. The navigation toolbox is a custom control that acts like a TAB control with three major categories: Applications, Network, and Physical, as shown in following figure. It shows the number of items in each view.



	Port State	Port Name	Port Captures	Control - Enable
1	✓	HTTP client@client network [(1, 1, 7)]	1	☑
2	✓	HTTP server@server network [(1, 1...	1	☑

Captures for port(s): HTTP server@server network [(1, 1, 8)]

Capture Name	Started	Ended	Duration	Packets	Summary	Connections	Conversations	Hosts	End points	Expert	Captured	Dropped	Received
HTTP server@s...	05/19/2012 1...	05/19/2012 1...	00:02:26	523123	4	116496	0	183	0	0	1000252	0	695669

Time	Severity	Source	Category	Message
Saturday, May 19, 2012 4:27:40 PM	Info	IxLoad	Test Controller	Test is Running.
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for test Test1...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for feature(s) IXLOAD,HTTP-Basic for chassis 10.205.27.41 on license server ['@10.205.29.33']...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	License check in succeeded for test Test1.
Saturday, May 19, 2012 4:29:41 PM	Info	IxLoad	IxLoadPlugin	Test has Stopped.

Figure 4-7. Summary Screen

The main viewer categories that can be accessed from the Navigation Toolbox are:

- **Application:**
  - **Summary** – points to the *Application Summary* view.
  - **Conversation –** points to the *Application Conversations* view.
  - **Endpoints** – points to the *Application Endpoint* view.
  - **Expert** – points to the *Application Expert Log* view.
- **Network:**
  - **Packets** – points to the *Network Packet* view.
  - **Connections** – points to the *Network Connections* view.
  - **Hosts** – points to the *Network Hosts* view.
  - **Protocols** – points to the *Protocols* view.
- **Physical:**
  - **Nodes** – points to the *Nodes* list view.

The main application viewers described in this section are:

- *Application Layer Views* on page 4-11.
- *Network Layer Views* on page 4-18.
- *Physical Layer View* on page 4-23.
- *Common View* on page 4-23.
- *Packet Tree View* on page 4-27.
- *Capture Statistics View* on page 4-27.

Application Layer Views

The Application Layer views are available for the SIP, MGCP, RTP, and MPEG Video protocols.

The default application ports are the ones listed in Table 4-2.

Table 4-2. Default Application Ports

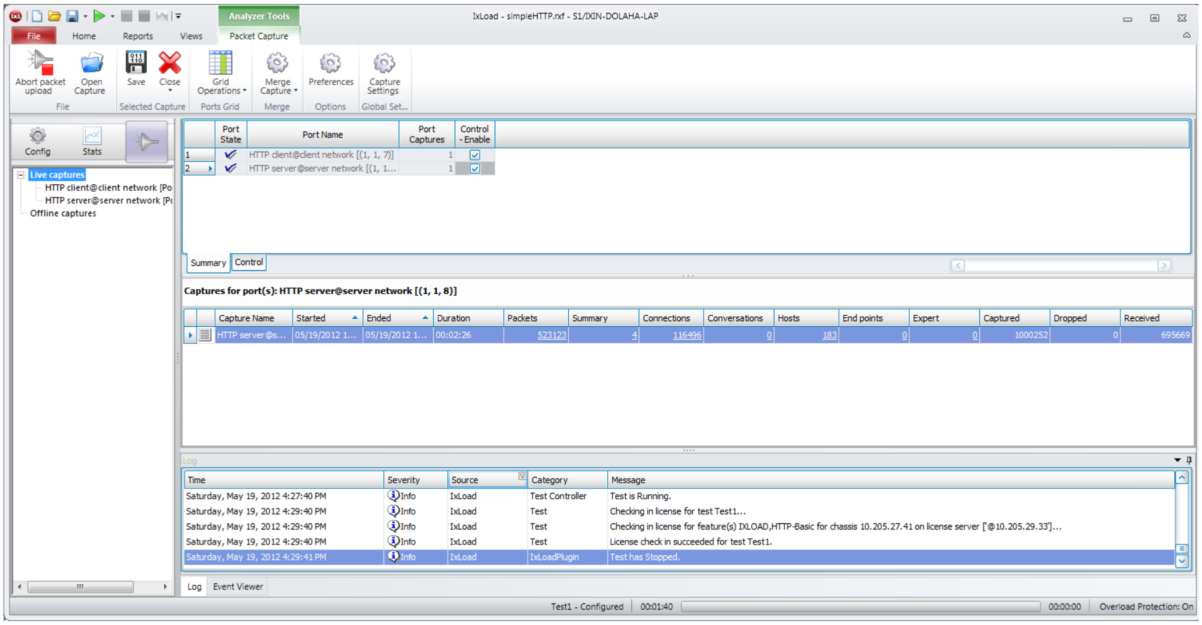
Application Protocol	Port
SIP	5060
MGCP	2427
MGCP	2428
MGCP	2727
MGCP	2728

The Application views are:

- *Application Summary*.
- *Application Conversations* on page 4-13.
- *Application Endpoints* on page 4-14.
- *Application Expert* on page 4-16.

Application Summary

The *Application Summary* view shows the global protocol statistics from the application layer point of view, as shown in the following figure:



	Port State	Port Name	Port Captures	Control - Enable
1	✓	HTTP client@client network [(1, 1, 7)]	1	☑
2	✓	HTTP server@server network [(1, 1...	1	☑

Captures for port(s): HTTP server@server network [(1, 1, 8)]

Capture Name	Started	Ended	Duration	Packets	Summary	Connections	Conversations	Hosts	End points	Expert	Captured	Dropped	Received
HTTP server@s...	05/19/2012 1...	05/19/2012 1...	00:02:26	523123	4	116496	0	183	0	0	1000252	0	695669

Log

Time	Severity	Source	Category	Message
Saturday, May 19, 2012 4:27:40 PM	Info	IxLoad	Test Controller	Test is Running.
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for test Test1...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for feature(s) IXLOAD,HTTP-Basic for chassis 10.205.27.41 on license server ['@10.205.29.33']...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	License check in succeeded for test Test1.
Saturday, May 19, 2012 4:29:41 PM	Info	IxLoad	IxLoadPlugin	Test has Stopped.

Test1 - Configured | 00:01:40 | 00:00:00 | Overload Protection: On

Figure 4-8. Application Summary View

Each protocol is highlighted using a specific color:

- SIP, MGCP– Green
- RTP – Blue
- MPEG – Orange
- Protocol Error – Red
- Others – White

> **Note:** The color representation listed above is valid for all the viewers in Analyzer, except for Protocol Error and Others, which are shown only in the packets list.

For each protocol, the statistics listed in Table 4-3 are provided:

Table 4-3. Application Summary Counters

Counter	Description
Bytes	The total number of bytes transferred during the capture.
Packets	The total number of packets transferred during the capture.
Retransmissions	The total number of retransmissions performed during the capture.
Errors	The total number of errors occurred during the capture.

Table 4-3. Application Summary Counters (Continued)

Counter	Description
Endpoints	The number of endpoints involved in the captured session.
Conversations	The total number of conversations performed during the capture.
Attempted	The number of conversations attempted during the capture.
Connected	The number of conversations connected during the capture.
Successful	The number of conversations successfully connected and completed during the capture.
Failed	The number of conversations that failed during the capture.
Utilization(%)	The percentage of bytes transferred.
BHCA	Busy Hour Call Attempts.
BHCC	Busy Hour Call Completions.

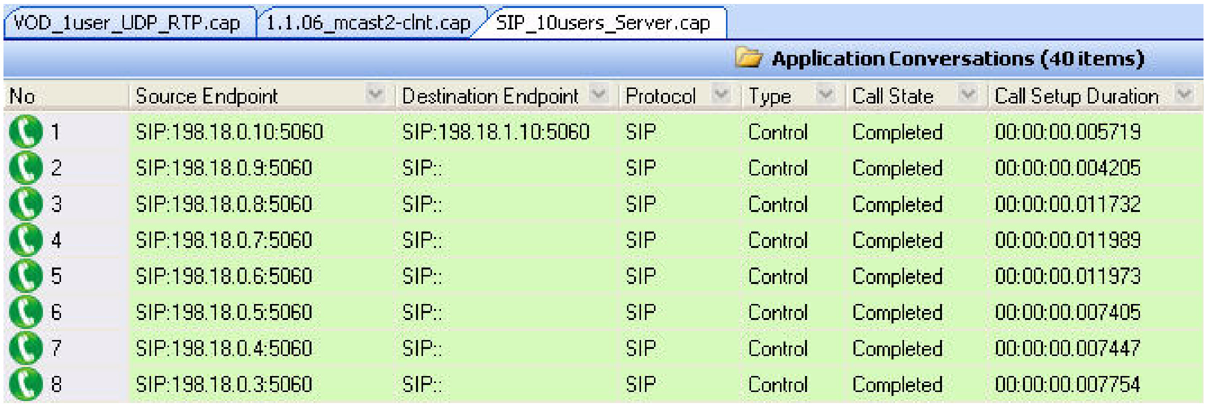
Selecting a protocol updates the *Common View* containing the related *Endpoints, Conversations, Errors.*

The three tabs in the *Common View* have links to their respective views (*Application Conversations/Application Endpoints* and *Application Expert*). Also, the significant columns in each list have links to their related views (that is, on the conversation list, the source and destination columns allow quick jumps to the corresponding *Application Endpoints* view).

No information is available in the *Packet Tree* view for *Application Summary.*

Application Conversations

The *Conversations* view displays a list of conversations (calls, streams, transactions, and so on) in progress, established or cleared for the network capture, as shown in Figure 4-9.



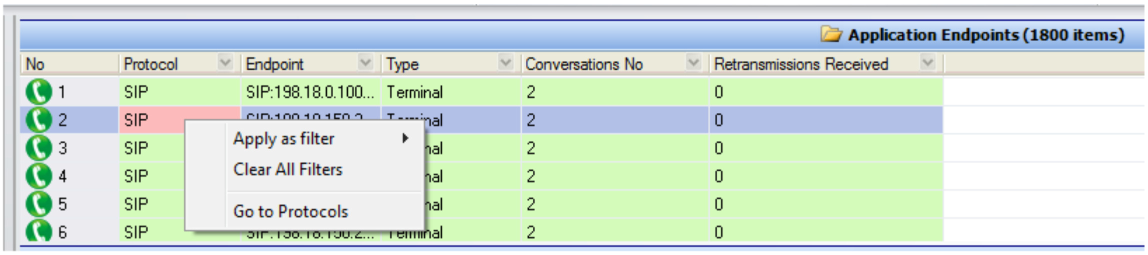
Application Conversations (40 items)

No	Source Endpoint	Destination Endpoint	Protocol	Type	Call State	Call Setup Duration
☎ 1	SIP:198.18.0.10:5060	SIP:198.18.1.10:5060	SIP	Control	Completed	00:00:00.005719
☎ 2	SIP:198.18.0.9:5060	SIP::	SIP	Control	Completed	00:00:00.004205
☎ 3	SIP:198.18.0.8:5060	SIP::	SIP	Control	Completed	00:00:00.011732
☎ 4	SIP:198.18.0.7:5060	SIP::	SIP	Control	Completed	00:00:00.011989
☎ 5	SIP:198.18.0.6:5060	SIP::	SIP	Control	Completed	00:00:00.011973
☎ 6	SIP:198.18.0.5:5060	SIP::	SIP	Control	Completed	00:00:00.007405
☎ 7	SIP:198.18.0.4:5060	SIP::	SIP	Control	Completed	00:00:00.007447
☎ 8	SIP:198.18.0.3:5060	SIP::	SIP	Control	Completed	00:00:00.007754

Figure 4-9. Application Conversations

Selecting a conversation updates the *Common View* (*Flow Summary, Ladder Diagram*) and the *Packet Tree* views.

Link to the *Endpoints* and the *Protocols* view by right-clicking an item in the *Source/Destination Endpoints* columns or an item in the *Protocol* column, as shown in the following figure



Application Endpoints (1800 items)

No	Protocol	Endpoint	Type	Conversations No	Retransmissions Received
1	SIP	SIP:198.18.0.100...	Terminal	2	0
2	SIP	SIP:198.18.150.2	Terminal	2	0
3	SIP		nal	2	0
4	SIP		nal	2	0
5	SIP		nal	2	0
6	SIP	SIP:198.18.150.2...	Terminal	2	0

Figure 4-10. Link from Application Conversations View to Endpoints View

The *Packet Tree* view displays the selected ladder packet or the first conversation packet, if the ladder tab is not active.

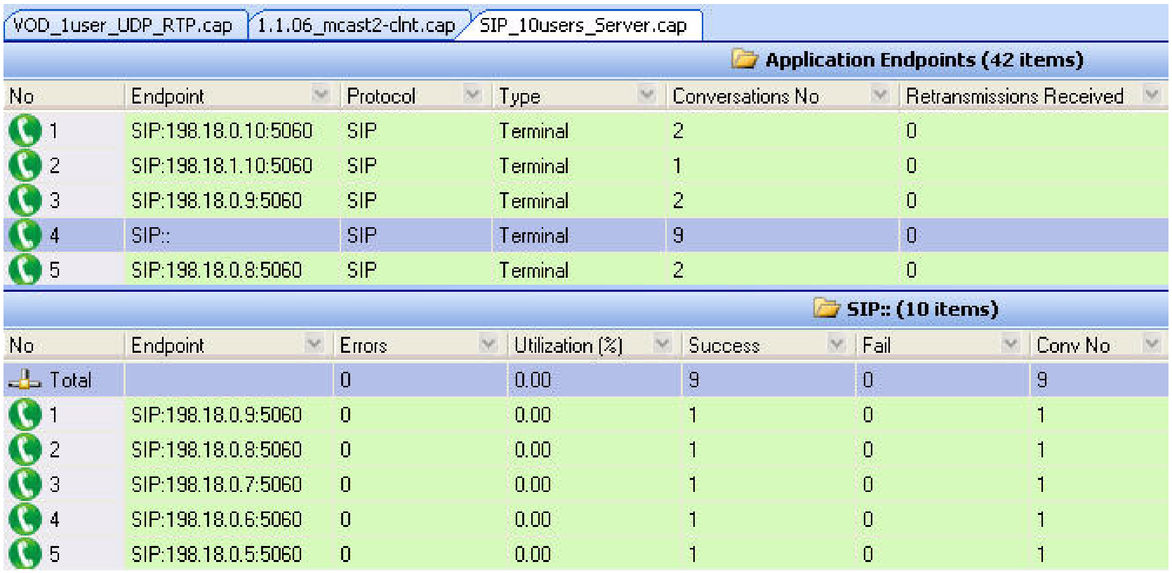
For each conversation, the statistics listed in Table 4-4 are provided.

Table 4-4. Application Conversations Statistics

Counter	Description
Protocol	The protocol used for message exchange.
Call State	The instantaneous call state of the conversation.
Type	The type of conversation.
Destination Endpoint	The receive endpoint of the call.
Source Endpoint	The originating endpoint of the call.
Protocol Specific Counters (SIP Calls, RTP Streams, MPEG, MGCP Calls)	For details about the protocol-specific counters, please refer to: - Chapter 5, *SIP Captures* - Chapter 6, *MGCP Captures* - Chapter 7, *MPEG Captures* - Chapter 8, *RTP Captures*.
Conversations	*Duration* – the conversation duration (that is, the time elapsed between *Start Time* and *Last Time*) *Start Time* – the timestamp for the conversation start *End Time* – the timestamp for the conversation end

Application Endpoints

The *Application Endpoints* view provides a list of all the endpoints involved in the conversations during the capture. For each endpoint, this view also provides a list of all the other endpoints with which it has communicated during the capture, as shown in the following figure.



Application Endpoints (42 items)

No	Endpoint	Protocol	Type	Conversations No	Retransmissions Received
1	SIP:198.18.0.10:5060	SIP	Terminal	2	0
2	SIP:198.18.1.10:5060	SIP	Terminal	1	0
3	SIP:198.18.0.9:5060	SIP	Terminal	2	0
4	SIP::	SIP	Terminal	9	0
5	SIP:198.18.0.8:5060	SIP	Terminal	2	0

SIP:: (10 items)

No	Endpoint	Errors	Utilization (%)	Success	Fail	Conv No
Total		0	0.00	9	0	9
1	SIP:198.18.0.9:5060	0	0.00	1	0	1
2	SIP:198.18.0.8:5060	0	0.00	1	0	1
3	SIP:198.18.0.7:5060	0	0.00	1	0	1
4	SIP:198.18.0.6:5060	0	0.00	1	0	1
5	SIP:198.18.0.5:5060	0	0.00	1	0	1

Figure 4-11. Application Endpoints View

The parameters listed in Table 4-5 are provided for each endpoint in the first list of the *Application Endpoints* view.

Table 4-5. Application Endpoints Parameters - First List Parameters

Counter	Description
Endpoint	The endpoint name.
Protocol	The protocol used by the endpoint.
Type	The endpoint type.
Conversation No	The number of conversations in which the endpoint was involved, during the capture.
Retransmissions Received	The number of retransmission received by the endpoint during the capture.

Selecting an endpoint updates the list of endpoints with which the selected endpoint had conversations.

The second endpoints list contains only the endpoints that share conversations with the selected endpoint, providing useful statistics related to the selected endpoint from the first list, as described in Table 4-6.

Table 4-6. Application Endpoints - Second List Parameters

Counter	Description
Endpoint	The endpoint name.
Errors	The number of errors that occurred in the conversations between the endpoints.

Table 4-6. Application Endpoints - Second List Parameters (Continued)

Counter	Description
Utilization (%)	The percentage of packets exchanged between the endpoint in the first list and the selected endpoint in the second list.
Success	The number of successfully competed conversations between the two selected endpoints.
Fail	The number of conversations between the two endpoints that did not complete successfully.
Control	The number of call control conversations performed during the capture.
Conv No	The total number of conversations in which the two endpoints took part.
BHCC	Busy Hour Call Completions.
BHCA	Busy Hour Call Attempts.

The *Common View* panel displays the errors, conversations, and ladder diagram related to the selected endpoint from the first and second endpoint lists.

Every list in this view offers links to the views associated with the important columns (conversations and protocols).

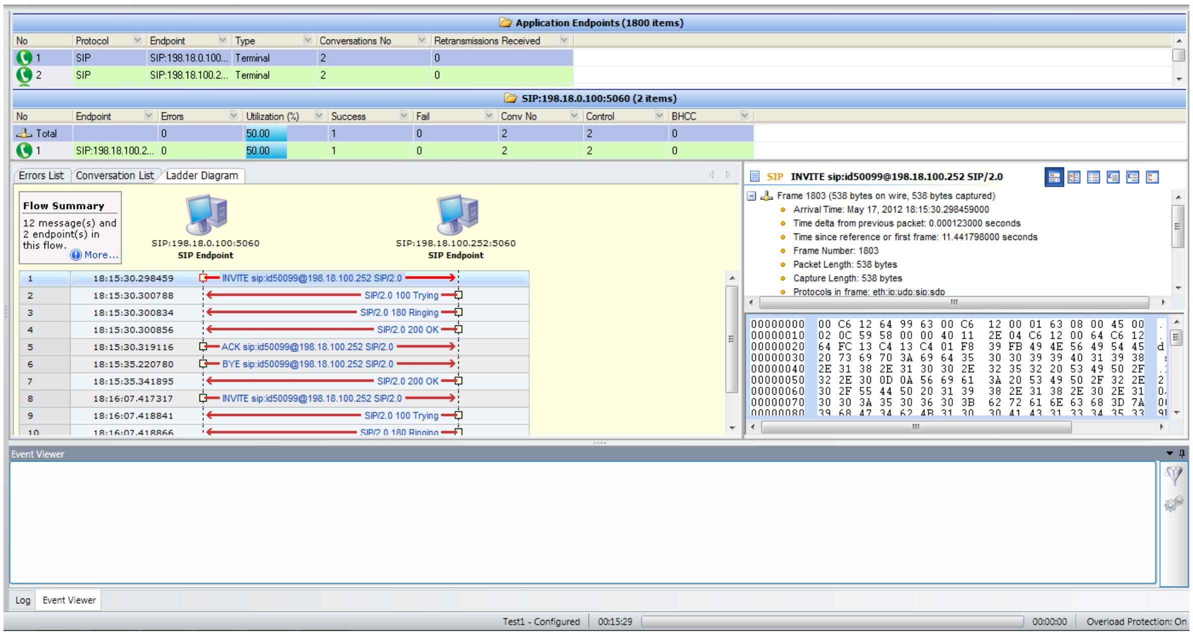
The *Packet Tree* view displays the selected ladder packet or the first packet of the first conversation between the selected endpoints.

Application Expert

The *Application Expert Log* view provides details about the errors and events logged by the analyzer during the capture.

Selecting an error updates the bottom area, which contains the flow summary, ladder diagram, and packet tree (or other specialized lists, if present) for the conversation related to the selected error/event.

The Application Expert Log links to the source or destination endpoint, as well as to the protocol as shown in the following figure.



Application Endpoints (1800 items)

No	Protocol	Endpoint	Type	Conversations No	Retransmissions Received
1	SIP	SIP:198.18.0.100...	Terminal	2	0
2	SIP	SIP:198.18.100.2...	Terminal	2	0

SIP:198.18.0.100:5060 (2 items)

No	Endpoint	Errors	Utilization (%)	Success	Fail	Conv No	Control	BHCC
Total		0	50.00	1	0	2	2	0
1	SIP:198.18.100.2...	0	50.00	1	0	2	2	0

Flow Summary

12 message(s) and 2 endpoint(s) in this flow.

More...

SIP:198.18.0.100:5060 SIP Endpoint

SIP:198.18.100.252:5060 SIP Endpoint

1	18:15:30.298459	INVITE sip:id50099@198.18.100.252 SIP/2.0
2	18:15:30.300788	SIP/2.0 100 Trying
3	18:15:30.300834	SIP/2.0 180 Ringing
4	18:15:30.300856	SIP/2.0 200 OK
5	18:15:30.319116	ACK sip:id50099@198.18.100.252 SIP/2.0
6	18:15:35.220780	BYE sip:id50099@198.18.100.252 SIP/2.0
7	18:15:35.341895	SIP/2.0 200 OK
8	18:16:07.417317	INVITE sip:id50099@198.18.100.252 SIP/2.0
9	18:16:07.418841	SIP/2.0 100 Trying
10	18:16:07.418866	SIP/2.0 180 Ringing

SIP INVITE sip:id50099@198.18.100.252 SIP/2.0

- Frame 1803 (538 bytes on wire, 538 bytes captured)
  - Arrival Time: May 17, 2012 18:15:30.298459000
  - Time delta from previous packet: 0.000123000 seconds
  - Time since reference or first frame: 11.441798000 seconds
  - Frame Number: 1803
  - Packet Length: 538 bytes
  - Capture Length: 538 bytes
  - Protocols in frame: eth:ip:udp:sip:sdp

```
00000000  00 C6 12 64 99 63 00 C6  12 00 01 63 08 00 45 00
00000010  02 0C 59 58 00 00 40 11  2E 04 C6 12 00 64 C6 12
00000020  64 FC 13 C4 13 C4 01 F8  39 FB 49 4E 56 49 54 45
00000030  20 73 69 70 3A 69 64 35  30 30 39 39 40 31 39 38
00000040  2E 31 38 2E 31 30 30 2E  32 35 32 20 53 49 50 2F
00000050  32 2E 30 0D 0A 56 69 61  3A 20 53 49 50 2F 32 2E
00000060  30 2F 55 44 50 20 31 39  38 2E 31 38 2E 30 2E 31
00000070  30 30 3A 35 30 36 30 3B  62 72 61 6E 63 68 3D 7A
00000080  39 68 47 34 62 4B 31 30  30 41 43 31 33 34 35 33
```

Test1 - Configured | 00:15:29 | 00:00:00 | Overload Protection: On

Figure 4-12. Application Expert View

The parameters shown in the Application Expert Log view are listed in Table 4-7.

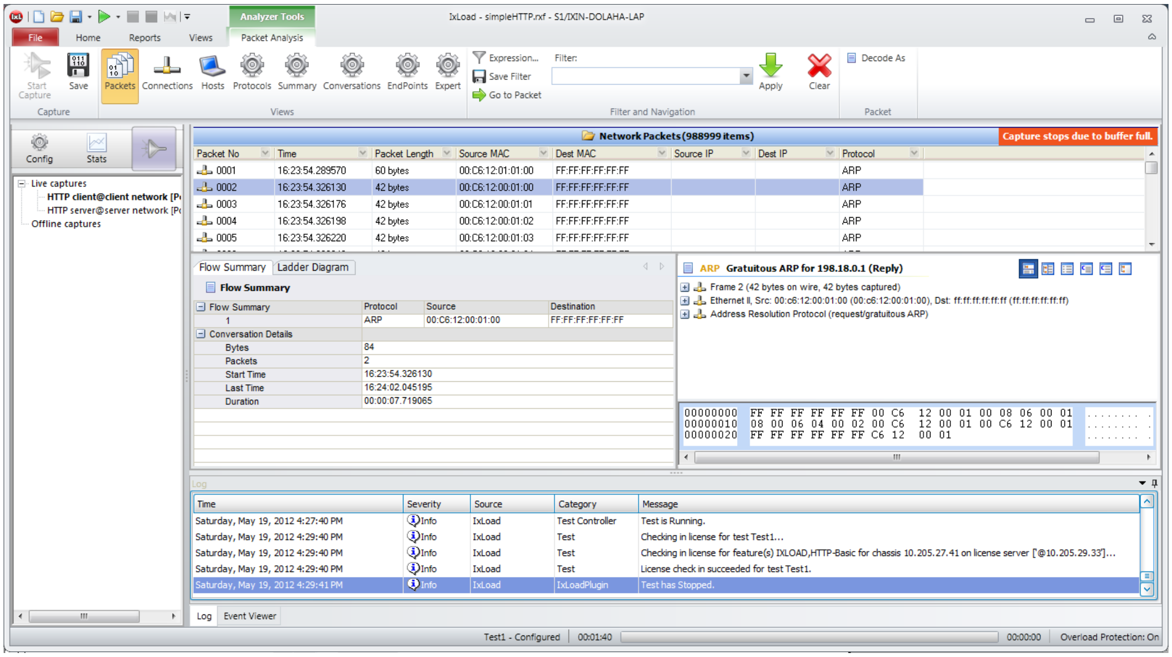
Table 4-7. Application Expert Log Parameters

Parameter	Description
Name	Error name
Description	Error details
Source Host	The IP address of the source host
Destination Host	The IP address of the destination host
Source Endpoint	The identifier of the source endpoint
Destination Endpoint	The identifier of the destination endpoint
Time	The timestamp when the error occurred. For information about timestamp interpretation.
Protocol	The protocol used for the conversation in which the error was encountered
Severity	The error severity. One of: *Warning* – highlighted in the Packet Tree view in yellow *Error* – highlighted in the Packet Tree view in red *Informational* – highlighted in the Packet Tree view in light blue

Network Layer Views

Network Packets

The *Network Packets* view provides a complete list of all packets exchanged during the capture, as shown in the following figure.



Network Packets (988999 items) — Capture stops due to buffer full.

Packet No	Time	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol
0001	16:23:54.289570	60 bytes	00:C6:12:01:01:00	FF:FF:FF:FF:FF:FF			ARP
0002	16:23:54.326130	42 bytes	00:C6:12:00:01:00	FF:FF:FF:FF:FF:FF			ARP
0003	16:23:54.326176	42 bytes	00:C6:12:00:01:01	FF:FF:FF:FF:FF:FF			ARP
0004	16:23:54.326198	42 bytes	00:C6:12:00:01:02	FF:FF:FF:FF:FF:FF			ARP
0005	16:23:54.326220	42 bytes	00:C6:12:00:01:03	FF:FF:FF:FF:FF:FF			ARP

Flow Summary

Flow Summary	Protocol	Source	Destination
1	ARP	00:C6:12:00:01:00	FF:FF:FF:FF:FF:FF
Conversation Details			
Bytes	84		
Packets	2		
Start Time	16:23:54.326130		
Last Time	16:24:02.045195		
Duration	00:00:07.719065		

ARP Gratuitous ARP for 198.18.0.1 (Reply)

- Frame 2 (42 bytes on wire, 42 bytes captured)
- Ethernet II, Src: 00:c6:12:00:01:00 (00:c6:12:00:01:00), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request/gratuitous ARP)

```
00000000  FF FF FF FF FF FF 00 C6  12 00 01 00 08 06 00 01  ........ .
00000010  08 00 06 04 00 02 00 C6  12 00 01 00 C6 12 00 01  ........ .
00000020  FF FF FF FF FF FF C6 12  00 01                    ........ .
```

Log

Time	Severity	Source	Category	Message
Saturday, May 19, 2012 4:27:40 PM	Info	IxLoad	Test Controller	Test is Running.
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for test Test1...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for feature(s) IXLOAD,HTTP-Basic for chassis 10.205.27.41 on license server ['@10.205.29.33']...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	License check in succeeded for test Test1.
Saturday, May 19, 2012 4:29:41 PM	Info	IxLoad	IxLoadPlugin	Test has Stopped.

Test1 - Configured | 00:01:40 | 00:00:00 | Overload Protection: On

Figure 4-13. Network Packets View

Selecting a packet updates the *Common View* (*Flow Summary* and *Ladder Diagram*) and the *Packet Tree* view.

The *Network Packets* view contains links to the *Network Hosts* view and to the *Network Protocols* view. You can access the *Network Hosts* view by right-clicking an item in the *Source* or *Destination* fields and by selecting **Go to Hosts.** To access the *Network Protocols* view, right-click an item in the *Protocol* field and select **Go to Protocols**, as shown in the following figure.

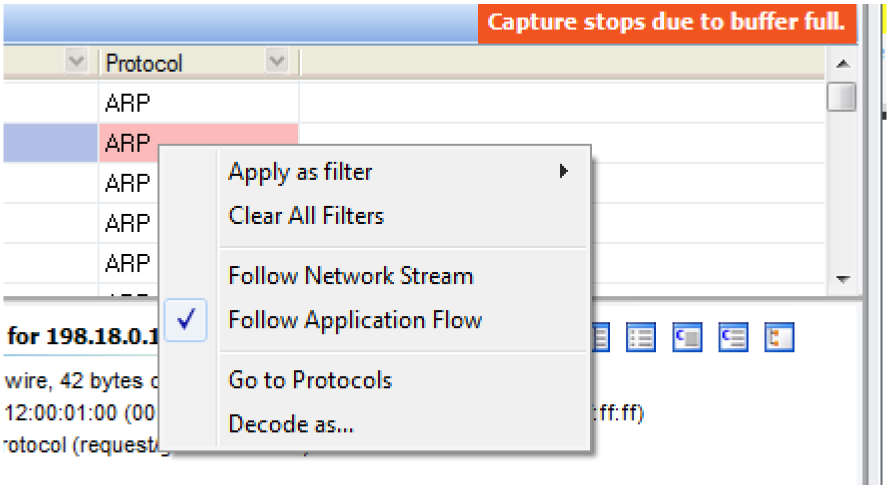


Figure 4-14. Link to Network Protocols View.

By right-clicking an item in the *Source*, *Destination*, or *Protocol* field, you can also choose to **Follow Network Stream** or **Follow Application Flow** in the ladder diagram, as shown in Figure 4-14. The **Decode as...** right-click option is also available, as described in *Decoding Packets* on page 4-31.

The **Export Packet** option allows you to save the selected packet as a *.ixnsc* file. You can open this file in IxLoad's *Packet Designer*, where you can customize the packet. For more details about editing packets, see the *IxLoad User Guide*.

The packet tree shows the selected packet in the Ladder Diagram*,* if active.

For each packet, the packet properties listed in Table 4-8 are provided.

Table 4-8. Network Packets Properties

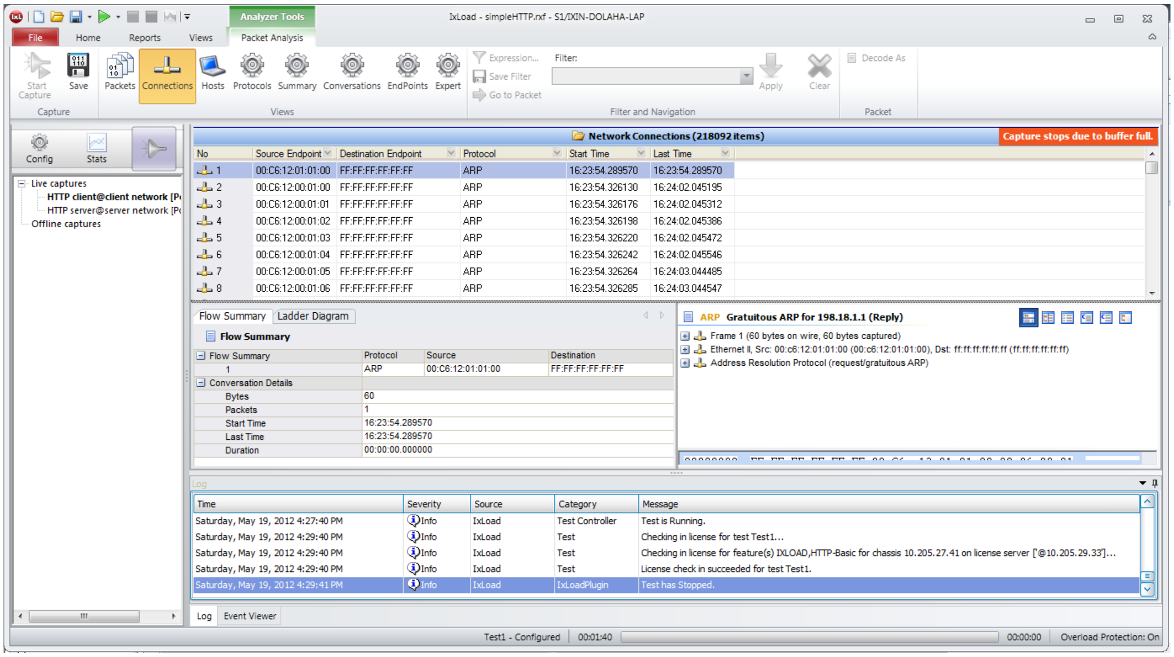
Counter	Description
Packet No	The packet number.
Time	The timestamp of the packet. For information on timestamp interpretation.
Source	The source IP address.
Destination	The destination IP address.
Delta Time	The time difference between the timestamp of the current packet and the previous packet. **NOTE:** This property is called *Delta Time* in IxLoad and *Timestamp - Relative to previous* in IxExplorer.
Source Port	The source port number.
Destination Port	The destination port number.
Packet Length	The packet length, in bytes.
Protocol	The protocol used.

Table 4-8. Network Packets Properties (Continued)

Counter	Description
Packet Summary	Some details related to the type of message and its syntax.
Source MAC	The source MAC address.
Destination MAC	The destination MAC address.
Source IP	The IP address of the source endpoint.
Dest IP	The IP address of the destination endpoint.
Relative Time	The timestamp of the packet related to the timestamp of the first packet. **NOTE:** This property is called *Relative Time* in IxLoad and *Timestamp - Relative to first* in IxExplorer.
Timestamp - From last clear	The timestamp of the packet related to the timestamp of the port's last clear. **NOTE:** This property is available only in IxExplorer.

Network Connections

The *Network Connections* view lists all the connections established between hosts and a few details for each, as shown in the following figure:



Network Connections (218092 items)

No	Source Endpoint	Destination Endpoint	Protocol	Start Time	Last Time
1	00:C6:12:01:01:00	FF:FF:FF:FF:FF:FF	ARP	16:23:54.289570	16:23:54.289570
2	00:C6:12:00:01:00	FF:FF:FF:FF:FF:FF	ARP	16:23:54.326130	16:24:02.045195
3	00:C6:12:00:01:01	FF:FF:FF:FF:FF:FF	ARP	16:23:54.326176	16:24:02.045312
4	00:C6:12:00:01:02	FF:FF:FF:FF:FF:FF	ARP	16:23:54.326198	16:24:02.045386
5	00:C6:12:00:01:03	FF:FF:FF:FF:FF:FF	ARP	16:23:54.326220	16:24:02.045472
6	00:C6:12:00:01:04	FF:FF:FF:FF:FF:FF	ARP	16:23:54.326242	16:24:02.045546
7	00:C6:12:00:01:05	FF:FF:FF:FF:FF:FF	ARP	16:23:54.326264	16:24:03.044485
8	00:C6:12:00:01:06	FF:FF:FF:FF:FF:FF	ARP	16:23:54.326285	16:24:03.044547

Flow Summary | Ladder Diagram

Flow Summary

Flow Summary	Protocol	Source	Destination
1	ARP	00:C6:12:01:01:00	FF:FF:FF:FF:FF:FF
Conversation Details			
Bytes	60		
Packets	1		
Start Time	16:23:54.289570		
Last Time	16:23:54.289570		
Duration	00:00:00.000000		

ARP Gratuitous ARP for 198.18.1.1 (Reply)

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 00:c6:12:01:01:00 (00:c6:12:01:01:00), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request/gratuitous ARP)
```

Time	Severity	Source	Category	Message
Saturday, May 19, 2012 4:27:40 PM	Info	IxLoad	Test Controller	Test is Running.
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for test Test1...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for feature(s) IXLOAD,HTTP-Basic for chassis 10.205.27.41 on license server ['@10.205.29.33']...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	License check in succeeded for test Test1.
Saturday, May 19, 2012 4:29:41 PM	Info	IxLoad	IxLoadPlugin	Test has Stopped.

Test1 - Configured | 00:01:40 | 00:00:00 | Overload Protection: On

Figure 4-15. Network Connections View

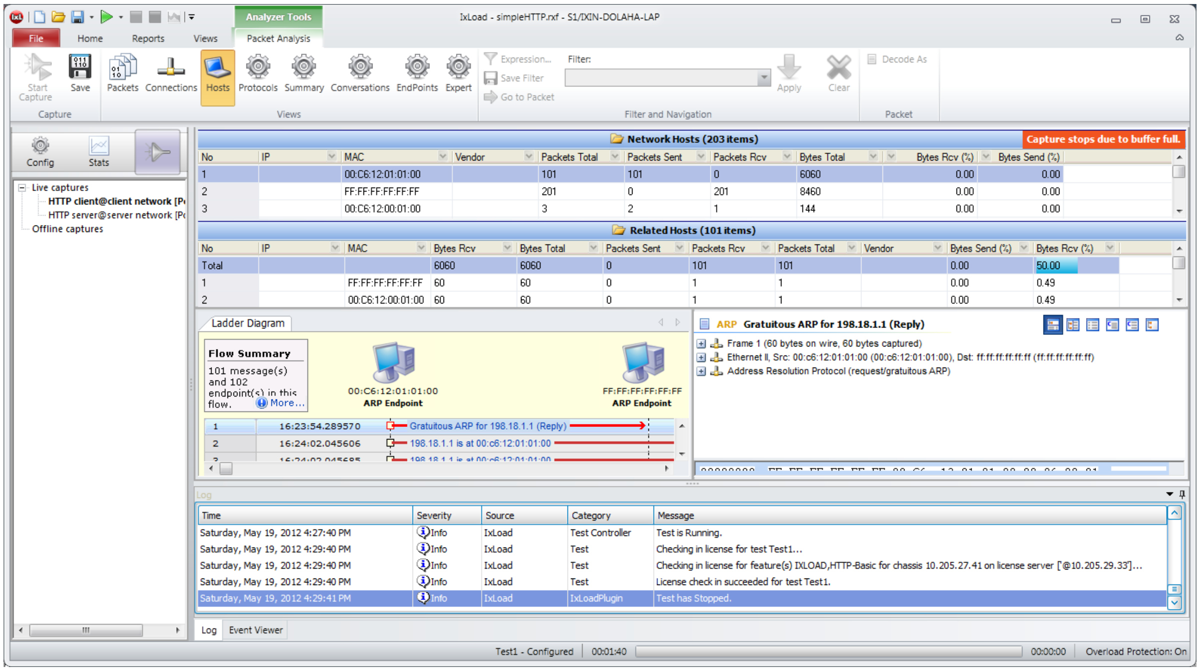
Selecting a connection updates the *Common View* (*Flow Summary* and *Ladder Diagram*).

The *Packet Tree* view shows the first packet of a connection or the selected packet in the *Ladder Diagram,* if active.

Network Hosts

The *Network Hosts* and *Related Hosts* views show details about the hosts of a network connection identified by IP Address and/or MAC Address. This view is similar to the *Application Endpoints* view.

Selecting a host updates the list of hosts with which the selected host exchanged packets, as shown in the following fiure:



Network Hosts (203 items)

No	IP	MAC	Vendor	Packets Total	Packets Sent	Packets Rcv	Bytes Total	Bytes Rcv (%)	Bytes Send (%)
1		00:C6:12:01:01:00		101	101	0	6060	0.00	0.00
2		FF:FF:FF:FF:FF:FF		201	0	201	8460	0.00	0.00
3		00:C6:12:00:01:00		3	2	1	144	0.00	0.00

Related Hosts (101 items)

No	IP	MAC	Bytes Rcv	Bytes Total	Packets Sent	Packets Rcv	Packets Total	Vendor	Bytes Send (%)	Bytes Rcv (%)
Total			6060	6060	0	101	101		0.00	50.00
1		FF:FF:FF:FF:FF:FF	60	60	0	1	1		0.00	0.49
2		00:C6:12:00:01:00	60	60	0	1	1		0.00	0.49

Flow Summary
101 message(s) and 102 endpoint(s) in this flow. More...

00:C6:12:01:01:00 ARP Endpoint — FF:FF:FF:FF:FF:FF ARP Endpoint

1	16:23:54.289570	Gratuitous ARP for 198.18.1.1 (Reply)
2	16:24:02.045606	198.18.1.1 is at 00:c6:12:01:01:00

ARP Gratuitous ARP for 198.18.1.1 (Reply)
- Frame 1 (60 bytes on wire, 60 bytes captured)
- Ethernet II, Src: 00:c6:12:01:01:00 (00:c6:12:01:01:00), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request/gratuitous ARP)

Time	Severity	Source	Category	Message
Saturday, May 19, 2012 4:27:40 PM	Info	IxLoad	Test Controller	Test is Running.
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for test Test1...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	Checking in license for feature(s) IXLOAD,HTTP-Basic for chassis 10.205.27.41 on license server ['@10.205.29.33']...
Saturday, May 19, 2012 4:29:40 PM	Info	IxLoad	Test	License check in succeeded for test Test1.
Saturday, May 19, 2012 4:29:41 PM	Info	IxLoad	IxLoadPlugin	Test has Stopped.

Test1 - Configured | 00:01:40 | 00:00:00 | Overload Protection: On

Figure 4-16. Network Hosts View

For each host, the parameters listed in Table 4-9 are provided.

Table 4-9. Network Hosts Parameters

Counter	Description
IP	The host IP address
MAC	The host MAC address
Vendor	The device vendor
Bytes Sent	The total number of bytes sent by the host
Bytes Rcv	The total number of bytes received by the host
Bytes Total	The total number of bytes sent and received by the host
Packets Sent	The total number of packets sent by the host

Table 4-9. Network Hosts Parameters (Continued)

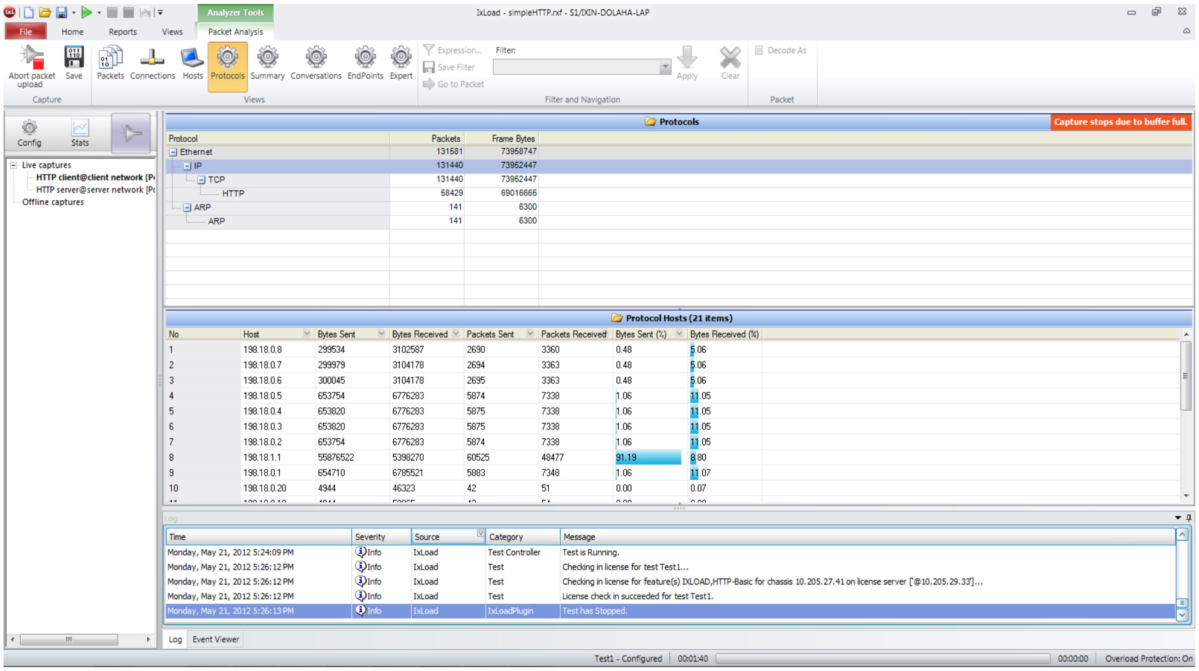
Counter	Description
Packets Rcv	The total number of packets received by the host
Packets Total	The total number of packets sent and received by the host
Bytes Send (%)	The percentage of bytes sent by the host out of the total number of bytes sent by all the hosts
Bytes Rcv (%)	The percentage of bytes received by the host out of the total number of bytes received by all the hosts
First Send Time	The timestamp when the host sends the first packet.
Last Send Time	The timestamp when the host sends its last packet.
First Rcv Time	The moment of time when the host received its first packet.
Last Rcv Time	The timestamp when the host received its last packet.
Throughput In (kbps)	The traffic rate to the host
Throughput Out (kbps)	The traffic rate from the host
Throughput In Min (kbps)	The minimum traffic rate (in kb/s) to the host
Throughput Out Min (kbps)	The minimum traffic rate (in kb/s) from the host
Throughput In Max (kbps)	The maximum traffic rate (in kb/s) to the host
Throughput Out Max (kbps)	The maximum traffic rate (in kb/s) from the host
Med In Throughput (kbps)	An average traffic rate (in kb/s) to the host
Med Out Throughput (kbps)	An average traffic rate (in kb/s) from the host
Packets In / Sec	The average received packets per second
Packets Out / Sec	The average sent packets per second

Selecting a host in the first and second list updates the Ladder Diagram to contain only the connections between the two selected hosts.

The Packet Tree shows the item selected in the Ladder Diagram.

Protocols

The *Protocols* view shows the protocols in a tree view, offering an outline of the structure of the captured packets and the distribution per protocol, as shown in the following figure:



Protocols

Protocol	Packets	Frame Bytes
Ethernet	131581	73958747
IP	131440	73952447
TCP	131440	73952447
HTTP	58429	69016665
ARP	141	6300
ARP	141	6300

Protocol Hosts (21 items)

No	Host	Bytes Sent	Bytes Received	Packets Sent	Packets Received	Bytes Sent (%)	Bytes Received (%)
1	198.18.0.8	299534	3102587	2690	3360	0.48	5.06
2	198.18.0.7	299979	3104178	2694	3363	0.48	5.06
3	198.18.0.6	300045	3104178	2695	3363	0.48	5.06
4	198.18.0.5	653754	6776283	5874	7338	1.06	11.05
5	198.18.0.4	653820	6776283	5875	7338	1.06	11.05
6	198.18.0.3	653820	6776283	5875	7338	1.06	11.05
7	198.18.0.2	653754	6776283	5874	7338	1.06	11.05
8	198.18.1.1	55876522	5398270	60525	48477	91.19	8.80
9	198.18.0.1	654710	6785521	5883	7348	1.06	11.07
10	198.18.0.20	4944	46323	42	51	0.00	0.07

```
Time                              Severity  Source   Category         Message
Monday, May 21, 2012 5:24:09 PM   Info      IxLoad   Test Controller  Test is Running.
Monday, May 21, 2012 5:26:12 PM   Info      IxLoad   Test             Checking in license for test Test1...
Monday, May 21, 2012 5:26:12 PM   Info      IxLoad   Test             Checking in license for feature(s) IXLOAD,HTTP-Basic for chassis 10.205.27.41 on license server ['@10.205.29.33']...
Monday, May 21, 2012 5:26:12 PM   Info      IxLoad   Test             License check in succeeded for test Test1.
Monday, May 21, 2012 5:26:13 PM   Info      IxLoad   IxLoadPlugin     Test has Stopped.
```

Figure 4-17. Protocols Tree View

Selecting a protocol updates the list of hosts that sent or received packets using this protocol.

The *Packet Tree* view is inactive.

Physical Layer View

Nodes

The *Nodes* list view is similar with the *Application Endpoints* on page 4-14 and the *Network Hosts* on page 4-21. The only difference is that all *Network Hosts* sharing the same MAC address are seen as a single endpoint at the *Physical* level.

Selecting an endpoint updates the list of nodes with which the selected node exchanged packets, providing statistics reflecting the relationship with the selected node.

The *Common View* and *Packet Tree* views are not active.

Common View

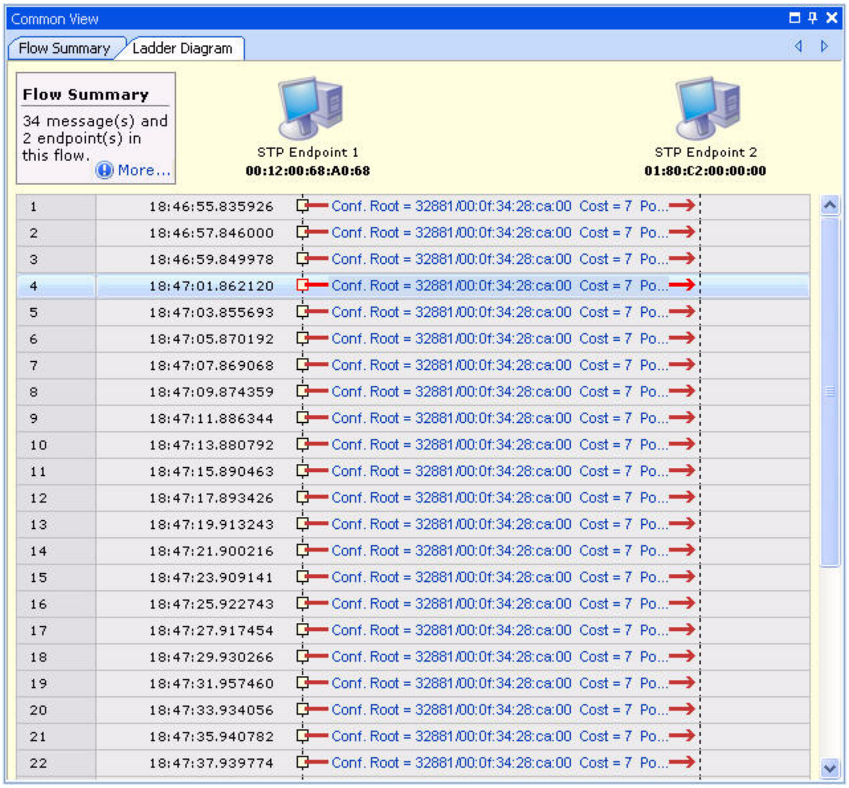
The *Common View* contains the Ladder Diagram and Flow Summary tabs, described later in this section. They are active or inactive, depending on the type of items shown in the main view (*Application*, *Network*, *Physical* viewers). Each of these tabs open a different view, providing information about the selected item in the main list.

For the RTP Conversations, the *Common View* also includes the RTP Stream and RTP Related Streams tabs, as described in *RTP Stream Viewer* on page 8-4.

For the MPEG Conversations, the *Common View* also includes the MPEG Stream tab.

Ladder Diagram

The *Ladder Diagram* view displays the flow between endpoints with time stamps (absolute and relative), delta times, and packet length, as shown in Figure 4-18.



Flow Summary

34 message(s) and 2 endpoint(s) in this flow.

STP Endpoint 1 **00:12:00:68:A0:68**

STP Endpoint 2 **01:80:C2:00:00:00**

1	18:46:55.835926	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
2	18:46:57.846000	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
3	18:46:59.849978	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
4	18:47:01.862120	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
5	18:47:03.855693	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
6	18:47:05.870192	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
7	18:47:07.869068	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
8	18:47:09.874359	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
9	18:47:11.886344	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
10	18:47:13.880792	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
11	18:47:15.890463	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
12	18:47:17.893426	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
13	18:47:19.913243	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
14	18:47:21.900216	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
15	18:47:23.909141	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
16	18:47:25.922743	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
17	18:47:27.917454	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
18	18:47:29.930266	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
19	18:47:31.957460	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
20	18:47:33.934056	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
21	18:47:35.940782	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...
22	18:47:37.939774	Conf. Root = 32881/00:0f:34:28:ca:00 Cost = 7 Po...

Figure 4-18. Ladder Diagram

Based on the view that generates the ladder diagram, the ladder can display the packets according to various criteria: conversation/connection packets, entire flow starting from a specific packet/conversation, all the packets from/to an endpoint or host, all the packets between two endpoints/hosts, and so on.

The selection in the ladder diagram is reflected in the *Packet Tree* view.

The selection of multiple packets in the ladder diagram shows relevant information related to the selection, instead of showing the packet content in the *Packet Tree* view.

Customizing the Endpoint Appearance

To customize the appearance of an entity in the Ladder diagram:

1. Right-click the endpoint in the Ladder Diagram. A set of options displays.
2. Select Entity (**Endpoint**) **Properties**. The Group Properties dialog opens.

3. Type the entity name in the appropriate field.
4. Select the entity type from the list (**Endpoint**).
5. Click **OK** to apply the settings.

Changing an Endpoint Position

To move or hide an entity shown in the Ladder Diagram:

1. Right-click the endpoint in the Ladder Diagram. A set of options displays.
2. Select the action that you want to perform from the following:
    - **Hide Endpoint** – hides the selected endpoint;
    - **Move Left** – moves the selected endpoint one position to the left;
    - **Move Right** – moves the selected endpoint one position to the right;
    - **Move to Begin** – moves the selected endpoint to the beginning of the list;
    - **Move to End** – moves the selected endpoint to the end of the list.

Adjusting the Distance between Two Endpoints

To adjust the distance between two consecutive items in the Ladder Diagram:

1. Click **More...** in the Ladder Diagram and select **Preferences**. The Preferences dialog opens.
2. Move the indicator between Tiny and Large, according to your preferences.
3. Click **OK** to apply the settings.

Filtering the Information in the Ladder Diagram

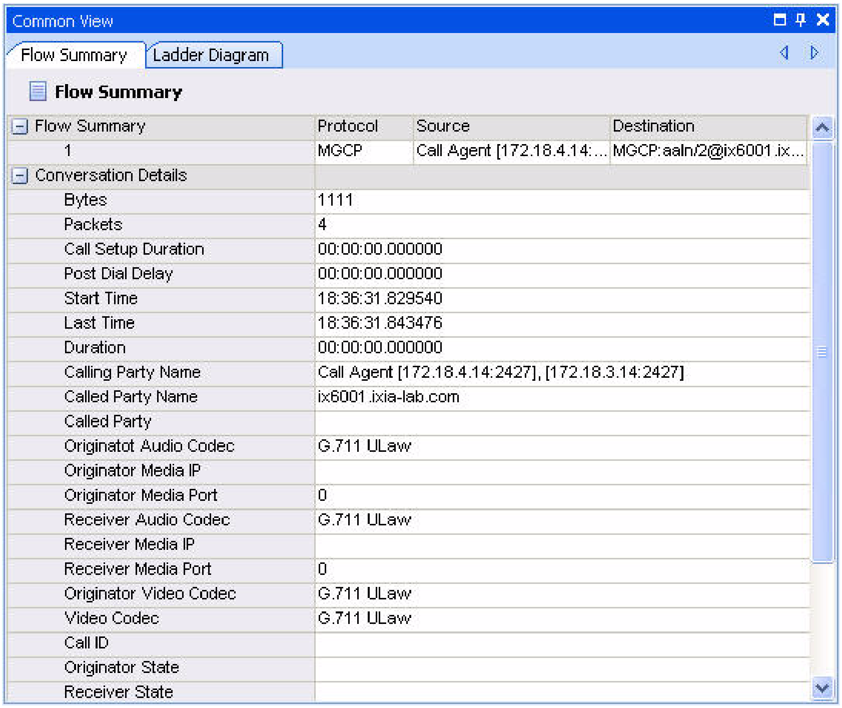
To filter the information in the Ladder Diagram:

1. Click **More...** in the Ladder Diagram and select **Filters**.The Filter dialog opens.
2. Select one of the three options, considering the explanations in the dialog for each option:
    - **Typical** – displays typical flow with all related conversations;
    - **Current Selection Only** – displays current selection only, without the related conversations;
    - **Entire Flow** – displays the entire flow, including the related conversations and the registrations.
3. You can also select **Custom Flow** if you want to filter by endpoint, by protocol, or by time. If you have selected **Custom Flow**, then click **Next** and continue with the next step; otherwise, click **Finish** to apply the selected filter.
4. In the Endpoint Filter screen, select the endpoints to be shown in the diagram, then click **Next**.

5. In the Protocol Filter screen, select the protocols to be shown in the diagram, then click **Next**.
6. In the Time Filter screen, select the time interval to be shown.
7. Click **Finish** to apply the customized filter.

Flow Summary

The *Flow Summary* view provides a summary of all the conversations and all the information available for the *Application Conversations*, *Application Expert Log, Network Packets*, and *Network Connections* views, as shown in Figure 4-19.

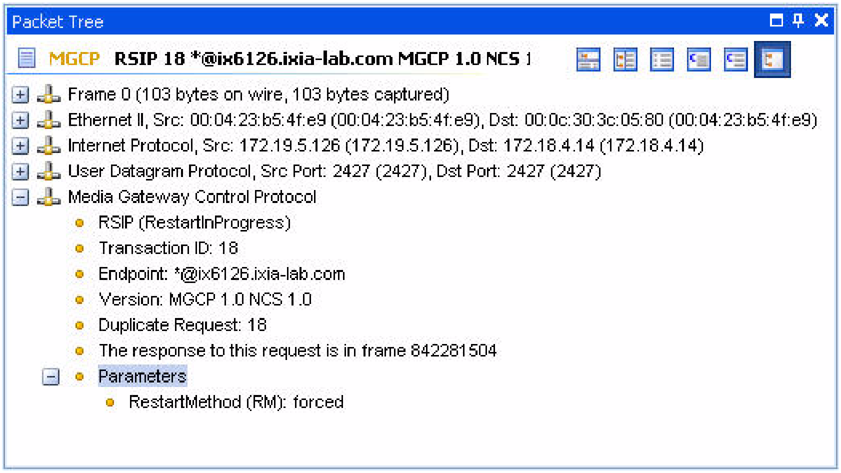


⊟ Flow Summary	Protocol	Source	Destination
1	MGCP	Call Agent [172.18.4.14:...	MGCP:aaln/2@ix6001.ix...
⊟ Conversation Details			
Bytes	1111		
Packets	4		
Call Setup Duration	00:00:00.000000		
Post Dial Delay	00:00:00.000000		
Start Time	18:36:31.829540		
Last Time	18:36:31.843476		
Duration	00:00:00.000000		
Calling Party Name	Call Agent [172.18.4.14:2427], [172.18.3.14:2427]		
Called Party Name	ix6001.ixia-lab.com		
Called Party			
Originatot Audio Codec	G.711 ULaw		
Originator Media IP			
Originator Media Port	0		
Receiver Audio Codec	G.711 ULaw		
Receiver Media IP			
Receiver Media Port	0		
Originator Video Codec	G.711 ULaw		
Video Codec	G.711 ULaw		
Call ID			
Originator State			
Receiver State			

Figure 4-19. Flow Summary

Packet Tree View

The *Packet Tree* view provides details about the packet content, according to the selection made in the Ladder Diagram, as shown in Figure 4-20.



MGCP RSIP 18 *@ix6126.ixia-lab.com MGCP 1.0 NCS 1

- Frame 0 (103 bytes on wire, 103 bytes captured)
- Ethernet II, Src: 00:04:23:b5:4f:e9 (00:04:23:b5:4f:e9), Dst: 00:0c:30:3c:05:80 (00:04:23:b5:4f:e9)
- Internet Protocol, Src: 172.19.5.126 (172.19.5.126), Dst: 172.18.4.14 (172.18.4.14)
- User Datagram Protocol, Src Port: 2427 (2427), Dst Port: 2427 (2427)
- Media Gateway Control Protocol
  - RSIP (RestartInProgress)
  - Transaction ID: 18
  - Endpoint: *@ix6126.ixia-lab.com
  - Version: MGCP 1.0 NCS 1.0
  - Duplicate Request: 18
  - The response to this request is in frame 842281504
  - Parameters
    - RestartMethod (RM): forced

Figure 4-20. Packet Tree View

The Packet Tree information can be shown in six different viewers, which you can access by using the buttons in the top-right corner of the Packet Tree window, shown in Table 4-10.

Table 4-10. Packet tree Viewers

Button	Description
Horizontal split Packet Tree and Hex viewer	Packet tree and hexadecimal format viewers.
Vertical split Packet Tree and Hex viewer	Packet tree and hexadecimal format viewers.
Application data as ASCII	Application data as ASCII format viewer.
Packet array	Viewer of the selected packet byte array.
Protocols arrays	Viewer of protocol arrays for the selected packet.
Packet tree view	The tree format view shows the packet content, where branches represent the main packet blocks and the leafs represent the block fields.

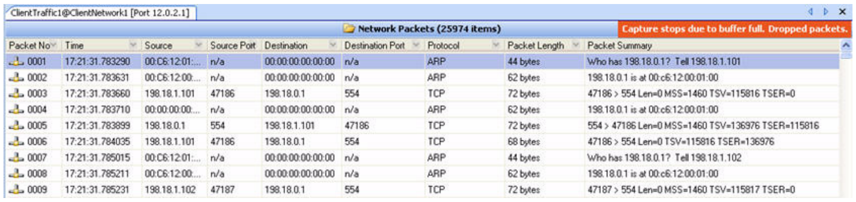
Capture Statistics View

Analyzer displays some statistics referring to a specific capture:

Warning messages appear as shown in the following figure:

Dropped packets – when there are packets that have been dropped during the capture;

- *Capture stops due to buffer full* – when the buffer of the capture agents is full due to the fact that the incoming traffic rate is greater than the rate of line between the capture agent and Analyzer.



Network Packets (25974 items)

Capture stops due to buffer full. Dropped packets.

Packet No	Time	Source	Source Port	Destination	Destination Port	Protocol	Packet Length	Packet Summary
0001	17:21:31.783290	00:C6:12:01:...	n/a	00:00:00:00:00:00	n/a	ARP	44 bytes	Who has 198.18.0.1? Tell 198.18.1.101
0002	17:21:31.783631	00:C6:12:00:...	n/a	00:00:00:00:00:00	n/a	ARP	62 bytes	198.18.0.1 is at 00:c6:12:00:01:00
0003	17:21:31.783660	198.18.1.101	47186	198.18.0.1	554	TCP	72 bytes	47186 > 554 Len=0 MSS=1460 TSV=115816 TSER=0
0004	17:21:31.783710	00:00:00:00:...	n/a	00:00:00:00:00:00	n/a	ARP	62 bytes	198.18.0.1 is at 00:c6:12:00:01:00
0005	17:21:31.783899	198.18.0.1	554	198.18.1.101	47186	TCP	72 bytes	554 > 47186 Len=0 MSS=1460 TSV=136976 TSER=115816
0006	17:21:31.784035	198.18.1.101	47186	198.18.0.1	554	TCP	68 bytes	47186 > 554 Len=0 TSV=115816 TSER=136976
0007	17:21:31.785015	00:C6:12:01:...	n/a	00:00:00:00:00:00	n/a	ARP	44 bytes	Who has 198.18.0.1? Tell 198.18.1.102
0008	17:21:31.785211	00:C6:12:00:...	n/a	00:00:00:00:00:00	n/a	ARP	62 bytes	198.18.0.1 is at 00:c6:12:00:01:00
0009	17:21:31.785231	198.18.1.102	47187	198.18.0.1	554	TCP	72 bytes	47187 > 554 Len=0 MSS=1460 TSV=115817 TSER=0

Figure 4-21. Warning Messages on Capture Statistics

Actions Performed in Analyzer

This section describes the main steps and actions to perform in order to open a capture with Analyzer and customize the specific views to suit your needs.

There are two situations in which Analyzer is used to view captures:

- Viewing a capture in little-endian format, no matter what was the method used to perform that capture;
- Viewing a capture performed using an Analyzer-equipped Ixia product.

Opening a Capture in Analyzer

To open a capture in Analyzer:

1. Select **File > Open** in the main menu, or click the **Open** tool bar button. The Open...dialog opens.
2. In the Files of type list, select one of the two options:
   - *Capture file (*.cap)* – used to open an existing capture.
   - *Live capture file (*.lcap)* – used to open a live capture that is being performed by using the application with which the Analyzer is integrated.
3. Browse for the capture file, select it, then click **Open.** The capture displays in the Analyzer main view.

You can have more than one capture opened at a time in Analyzer and navigate between them by selecting the corresponding capture.

Customizing the Main View

You can customize the main view in Analyzer to suit your needs by filtering the shown information and choosing the fields to display.

Filtering the Information

You can filter the information shown in Analyzer by using:

- The field filters
- The column filters

To filter the information shown in the Analyzer view by using the column filters:

1. Click the arrow in the column header, as shown in Figure 4-22 on page 4-30.

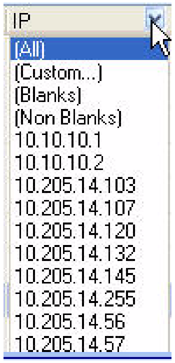
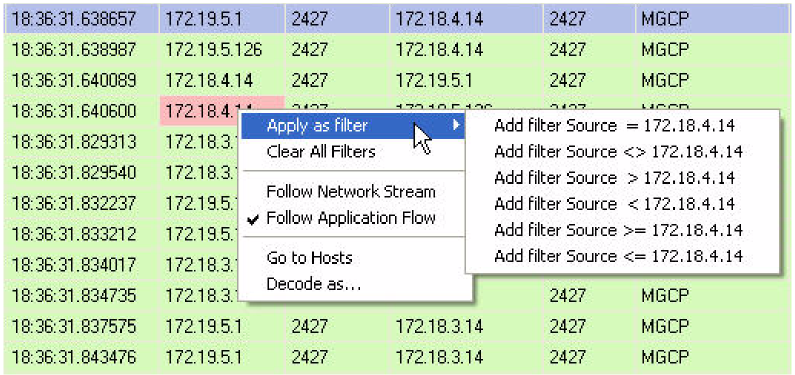


Figure 4-22. Column Filtering

2. Select one of the available options:
   - **All** – shows all the records, no filter is applied;
   - **Custom** – opens a dialog, where you can set your filter condition;
   - **Blanks** – shows only the records having the selected column blank;
   - **Non Blanks** – shows only the records having the selected column filled in;
   - One of the current values of the selected column – shows only the records having the selected column filled in with the selected value.

To filter the information shown in the Analyzer view by using the field filters:

1. Right-click the item in the list by which you want to filter (for example, if you want to show only the conversations with a specific IP source address in the *Network Packets* view, right-click the item having that value in the *Source* field, as shown in Figure 4-23).



18:36:31.638657	172.19.5.1	2427	172.18.4.14	2427	MGCP
18:36:31.638987	172.19.5.126	2427	172.18.4.14	2427	MGCP
18:36:31.640089	172.18.4.14	2427	172.19.5.1	2427	MGCP
18:36:31.640600	172.18.4.1				
18:36:31.829313	172.18.3.				
18:36:31.829540	172.18.3.1				
18:36:31.832237	172.19.5.1				
18:36:31.833212	172.19.5.1				
18:36:31.834017	172.18.3.1				
18:36:31.834735	172.18.3.1			2427	MGCP
18:36:31.837575	172.19.5.1	2427	172.18.3.14	2427	MGCP
18:36:31.843476	172.19.5.1	2427	172.18.3.14	2427	MGCP

Apply as filter
Clear All Filters
Follow Network Stream
✓ Follow Application Flow
Go to Hosts
Decode as...
Add filter Source = 172.18.4.14
Add filter Source <> 172.18.4.14
Add filter Source > 172.18.4.14
Add filter Source < 172.18.4.14
Add filter Source >= 172.18.4.14
Add filter Source <= 172.18.4.14

Figure 4-23. Filtering the Shown Information

2. Select the **Apply as filter** option and choose the desired filter condition.

To remove the applied filter, you have two options:

- Simply click the **Remove All Filters...** button at the bottom of the list.
- Right-click an item in the list and select the **Clear All Filters** option.

Decoding Packets

There are some cases when a packet cannot be identified as it should be—for example, MPEG packets. By using the **decode as** feature, decoders can be instructed to decode a stream of packets as a specified protocol. Using this feature, UDP packets can be forced to be decoded as MPEG packets.

To decode packets in a capture as a specified protocol:

1. Right-click the packet in the *Network Packets* view and select **Decode as...**. The Decode as...dialog opens, as shown in Figure 4-24.

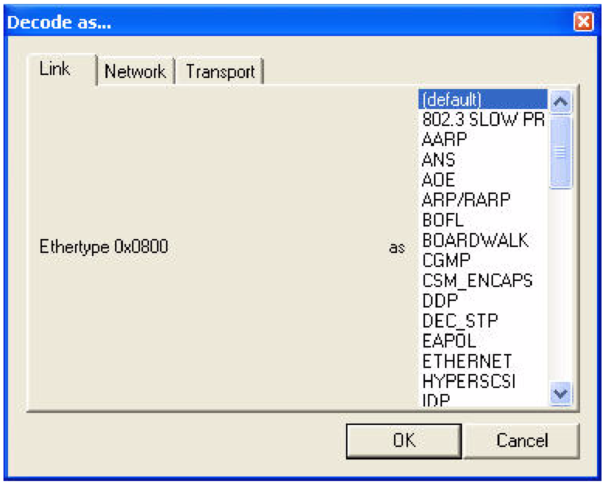


Figure 4-24. Decode as... Dialog

2. Select the tab according to the protocol layer by which the decoding is performed (for example, if you want to decode UDP packets, you must select the Transport tab)

3. From the list shown on the right side of the window, select the protocol that the stream should be decoded as (for example, if you want to decode UDP packets as MPEG, you must select **MPEG** in the list shown in the *Transport* section).

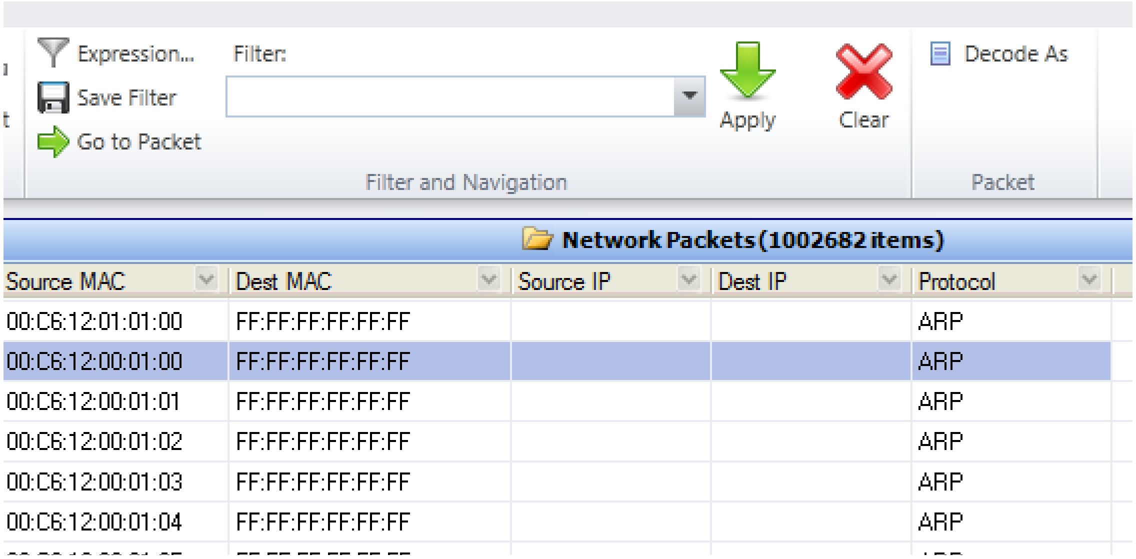
For each layer, there is a list of protocols that can be interpreted. *Default* (the first entry) means that all decoding applied to the capture is canceled, but only for that layer.

If there is more than one capture window open, each one has its own set of **decode as** rules. If the same capture is opened twice and a decoding is performed in one of the instances, the operation takes effect only in that particular one. As a result, the same capture can be opened twice, but with different decodes.

> **Note:** It is possible to request that a protocol be decoded as another protocol, but this does not ensure that the selected protocol is decoded as indicated. Each decoder has its own packet check, and if the packets do not pass the validity check, they are decoded as before. For example, if a TCP packet is forced to be decoded as a SIP packet, but does not have the SIP header (SIP2.0), it is not shown as SIP, even if the **decode as** operation is performed.

Applying a Packets Filter

The Packets Filter allows you to filter network packets by any field of a protocol, at any layer. The Packets Filter bar, shown in the following figure:



Network Packets (1002682 items)

Source MAC	Dest MAC	Source IP	Dest IP	Protocol
00:C6:12:01:01:00	FF:FF:FF:FF:FF:FF			ARP
00:C6:12:00:01:00	FF:FF:FF:FF:FF:FF			ARP
00:C6:12:00:01:01	FF:FF:FF:FF:FF:FF			ARP
00:C6:12:00:01:02	FF:FF:FF:FF:FF:FF			ARP
00:C6:12:00:01:03	FF:FF:FF:FF:FF:FF			ARP
00:C6:12:00:01:04	FF:FF:FF:FF:FF:FF			ARP

Figure 4-25. Packets Filter Bar

To set a packets filter:

1. Click the **Expression...** button. The Filter Expression dialog opens, as shown in the follwoing figures:

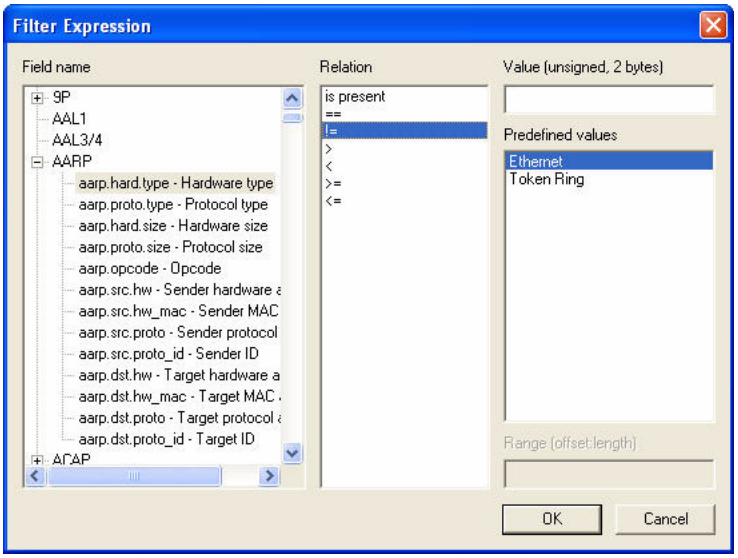

Filter Expression
Field name
9P
AAL1
AAL3/4
AARP
aarp.hard.type - Hardware type
aarp.proto.type - Protocol type
aarp.hard.size - Hardware size
aarp.proto.size - Protocol size
aarp.opcode - Opcode
aarp.src.hw - Sender hardware a
aarp.src.hw_mac - Sender MAC
aarp.src.proto - Sender protocol
aarp.src.proto_id - Sender ID
aarp.dst.hw - Target hardware a
aarp.dst.hw_mac - Target MAC .
aarp.dst.proto - Target protocol a
aarp.dst.proto_id - Target ID
ACAP
Relation
is present
==
!=
>
<
>=
<=
Value (unsigned, 2 bytes)
Predefined values
Ethernet
Token Ring
Range (offset:length)
OK
Cancel

Figure 4-26. Filter Expression Dialog

2. Select the protocol field in the *Field name* tree view.

3. Select a relation. The *Value* area becomes available. Depending on the selected protocol field, the *Range* area may or may not become available.

4. Click the **OK** button. The filter expression is created and the Filter Expressions dialog closes.

5. Click the **Apply** button to filter the packets. The filter expression is shown in the quick expression editor.

You can skip the first four steps by directly typing the expression in the quick expression editor. The expression syntax is verified while typed. If the syntax is incorrect, the quick expression editor's background becomes red. If the expression is typed correctly, the background is green.

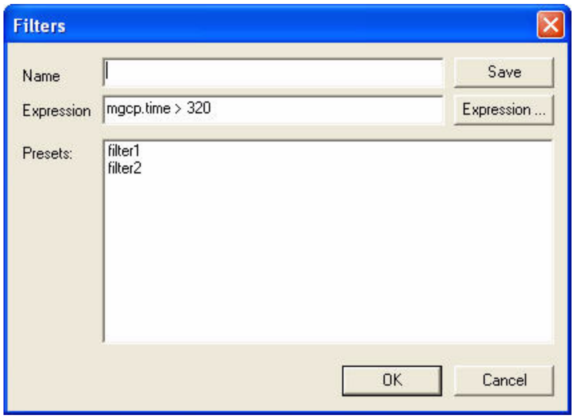
When a correct expression is applied, it is retained in the quick expression editor's history. History can be accessed by clicking the editor's arrow button.

To remove an applied filter, you can either click the **Clear** button on the Packets Filter bar, or the **Remove All Filters** button on the bottom bar.

Saving a Packets Filter

You can save frequently used expressions. To do this:

1. Click the **Filter** button, on the Packets Filter bar. The Filters dialog, shown in Figure 4-27, opens.



Filters

Name:

Expression: mgcp.time > 320

Presets:
filter1
filter2

Figure 4-27. Filters Dialog

2. Insert a name for the filter expression in the *Name* field.

Note: When the Filters dialog displays, both the *Name* and the *Expression* fields are automatically filled in with the quick expression editor content.

3. Click the **Save** button. The name of the saved filter expression displays in the *Presets* area.
4. Click **OK** to close the Filters dialog.

You can also build a new filter expression by clicking **Expression...** in the Filters dialog and saving it afterwards. This button opens the Filter Expression dialog, described in *Applying a Packets Filter* on page 4-32.

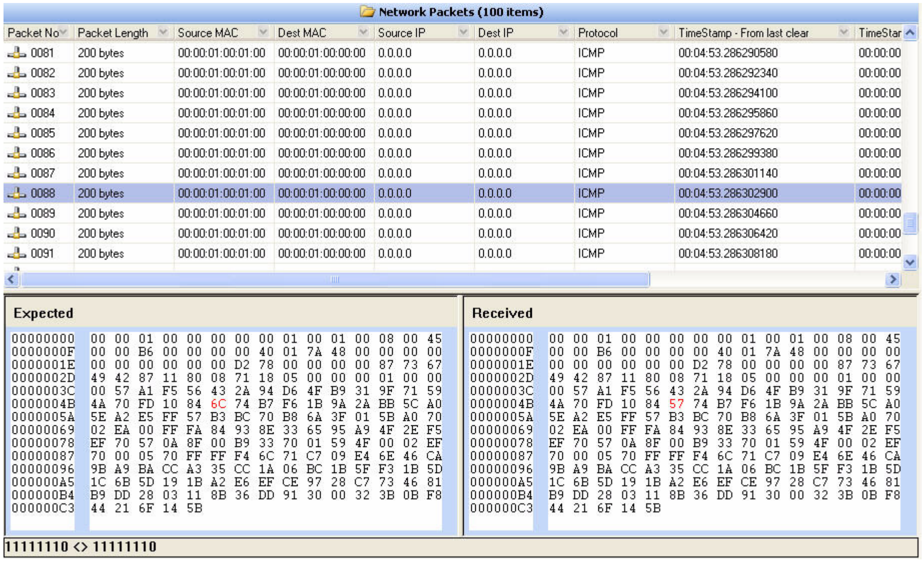
Loading a Packets Filter

You can load previously saved filters. To load a packets filter:

1. Click the **Filter** button, on the Packets Filter bar. The Filters dialog, shown in Figure 4-27 on page 4-34, opens.
2. Select a filter expression in the *Presets* area.
3. Click the **OK** button.
4. Click the **Apply** button to filter the packets.

PRBS Packet Compare

In IxExplorer, Analyzer allows you to verify whether a packet has suffered any changes on its way from the source to the destination through the device under test by using Pseudo Random Bit Sequences. The content of the received packet and of the expected packet is represented in hexadecimal format in the *Packet Compare* view, as shown in Figure 4-28.



Network Packets (100 items)

Packet No	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol	TimeStamp - From last clear	TimeStar
0081	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286290580	00:00:00
0082	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286292340	00:00:00
0083	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286294100	00:00:00
0084	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286295860	00:00:00
0085	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286297620	00:00:00
0086	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286299380	00:00:00
0087	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286301140	00:00:00
0088	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286302900	00:00:00
0089	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286304660	00:00:00
0090	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286306420	00:00:00
0091	200 bytes	00:00:01:00:01:00	00:00:01:00:00:00	0.0.0.0	0.0.0.0	ICMP	00:04:53.286308180	00:00:00

Expected

```
00000000  00 00 01 00 00 00 00 00 01 00 01 00 08 00 45
0000000F  00 00 B6 00 00 00 00 40 01 7A 48 00 00 00 00
0000001E  00 00 00 00 00 00 D2 78 00 00 00 00 87 73 67
0000002D  49 42 87 11 80 08 71 18 05 00 00 00 01 00 00
0000003C  00 57 A1 F5 56 43 2A 94 D6 4F B9 31 9F 71 59
0000004B  4A 70 FD 10 84 6C 74 B7 F6 1B 9A 2A BB 5C A0
0000005A  5E A2 E5 FF 57 B3 BC 70 B8 6A 3F 01 5B A0 70
00000069  02 EA 00 FF FA 84 93 8E 33 65 95 A9 4F 2E F5
00000078  EF 70 57 0A 8F 00 B9 33 70 01 59 4F 00 02 EF
00000087  70 00 05 70 FF FF F4 6C 71 C7 09 E4 6E 46 CA
00000096  9B A9 BA CC A3 35 CC 1A 06 BC 1B 5F F3 1B 5D
000000A5  1C 6B 5D 19 1B A2 E6 EF CE 97 28 C7 73 46 81
000000B4  B9 DD 28 03 11 8B 36 DD 91 30 00 32 3B 0B F8
000000C3  44 21 6F 14 5B
```

Received

```
00000000  00 00 01 00 00 00 00 00 01 00 01 00 08 00 45
0000000F  00 00 B6 00 00 00 00 40 01 7A 48 00 00 00 00
0000001E  00 00 00 00 00 00 D2 78 00 00 00 00 87 73 67
0000002D  49 42 87 11 80 08 71 18 05 00 00 00 01 00 00
0000003C  00 57 A1 F5 56 43 2A 94 D6 4F B9 31 9F 71 59
0000004B  4A 70 FD 10 84 57 74 B7 F6 1B 9A 2A BB 5C A0
0000005A  5E A2 E5 FF 57 B3 BC 70 B8 6A 3F 01 5B A0 70
00000069  02 EA 00 FF FA 84 93 8E 33 65 95 A9 4F 2E F5
00000078  EF 70 57 0A 8F 00 B9 33 70 01 59 4F 00 02 EF
00000087  70 00 05 70 FF FF F4 6C 71 C7 09 E4 6E 46 CA
00000096  9B A9 BA CC A3 35 CC 1A 06 BC 1B 5F F3 1B 5D
000000A5  1C 6B 5D 19 1B A2 E6 EF CE 97 28 C7 73 46 81
000000B4  B9 DD 28 03 11 8B 36 DD 91 30 00 32 3B 0B F8
000000C3  44 21 6F 14 5B
```

```
11111110 <> 11111110
```

Figure 4-28. Packet Compare View

If there are different bytes between the received packet and the expected packet, they are highlighted in red. Further differences are shown on the bottom status bar, where the bytes are compared in binary format.

To view the differences at bit level on the status bar, select a byte in either the expected packet window or the received packet window.

Only altered PRBS packets are displayed. If no PRBS errors occurred, no packets display.

Capture Buffer

You can control the capture buffer behavior by defining the buffer policy and per port buffer size settings. Both these settings can only be changed while capture is stopped and the packet download from the buffer is finished. You can also upload packets from buffer to capture. For more information, see Analyzer Global Settings.

Note: You cannot capture or upload any packet after reaching the 2 million packets limit (of packets uploaded in all opened captures) and the solution is to close the opened captures in order to capture or upload any other packets.

Analyzer Global Settings

The control buffer settings are shown in the following table:

Section	Field/Control	Description
Buffer full Behavior		When the new packets are captured faster than they are sent to the Analyzer, and the capture buffer gets full, you can do any of the following actions before starting the capture. • Stop capture • Override old packets
	Stop capture	Select this check box to stop capturing packets.
	Override oldest packets (circular buffer)	Select this check box to continue capturing packets, and overwrite the oldest packets that have not yet been sent.
Capture View Display Mode		Enables you to choose the way in which you want to upload the packets.
	Stream (real-time)	Click this option to upload packets while the capture is in progress (live).
	Upload captured packets after capture stops	Click this option to upload packets only after the capture is stopped. Capture is stopped either because the buffer is full, or because you have stopped the capture.
Capture buffer size	*Memory allocated for the capture buffer per port*	Permitted values are between 5% and 70% Enables you to specify the amount of memory on the port that should be used by PPC capture plug-in for storing captured packets. This value is a percentage of the total memory.

5

SIP Captures

Analyzer can trace SIP flows, providing ladder diagrams and specific SIP statistics and protocol errors.

Analyzer groups all messages belonging to a specific call and provides specific call statistics. The Analyzer SIP module allows you to easily view the SIP call flow on a large IP messages capture.

This chapter describes the specific SIP statistics and views provided by Analyzer.

SIP Conversations

This section briefly describes the SIP call types that can be traced. Except for the list in Figure 5-1 on page 5-2, Analyzer detects only isolated segments of a call.

There are three basic SIP conversation types shown in Analyzer:

- Registration conversations
- Call Control conversations
- Miscellaneous conversations

The SIP call types that can be traced by Analyzer are shown in Figure 5-1 on page 5-2.

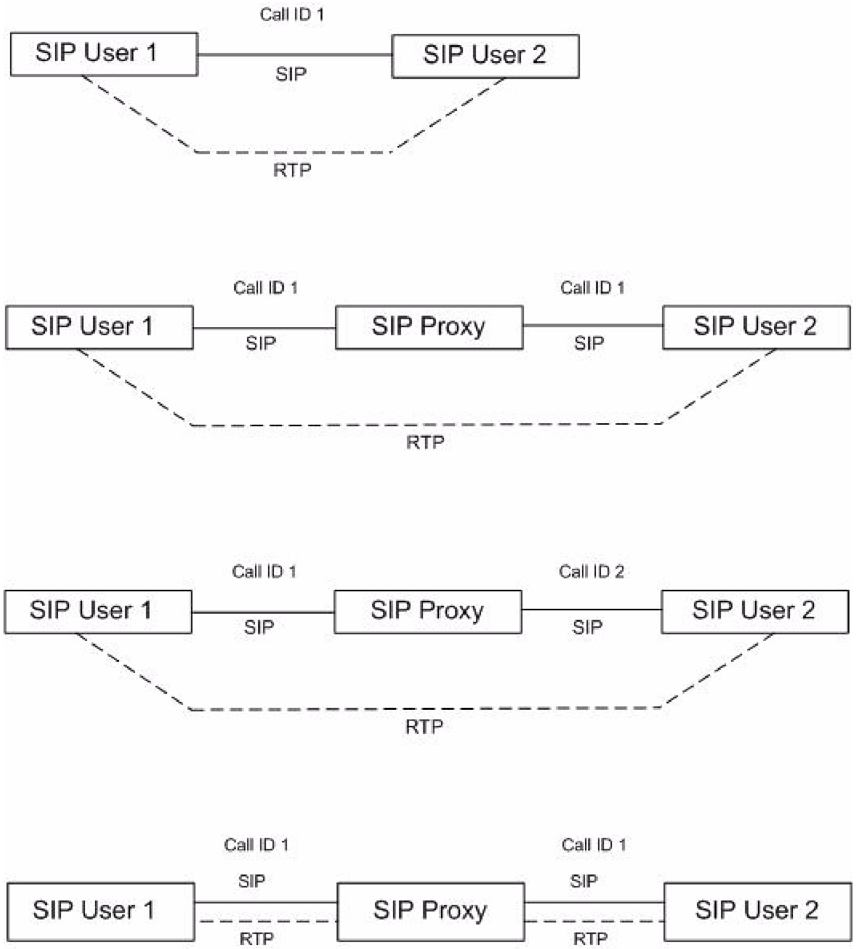
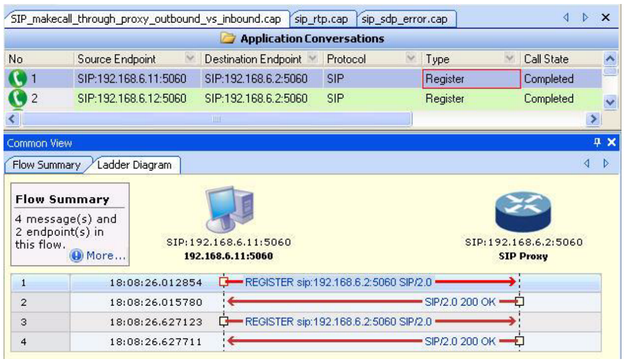


Figure 5-1. SIP Call Types Traced by Analyzer

SIP Registration in Analyzer

The SIP registration flows consisting of *Register* and *Unregister* transactions can be identified in the *Application Conversations* view by the **Register** value in the *Type* field, as shown in Figure 5-2.


SIP_makecall_through_proxy_outbound_vs_inbound.cap
sip_rtp.cap
sip_sdp_error.cap
Application Conversations
Common View
Flow Summary
Ladder Diagram

No	Source Endpoint	Destination Endpoint	Protocol	Type	Call State
1	SIP:192.168.6.11:5060	SIP:192.168.6.2:5060	SIP	Register	Completed
2	SIP:192.168.6.12:5060	SIP:192.168.6.2:5060	SIP	Register	Completed

Flow Summary

4 message(s) and 2 endpoint(s) in this flow.

More...

SIP:192.168.6.11:5060
192.168.6.11:5060

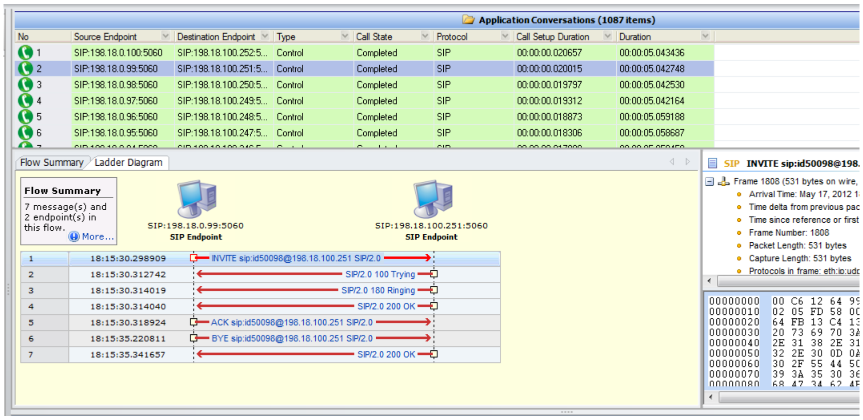
SIP:192.168.6.2:5060
SIP Proxy

1	18:08:26.012854	REGISTER sip:192.168.6.2:5060 SIP/2.0 →
2	18:08:26.015780	← SIP/2.0 200 OK
3	18:08:26.627123	REGISTER sip:192.168.6.2:5060 SIP/2.0 →
4	18:08:26.627711	← SIP/2.0 200 OK

Figure 5-2. SIP Registration Conversation in Analyzer

SIP Call Control in Analyzer

The SIP calls (also known as control flows) are identified in the *Application Conversations* view by the **Control** value in the *Type* field, as shown in Figure 5-3.



Application Conversations (1087 items)

No	Source Endpoint	Destination Endpoint	Type	Call State	Protocol	Call Setup Duration	Duration
1	SIP:198.18.0.100:5060	SIP:198.18.100.252:5...	Control	Completed	SIP	00:00:00.020657	00:00:05.043436
2	SIP:198.18.0.99:5060	SIP:198.18.100.251:5...	Control	Completed	SIP	00:00:00.020015	00:00:05.042748
3	SIP:198.18.0.98:5060	SIP:198.18.100.250:5...	Control	Completed	SIP	00:00:00.019797	00:00:05.042530
4	SIP:198.18.0.97:5060	SIP:198.18.100.249:5...	Control	Completed	SIP	00:00:00.019312	00:00:05.042164
5	SIP:198.18.0.96:5060	SIP:198.18.100.248:5...	Control	Completed	SIP	00:00:00.018873	00:00:05.059188
6	SIP:198.18.0.95:5060	SIP:198.18.100.247:5...	Control	Completed	SIP	00:00:00.018306	00:00:05.058687

Flow Summary
7 message(s) and 2 endpoint(s) in this flow.
More...

SIP:198.18.0.99:5060
SIP Endpoint

SIP:198.18.100.251:5060
SIP Endpoint

1	18:15:30.298909	INVITE sip:id50098@198.18.100.251 SIP/2.0
2	18:15:30.312742	SIP/2.0 100 Trying
3	18:15:30.314019	SIP/2.0 180 Ringing
4	18:15:30.314040	SIP/2.0 200 OK
5	18:15:30.318924	ACK sip:id50098@198.18.100.251 SIP/2.0
6	18:15:35.220811	BYE sip:id50098@198.18.100.251 SIP/2.0
7	18:15:35.341657	SIP/2.0 200 OK

SIP INVITE sip:id50098@198.
Frame 1808 (531 bytes on wire,
- Arrival Time: May 17, 2012 1
- Time delta from previous pac
- Time since reference or first
- Frame Number: 1808
- Packet Length: 531 bytes
- Capture Length: 531 bytes
- Protocols in frame: eth:ip:udp

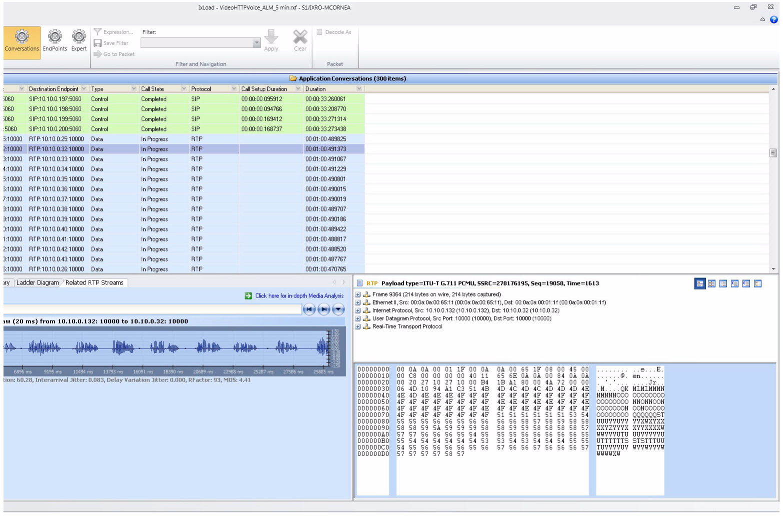
```
00000000  00 C6 12 64 99
00000010  02 05 FD 58 00
00000020  64 FB 13 C4 13
00000030  20 73 69 70 3A
00000040  2E 31 38 2E 31
00000050  32 2E 30 0D 0A
00000060  30 2F 55 44 50
00000070  39 3A 35 30 36
```

Figure 5-3. SIP Call Control Messages in Analyzer

If the SIP capture contains a registration, you can view in the Ladder Diagram the registration messages by selecting **More...** > **Filters** and by choosing **Entire Flow** in the opened dialog.

> **Note:** The SIP Endpoints can be identified as Proxy only if the registration part is present in the flow.

If the SIP call contains RTP streams, the *Common View* also displays the Related RTP Streams tab, as shown in Figure 5-4.



IxLoad - VideoHTTPVoice_ALM_5 min.rxf - S1/IXRO-MCORNEA

Application Conversations (300 items)

	Destination Endpoint	Type	Call State	Protocol	Call Setup Duration	Duration
5060	SIP:10.10.0.197:5060	Control	Completed	SIP	00:00:00.095912	00:00:33.260061
5060	SIP:10.10.0.198:5060	Control	Completed	SIP	00:00:00.094766	00:00:33.208770
5060	SIP:10.10.0.199:5060	Control	Completed	SIP	00:00:00.169412	00:00:33.271314
:5060	SIP:10.10.0.200:5060	Control	Completed	SIP	00:00:00.168737	00:00:33.273438
5:10000	RTP:10.10.0.25:10000	Data	In Progress	RTP		00:01:00.489825
2:10000	RTP:10.10.0.32:10000	Data	In Progress	RTP		00:01:00.491373
3:10000	RTP:10.10.0.33:10000	Data	In Progress	RTP		00:01:00.491067
4:10000	RTP:10.10.0.34:10000	Data	In Progress	RTP		00:01:00.491229
5:10000	RTP:10.10.0.35:10000	Data	In Progress	RTP		00:01:00.490801
6:10000	RTP:10.10.0.36:10000	Data	In Progress	RTP		00:01:00.490015
7:10000	RTP:10.10.0.37:10000	Data	In Progress	RTP		00:01:00.490019
8:10000	RTP:10.10.0.38:10000	Data	In Progress	RTP		00:01:00.489707
9:10000	RTP:10.10.0.39:10000	Data	In Progress	RTP		00:01:00.490186
0:10000	RTP:10.10.0.40:10000	Data	In Progress	RTP		00:01:00.489422
1:10000	RTP:10.10.0.41:10000	Data	In Progress	RTP		00:01:00.488817
2:10000	RTP:10.10.0.42:10000	Data	In Progress	RTP		00:01:00.488520
3:10000	RTP:10.10.0.43:10000	Data	In Progress	RTP		00:01:00.487767
6:10000	RTP:10.10.0.26:10000	Data	In Progress	RTP		00:01:00.470765

tion: 60.28, Interarrival Jitter: 0.083, Delay Variation Jitter: 0.000, RFactor: 93, MOS: 4.41

RTP Payload type=ITU-T G.711 PCMU, SSRC=278176195, Seq=19058, Time=1613
- Frame 9364 (214 bytes on wire, 214 bytes captured)
- Ethernet II, Src: 00:0a:0a:00:65:1f (00:0a:0a:00:65:1f), Dst: 00:0a:0a:00:01:1f (00:0a:0a:00:01:1f)
- Internet Protocol, Src: 10.10.0.132 (10.10.0.132), Dst: 10.10.0.32 (10.10.0.32)
- User Datagram Protocol, Src Port: 10000 (10000), Dst Port: 10000 (10000)
- Real-Time Transport Protocol

```
00000000  00 0A 0A 00 01 1F 00 0A  0A 00 65 1F 08 00 45 00  ........ ..e...E.
00000010  00 C8 00 00 00 00 40 11  65 6E 0A 0A 00 84 0A 0A  ......@. en......
00000020  00 20 27 10 27 10 00 B4  1B A1 80 00 4A 72 00 00  . '.'... ....Jr..
00000030  06 4D 10 94 A1 C3 51 4B  4D 4C 4D 4C 4D 4D 4D 4E  .M....QK MLMLMMMN
00000040  4E 4D 4E 4E 4E 4F 4F 4F  4F 4F 4F 4F 4F 4F 4F 4F  NMNNNOOO OOOOOOOO
00000050  4F 4F 4F 4F 4F 4F 4F 4F  4E 4E 4F 4E 4E 4F 4F 4E  OOOOOOOO NNONNOON
00000060  4F 4F 4F 4F 4F 4F 4F 4E  4F 4F 4E 4F 4F 4F 4F 4F  OOOOOOON OONOOOOO
00000070  4F 4F 4F 4F 4F 4F 4F 4F  51 51 51 51 51 51 53 54  OOOOOOOO QQQQQQST
00000080  55 55 55 56 56 55 56 56  56 56 58 57 58 59 58 58  UUUVVUVV VVXWXYXX
00000090  58 58 59 5A 59 59 59 58  58 59 59 58 58 58 58 57  XXYZYYYX XYYXXXXW
000000A0  57 57 56 56 56 55 54 55  55 55 56 56 56 56 56 55  WWVVVUTU UUVVVVVU
000000B0  55 54 54 54 54 54 54 53  53 54 53 54 54 54 55 55  UTTTTTTS STSTTTUU
000000C0  54 55 56 56 56 56 55 56  57 56 56 57 56 56 56 57  TUVVVVUV WVVWVVVW
000000D0  57 57 57 57 58 57                                 WWWWXW
```

Figure 5-4. Related RTP Streams in Common View

SIP Statistics

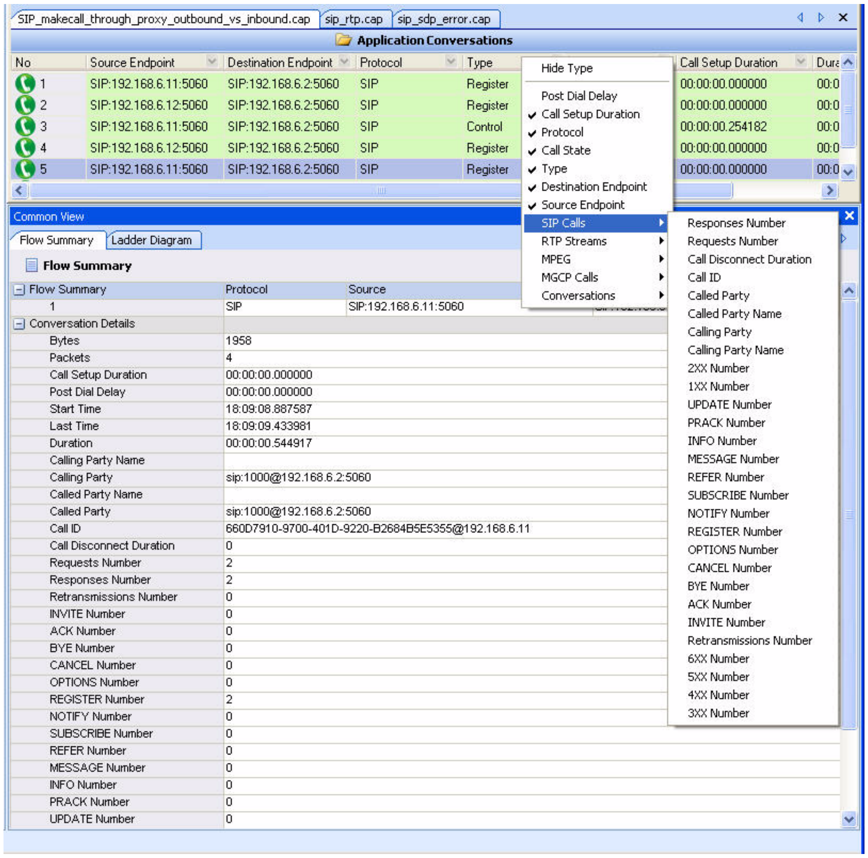
This section describes the SIP specific parameters provided by Analyzer, grouped by:

- Conversation Statistics – the SIP specific counters shown in the *Application Conversations* view, also available in the *Flow Summary* section of the *Common View*
- Endpoint Statistics – the counters shown in the *Application Summary* and *Application Endpoints* views

To view only the SIP statistics in the *Application Conversation* or *Application Endpoints* view, select **SIP** from the *Filter* field in the left pane of the *Analyzer* main window.

SIP Conversation Statistics

The SIP specific flow statistics can be viewed in the *Application Conversation* main view, and also in the *Flow Summary* panel of the *Common View* under *Application Conversations*, as shown in Figure 5-5.



No	Source Endpoint	Destination Endpoint	Protocol	Type	Call Setup Duration	Dura
☎ 1	SIP:192.168.6.11:5060	SIP:192.168.6.2:5060	SIP	Register	00:00:00.000000	00:0
☎ 2	SIP:192.168.6.12:5060	SIP:192.168.6.2:5060	SIP	Register	00:00:00.000000	00:0
☎ 3	SIP:192.168.6.11:5060	SIP:192.168.6.2:5060	SIP	Control	00:00:00.254182	00:0
☎ 4	SIP:192.168.6.12:5060	SIP:192.168.6.2:5060	SIP	Register	00:00:00.000000	00:0
☎ 5	SIP:192.168.6.11:5060	SIP:192.168.6.2:5060	SIP	Register	00:00:00.000000	00:0

⊟ Flow Summary	Protocol	Source
1	SIP	SIP:192.168.6.11:5060
⊟ Conversation Details		
Bytes	1958	
Packets	4	
Call Setup Duration	00:00:00.000000	
Post Dial Delay	00:00:00.000000	
Start Time	18:09:08.887587	
Last Time	18:09:09.433981	
Duration	00:00:00.544917	
Calling Party Name		
Calling Party	sip:1000@192.168.6.2:5060	
Called Party Name		
Called Party	sip:1000@192.168.6.2:5060	
Call ID	660D7910-9700-401D-9220-B2684B5E5355@192.168.6.11	
Call Disconnect Duration	0	
Requests Number	2	
Responses Number	2	
Retransmissions Number	0	
INVITE Number	0	
ACK Number	0	
BYE Number	0	
CANCEL Number	0	
OPTIONS Number	0	
REGISTER Number	2	
NOTIFY Number	0	
SUBSCRIBE Number	0	
REFER Number	0	
MESSAGE Number	0	
INFO Number	0	
PRACK Number	0	
UPDATE Number	0	

Figure 5-5. SIP Flow Statistics

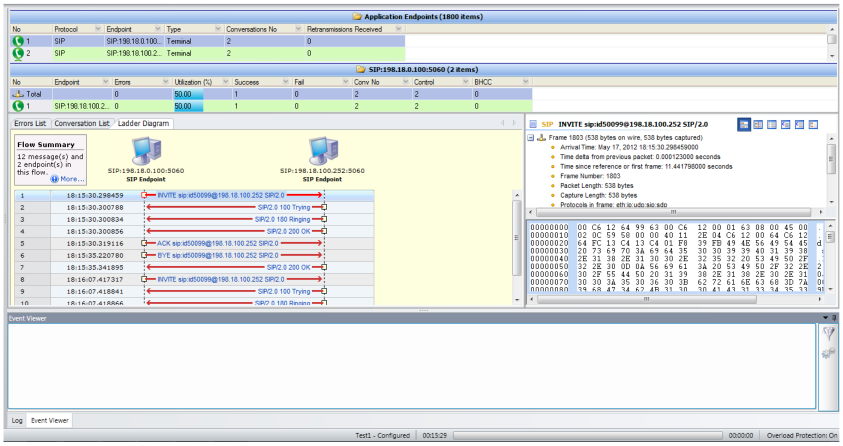
The SIP specific flow statistics provided by Analyzer are the following:

- *Call Setup Duration* – the duration of the call setup phase.
- *Receiver Media Port* – the port used by the receiver endpoint for RTP traffic.
- *Receiver Media IP* – the IP address used by the receiver endpoint for RTP traffic.
- *Receiver Audio Codec* – the audio codec negotiated by the receiver.
- *Originator Media Port* – the port used by the originator endpoint for RTP traffic.
- *Originator Media IP* – the IP address used by the originator endpoint for RTP traffic.
- *Originator Audio Codec* – the audio codec negotiated by the originator.
- *Call ID* – call ID.
- *Calling Party Name* – calling party name, if available.
- *Calling Party* – calling party, in URI format.
- *Called Party Name* – called party name, if available.
- *Called Party* – called party URI.
- *Call Disconnect Duration* – defined as the time between a BYE and a 200 OK message.
- *Requests Number* – total number of requests.
- *Responses Number* – total number of responses.
- *Retransmissions Number* – total number of messages detected as retransmissions in this call.
- *INVITE Number* – total number of INVITE messages.
- *ACK Number* – total number of ACK messages.
- *BYE Number* – total number of BYE messages.
- *CANCEL Number* – total number of CANCEL messages.
- *OPTIONS Number* – total number of OPTIONS messages.
- *REGISTER Number* – total number of REGISTER messages.
- *NOTIFY Number* – total number of NOTIFY messages.
- *SUBSCRIBE Number* – total number of SUBSCRIBE messages.
- *REFER Number* – total number of REFER messages.
- *MESSAGE Number* – total number of MESSAGE messages.
- *INFO Number* – total number of INFO messages.
- *PRACK Number* – total number of PRACK messages.
- *UPDATE Number* – total number of UPDATE messages.
- *1XX Number* – total number of 1XX messages (defined as messages between 100 and 199).

- *2XX Number* – total number of 2XX messages (defined as messages between 200 and 299).
- *3XX Number* – total number of 3XX messages (defined as messages between 300 and 399).
- *4XX Number* – total number of 4XX messages (defined as messages between 400 and 499).
- *5XX Number* – total number of 5XX messages (defined as messages between 500 and 599).
- *6XX Number* – total number of 6XX messages (defined as messages between 600 and 699).

SIP Endpoint Statistics

The SIP endpoint statistics can be viewed in the *Application Summary* and *Application Endpoints* views, as shown in Figure 5-6.



Application Endpoints (1800 items)

No	Protocol	Endpoint	Type	Conversations No	Retransmissions Received
☎ 1	SIP	SIP:198.18.0.100...	Terminal	2	0
☎ 2	SIP	SIP:198.18.100.2...	Terminal	2	0

SIP:198.18.0.100:5060 (2 items)

No	Endpoint	Errors	Utilization (%)	Success	Fail	Conv No	Control	BHCC
Total		0	50.00	1	0	2	2	0
☎ 1	SIP:198.18.100.2...	0	50.00	1	0	2	2	0

Flow Summary
12 message(s) and 2 endpoint(s) in this flow.
More...

1	18:15:30.298459	INVITE sip:id50099@198.18.100.252 SIP/2.0
2	18:15:30.300788	SIP/2.0 100 Trying
3	18:15:30.300834	SIP/2.0 180 Ringing
4	18:15:30.300856	SIP/2.0 200 OK
5	18:15:30.319116	ACK sip:id50099@198.18.100.252 SIP/2.0
6	18:15:35.220780	BYE sip:id50099@198.18.100.252 SIP/2.0
7	18:15:35.341895	SIP/2.0 200 OK
8	18:16:07.417317	INVITE sip:id50099@198.18.100.252 SIP/2.0
9	18:16:07.418841	SIP/2.0 100 Trying
10	18:16:07.418866	SIP/2.0 180 Ringing

SIP INVITE sip:id50099@198.18.100.252 SIP/2.0

- Frame 1803 (538 bytes on wire, 538 bytes captured)
  - Arrival Time: May 17, 2012 18:15:30.298459000
  - Time delta from previous packet: 0.000123000 seconds
  - Time since reference or first frame: 11.441798000 seconds
  - Frame Number: 1803
  - Packet Length: 538 bytes
  - Capture Length: 538 bytes
  - Protocols in frame: eth:ip:udp:sip:sdp

```
00000000  00 C6 12 64 99 63 00 C6  12 00 01 63 08 00 45 00
00000010  02 0C 59 58 00 00 40 11  2E 04 C6 12 00 64 C6 12
00000020  64 FC 13 C4 13 C4 01 F8  39 FB 49 4E 56 49 54 45
00000030  20 73 69 70 3A 69 64 35  30 30 39 39 40 31 39 38
00000040  2E 31 38 2E 31 30 30 2E  32 35 32 20 53 49 50 2F
00000050  32 2E 30 0D 0A 56 69 61  3A 20 53 49 50 2F 32 2E
00000060  30 2F 55 44 50 20 31 39  38 2E 31 38 2E 30 2E 31
00000070  30 30 3A 35 30 36 30 3B  62 72 61 6E 63 68 3D 7A
00000080  39 68 47 34 62 4B 31 30  30 41 43 31 33 34 35 33
```

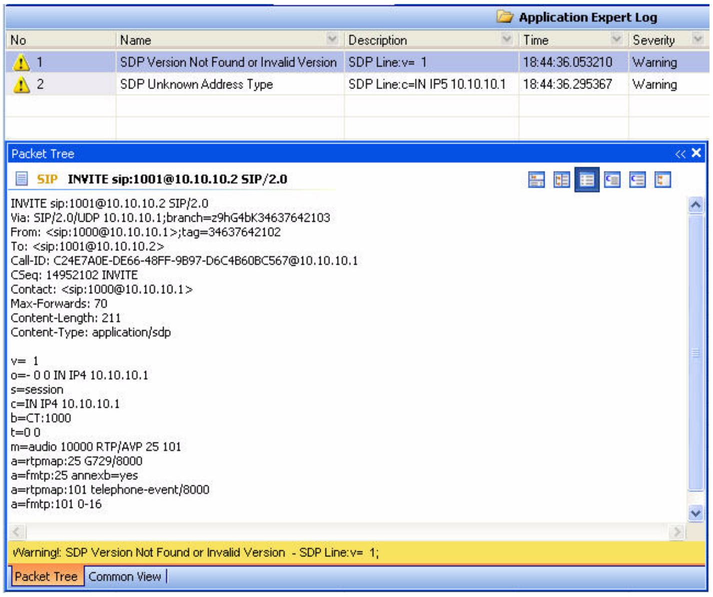
Figure 5-6. SIP Endpoint Statistics

Analyzer provides a common set of endpoint statistics for all supported *Application* layer protocols, as described in Table 4-5 and Table 4-6 on page 4-15.

SIP Errors Logged by Analyzer

You can view the errors logged in Analyzer by accessing the *Application Expert Log* view. From a SIP analyzer point of view, there are three types of errors, as shown in Figure 5-7:

- SIP Error with *Severity* = *Error*, where invalid SIP messages are received by the analyzer. More exactly, the messages are too malformed to reach any conclusion.
- SIP Error with *Severity* = *Warning*, which contains malformed packets that can be processed.
- SIP Error with *Severity* = *Informational*—for miscellaneous events (for example, packet duplicates).



No	Name	Description	Time	Severity
⚠ 1	SDP Version Not Found or Invalid Version	SDP Line:v= 1	18:44:36.053210	Warning
⚠ 2	SDP Unknown Address Type	SDP Line:c=IN IP5 10.10.10.1	18:44:36.295367	Warning

SIP INVITE sip:1001@10.10.10.2 SIP/2.0

```
INVITE sip:1001@10.10.10.2 SIP/2.0
Via: SIP/2.0/UDP 10.10.10.1;branch=z9hG4bK34637642103
From: <sip:1000@10.10.10.1>;tag=34637642102
To: <sip:1001@10.10.10.2>
Call-ID: C24E7A0E-DE66-48FF-9B97-D6C4B60BC567@10.10.10.1
CSeq: 14952102 INVITE
Contact: <sip:1000@10.10.10.1>
Max-Forwards: 70
Content-Length: 211
Content-Type: application/sdp

v= 1
o=- 0 0 IN IP4 10.10.10.1
s=session
c=IN IP4 10.10.10.1
b=CT:1000
t=0 0
m=audio 10000 RTP/AVP 25 101
a=rtpmap:25 G729/8000
a=fmtp:25 annexb=yes
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

Warning!: SDP Version Not Found or Invalid Version - SDP Line:v= 1;

Figure 5-7. SIP Errors

The SDP errors that can be detected and displayed in Analyzer are:

- SDP Not Enough Lines
- SDP Version Not Found or Invalid Version
- SDP Not Enough Parameters
- SDP Unknown Network Type
- SDP Unknown Address Type
- SDP Unknown Line
- SDP Time Not Enough Parameters
- SDP Bandwidth Not Enough Parameters
- SDP Bandwidth Unknown Modifier

- SDP Attributes Not Enough Parameters
- SDP Encrypt Key Not Enough Parameters
- SDP Media Not Enough Parameters
- SDP Media Attributes Not Enough Parameters
- SDP Media Bandwidth Not Enough Parameters
- SDP Media Bandwidth Unknown Modifier
- SDP Media Encrypt Key Unknown Modifier
- SDP Media Unknown Parameter
- SDP Media Unknown Network Type
- SDP Media Unknown Address Type

6

MGCP Captures

Analyzer can trace MGCP flows, providing ladder diagrams and specific MGCP statistics and protocol errors.

Analyzer can detect two types of MGCP endpoints: *Gateway* endpoints and *Call Agent* endpoints. Actually, a *Gateway* endpoint in Analyzer may mean a real gateway or an endpoint of a real gateway, while a *Call Agent* endpoint means a real Call Agent.

MGCP Conversations

This section briefly describes the MGCP call types that can be traced by Analyzer. Except for this list, Analyzer detects only isolated call segments.

There are three basic MGCP conversation types shown in Analyzer:

- Registration conversations
- Call Control conversations
- Miscellaneous conversations

The MGCP call types traced by Analyzer are:

- MGCP Gateway – MGCP Call Agent basic call with one call ID and one conversation, as shown in Figure 6-1.

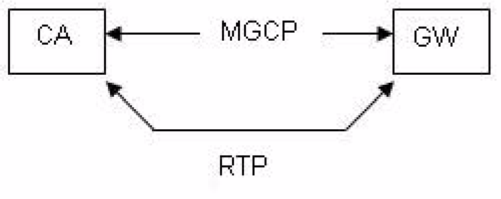


Figure 6-1. MGCP Gateway - MGCP Call Agent Basic Call with One Call ID and One Conversation

- MGCP Gateway - MGCP Call Agent – MGCP Gateway basic call, with the same call ID provided by the Call Agent for both connections (one call ID, one conversation); the RTP stream goes directly from one gateway to another, as shown in Figure 6-2.

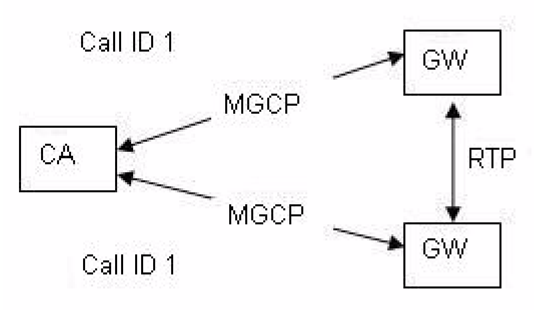


Figure 6-2. MGCP Gateway - MGCP Call Agent - MGCP Gateway Basic Call with One Call ID and One Conversation

- MGCP Gateway - MGCP Call Agent – MGCP Gateway basic call, with different call IDs provided by the Call Agent for each connection (two call IDs, two conversations); the RTP stream goes directly from one gateway to another, as shown in Figure 6-3.

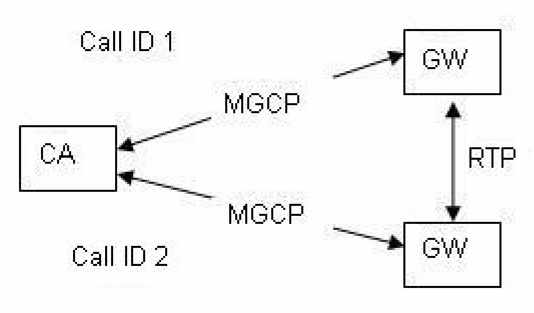


Figure 6-3. MGCP Gateway - MGCP Call Agent - MGCP Gateway Basic Call with Two Call IDs and Two Conversations Joined through the RTP Stream

MGCP Statistics

The MGCP specific statistics provided by Analyzer are grouped into two main categories:

- Conversation Statistics – the MGCP conversation specific parameters shown in the *Application Conversations* view
- Endpoint Statistics – the statistics shown in the *Application Summary* and *Application Endpoints* views

To view only the MGCP related data in the *Application Conversation* or *Application Endpoints* view, select **MGCP** from the *Filter* field in the left pane of the *Analyzer* main window, as shown in Figure 6-4.

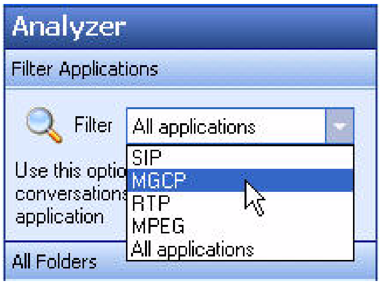
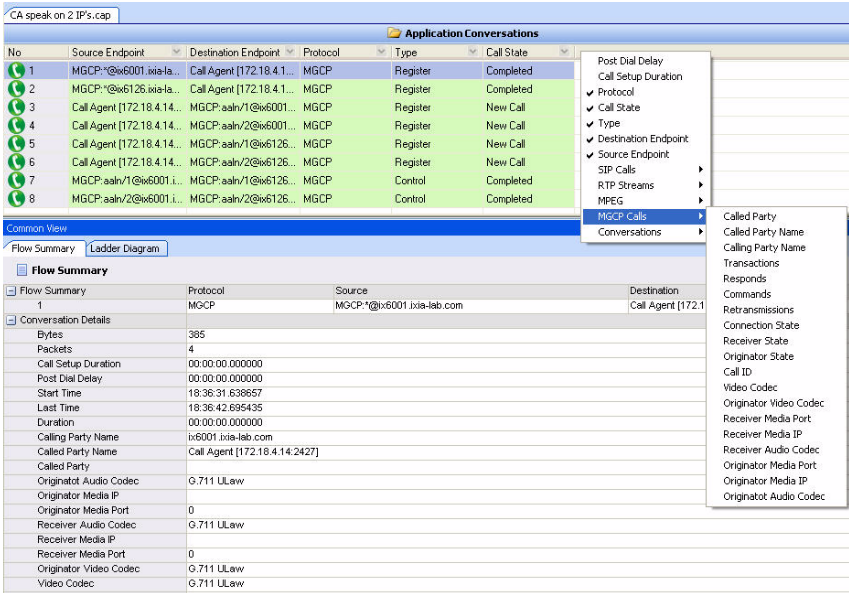


Figure 6-4. Applications Filter - MGCP

Conversation Statistics

The MGCP specific flow statistics can be viewed in the *Application Conversation* main view and in the *Flow Summary* panel of the *Common View* under *Application Conversations*, as shown in Figure 6-5.



No	Source Endpoint	Destination Endpoint	Protocol	Type	Call State
1	MGCP:*@ix6001.ixia-la...	Call Agent [172.18.4.1...	MGCP	Register	Completed
2	MGCP:*@ix6126.ixia-la...	Call Agent [172.18.4.1...	MGCP	Register	Completed
3	Call Agent [172.18.4.14...	MGCP:aaln/1@ix6001...	MGCP	Register	New Call
4	Call Agent [172.18.4.14...	MGCP:aaln/2@ix6001...	MGCP	Register	New Call
5	Call Agent [172.18.4.14...	MGCP:aaln/1@ix6126...	MGCP	Register	New Call
6	Call Agent [172.18.4.14...	MGCP:aaln/2@ix6126...	MGCP	Register	New Call
7	MGCP:aaln/1@ix6001.i...	MGCP:aaln/1@ix6126...	MGCP	Control	Completed
8	MGCP:aaln/2@ix6001.i...	MGCP:aaln/2@ix6126...	MGCP	Control	Completed

Flow Summary	Protocol	Source	Destination
1	MGCP	MGCP:*@ix6001.ixia-lab.com	Call Agent [172.1
Conversation Details			
Bytes	385		
Packets	4		
Call Setup Duration	00:00:00.000000		
Post Dial Delay	00:00:00.000000		
Start Time	18:36:31.638657		
Last Time	18:36:42.695435		
Duration	00:00:00.000000		
Calling Party Name	ix6001.ixia-lab.com		
Called Party Name	Call Agent [172.18.4.14:2427]		
Called Party			
Originatot Audio Codec	G.711 ULaw		
Originator Media IP			
Originator Media Port	0		
Receiver Audio Codec	G.711 ULaw		
Receiver Media IP			
Receiver Media Port	0		
Originator Video Codec	G.711 ULaw		
Video Codec	G.711 ULaw		

Figure 6-5. MGCP Conversation Statistics

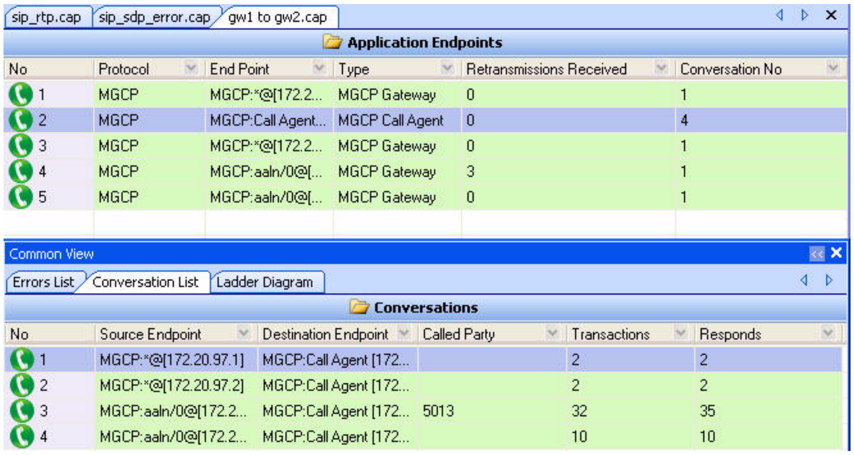
The MGCP specific flow statistics provided by Analyzer are described in Table 6-1.

Table 6-1. MGCP Conversation Statistics

Parameter	Description
Call Setup Duration	The duration of the call setup phase
Called Party	Called party URI
Called Party Name	Called party name, if available
Calling Party Name	Calling party name, if available
Transactions	The number of MGCP transactions performed during the conversation
Responds	The number of response messages for the selected conversation
Commands	The number of command messages for the selected conversation
Retransmissions	The number of retransmitted messages during the conversation
Connection State	The connection state (inactive, receive only, send-receive)
Post Dial Delay	The time between typing in the last digit of a telephone number and receiving a ring or busy signal
Receiver State	The receiver endpoint state (off-hook, on-hook, hook-flash, send digits, and so on)
Originator State	The originator endpoint state (off-hook, on-hook, hook-flash, send digits, and so on)
Call ID	The call identifier
Receiver Media Port	The port used by the receiver endpoint for RTP traffic
Receiver Media IP	The IP address used by the receiver endpoint for RTP traffic
Receiver Audio Codec	The audio codec negotiated by the receiver
Originator Media Port	The port used by the originator endpoint for RTP traffic
Originator Media IP	The IP address used by the originator endpoint for RTP traffic
Originator Audio Codec	The audio codec negotiated by the originator

Endpoint Statistics

The MGCP endpoint statistics can be viewed in the *Application Summary* and *Application Endpoints* views, as shown in Figure 6-6. Analyzer provides a common set of endpoint statistics for all the supported *Application* layer protocols, as described in Table 4-5 and Table 4-6 on page 4-15.



Application Endpoints

No	Protocol	End Point	Type	Retransmissions Received	Conversation No
☎ 1	MGCP	MGCP:*@[172.2...	MGCP Gateway	0	1
☎ 2	MGCP	MGCP:Call Agent...	MGCP Call Agent	0	4
☎ 3	MGCP	MGCP:*@[172.2...	MGCP Gateway	0	1
☎ 4	MGCP	MGCP:aaln/0@[...	MGCP Gateway	3	1
☎ 5	MGCP	MGCP:aaln/0@[...	MGCP Gateway	0	1

Conversations

No	Source Endpoint	Destination Endpoint	Called Party	Transactions	Responds
☎ 1	MGCP:*@[172.20.97.1]	MGCP:Call Agent [172...		2	2
☎ 2	MGCP:*@[172.20.97.2]	MGCP:Call Agent [172...		2	2
☎ 3	MGCP:aaln/0@[172.2...	MGCP:Call Agent [172...	5013	32	35
☎ 4	MGCP:aaln/0@[172.2...	MGCP:Call Agent [172...		10	10

Figure 6-6. MGCP Endpoint Statistics

MGCP Errors Logged by Analyzer

You can view the errors logged in Analyzer by accessing the *Application Expert Log* view.

There are two types of MGCP errors logged: one depending on the gateway endpoint state, and another one, coming as a result of receiving an error code in a response message:

- MGCP Protocol Error – Parser error
- MGCP Protocol Error – Endpoint Name empty
- MGCP Protocol Error – MGCP Verb empty
- MGCP Protocol Error RESPONSE – Absent Transaction ID
- MGCP Error – Unknown source/destination for this response
- MGCP Protocol Error CRCX – Error on the CRCX (Create Connection message) parameters
- MGCP Protocol Error MDCX – Error on the MDCX (Modify Connection message) parameters
- MGCP Protocol Error NTFY – Error on the NTFY (Notify message) parameters
- MGCP Protocol Error RSIP – Error on the RSIP (Registration in Progress message) parameters
- MGCP Protocol Error RESPONSE – Error on the RESPONSE parameters

- MGCP Protocol Error RQNT – Error on the RQNT (Request Notification message) parameters
- MGCP Protocol Error AUCX – Error on the AUCX (Audit Connection message) parameters

The SDP errors that can be detected and displayed in *Analyzer* are:

- SDP Not Enough Lines
- SDP Version Not Found or Invalid Version
- SDP Not Enough Parameters
- SDP Unknown Network Type
- SDP Unknown Address Type
- SDP Unknown Line
- SDP Time Not Enough Parameters
- SDP Bandwidth Not Enough Parameters
- SDP Bandwidth Unknown Modifier
- SDP Attributes Not Enough Parameters
- SDP Encrypt Key Not Enough Parameters
- SDP Media Not Enough Parameters
- SDP Media Attributes Not Enough Parameters
- SDP Media Bandwidth Not Enough Parameters
- SDP Media Bandwidth Unknown Modifier
- SDP Media Encrypt Key Unknown Modifier
- SDP Media Unknown Parameter
- SDP Media Unknown Network Type
- SDP Media Unknown Address Type

7 MPEG Captures

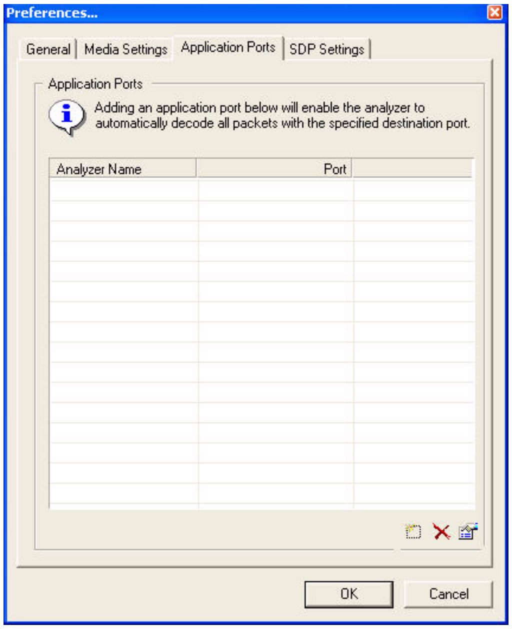
Analyzer provides the ability to decode MPEG Multi Program Transport streams, allowing the user to play back the streams.

To view a video stream in Analyzer, you must decode the stream as video. There are two options available:

- Configure the *Application Ports* to ensure that all the packets with a specified destination port decoded as video (MPEG) stream, before performing or opening the capture;
- Use the **Decode as..**. option after the capture is performed.

To set the *Application Ports* to automatically decode the packets as MPEG:

1. Select **Options** > **Preferences** from the main menu. The Preferences dialog opens.
2. Select the Application Ports tab, as shown in Figure 7-1 on page 7-2.

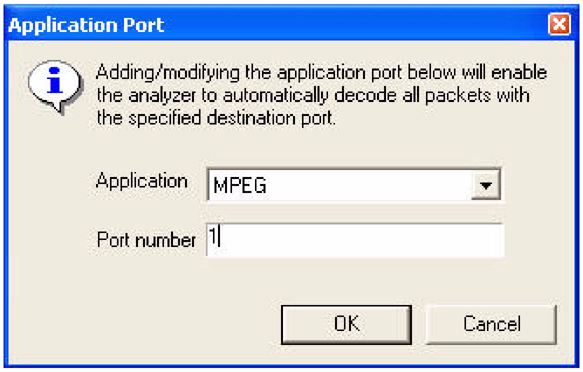


Adding an application port below will enable the analyzer to automatically decode all packets with the specified destination port.

Analyzer Name	Port

Figure 7-1. Setting the Application Ports

3. Click the **Add new port** button in the bottom-right corner of the window. The Application Port dialog opens.
4. Select **MPEG** from the Application drop-down list and type the appropriate port value in the *Port number* field, as shown in Figure 7-2.



Adding/modifying the application port below will enable the analyzer to automatically decode all packets with the specified destination port.

Application MPEG

Port number 1

Figure 7-2. Adding a New Port to the Application Ports Lists

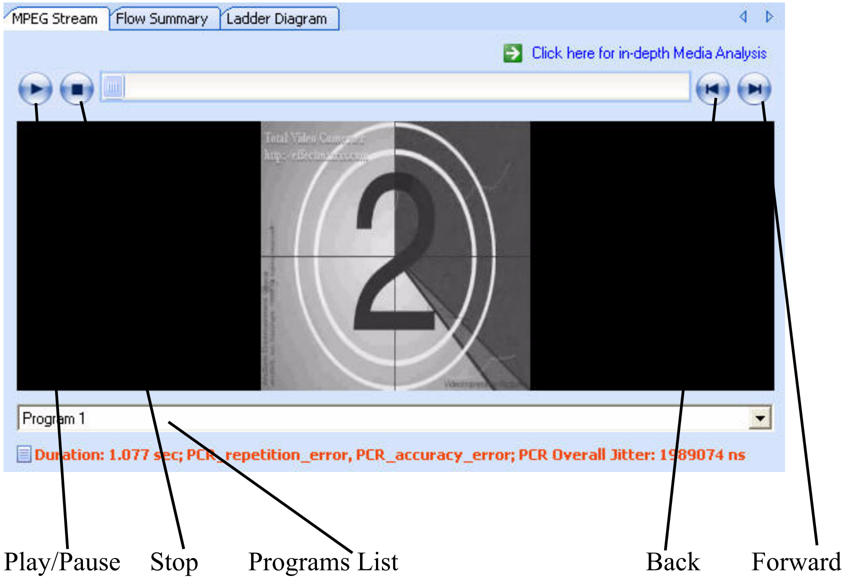
5. Click **OK** to apply the settings. The port is added to the list, and all the packets having as destination port the value set at step 4 are decoded as MPEG streams.

To decode a video stream in Analyzer by using **Decode as...**:

1. Open the video capture in Analyzer.
2. In the *Network Packets* view, select the packet, right-click it, and select **Decode as...**.

3. In the Decode as... dialog, click the Transport tab and select **MPEG** from the list.
4. Click OK.

The packet is decoded as MPEG and you can play back the video sequence by using the available buttons, as shown in Figure 7-3.



Duration: 1.077 sec; PCR_repetition_error, PCR_accuracy_error; PCR Overall Jitter: 1989074 ns

Figure 7-3. Video Viewer

8 RTP Captures

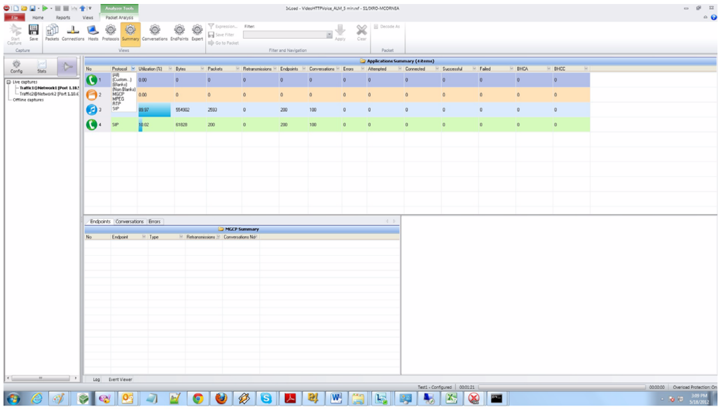
Analyzer can trace RTP streams, providing RTP quality metrics for Voice over IP networks and a lot of viewers for in-depth Media Analysis.

This chapter describes the RTP specific viewers in Analyzer and the provided statistics for the RTP captures:

- *RTP Application Conversations View* on page 8-1.
- *Detailed RTP Viewers* on page 8-6.
- *RTP Specific Errors* on page 8-9.

RTP Application Conversations View

To view only the RTP related data in the *Application Conversation* or *Application Endpoints* views, select **RTP** from the *Filter* field in the left pane of the Analyzer main window, as shown in Figure 8-1.



Applications Summary (4 items)

No	Protocol	Utilization (%)	Bytes	Packets	Retransmissions	Endpoints	Conversations	Errors	Attempted	Connected	Successful	Failed	BHCA	BHCC
1		0.00	0	0	0	0	0	0	0	0	0	0	0	0
2		0.00	0	0	0	0	0	0	0	0	0	0	0	0
3		89.97	554902	2593	0	200	100	0	0	0	0	0	0	0
4	SIP	10.02	61828	200	0	200	100	0	0	0	0	0	0	0

MGCP Summary

No	Endpoint	Type	Retransmissions	Conversations No

Figure 8-1. Applications Filter - RTP

By selecting an RTP conversation in the *Application Conversations* view, you can view in the *Common View* pane, the *RTP Stream* view, as shown in Figure 8-2 on page 8-2.

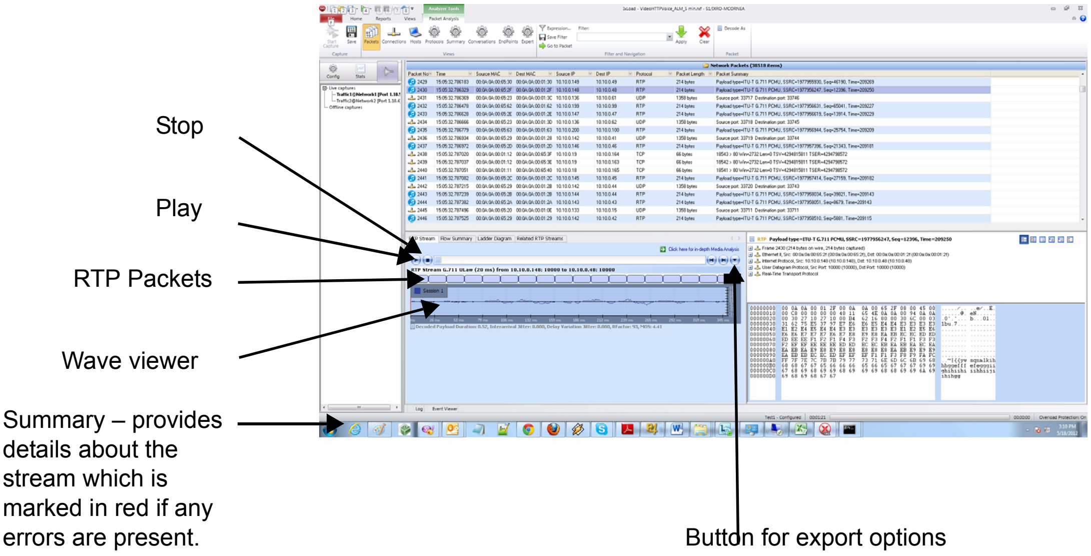

Stop
Play
RTP Packets
Wave viewer
Summary – provides details about the stream which is marked in red if any errors are present.
Button for export options

Figure 8-2. RTP Application Conversations

The RTP specific statistics provided can be shown by right-clicking the header in the *Application Conversations* view and selecting from the *RTP Streams* the statistics to show, from the ones described in Table 8-1.

Table 8-1. RTP Statistics in Application Conversations View

Statistic	Description
Codec	The codec used to transmit the RTP Stream
Payload Size	The payload size for one packet from the selected conversation
PTime (ms)	The packetization interval
RTP Bytes	The total number of bytes for the selected RTP Conversation
RTP Packets	The total number of packets for the selected RTP Conversation
Packet Loss	The total number of packets lost or dropped by the network, for the selected RTP Conversation (packet loss occurs when one or more packets of data traveling across a network fail to reach their destination).
Late Packets	The number of packets arrived with a certain delay at the receiving IP test point

Table 8-1. RTP Statistics in Application Conversations View (Continued)

Statistic	Description
Error Packets	The number of packets that fail the validity check on being received at an IP test point. This includes the malformed RTP, RTCP, and XRTCP packets.
Misorder Packets	The number of out-of-sequence packets at the receiving IP test point
Interarrival Jitter	The interarrival jitter *J* is defined as the mean deviation (smoothed absolute value) of the difference *D* in packet spacing at the receiver, as compared to the sender for a pair of packets. It is a measure of sudden delay variation, an estimate of the statistical variance of the RTP data packet interarrival time, measured in the timestamp unit.
Max Interarrival Jitter	The maximum value of the *Interarrival Jitter* for the selected RTP conversation
Delay Variation Jitter	The sum of all the delays corresponding to all the received packets
Max Delay Variation Jitter	The maximum value of the *Delay Variation Jitter* for the selected RTP conversation
R Factor	The *R factor* is a voice quality metric describing the segment of the call that is carried over this RTP session. It is expressed as an integer in the 0 to 100 range.
MOS	In voice telephony, especially when codecs are used to compress the bandwidth requirement of a digitized voice connection from the standard 64 kilobit/second PCM modulation, the Mean Opinion Score (MOS) provides a numerical indication of the perceived quality of received human speech over the connection. The MOS is expressed as a single number in the 1 to 5 range, where 1 is lowest perceived quality, and 5 is the highest perceived quality.
Bandwidth (kBps)	The data transmission rate for the selected conversation
Duplicate Packets	The total number of duplicate packets found for the selected conversation.
RTCP Packets	The total number of RTCP packets for the selected RTP Conversation.
RTCP Bytes	The total number of RTCP bytes for the selected RTP Conversation.
RTCP Sender Reports	The total number of RTCP Sender Reports packets for the selected RTP Conversation.
RTCP Receiver Reports	The total number of RTCP Receiver Reports packets for the selected RTP Conversation.

Table 8-1. RTP Statistics in Application Conversations View (Continued)

Statistic	Description
RTCP SDES	The total number of RTCP SDES packets for the selected RTP Conversation.
RTCP APP	The total number of RTCP APP packets for the selected RTP Conversation
RTCP BYE	The total number of RTCP BYE packets for the selected RTP Conversation
RTCP Malformed Packets	The total number of RTCP packets that are not part of the previous 5 categories

RTP Stream Viewer

For a selected RTP conversation, two stream representations are available in *Common View: RTP Stream* and *Related RTP Stream*, as shown in Figure 8-2 on page 8-2.

In the *RTP Stream* viewer, you can play back the selected audio stream.

A set of RTP statistics for the selected audio stream is provided, as described in Table 8-2.

Table 8-2. RTP Statistics in RTP Stream Viewer

Statistic	Description
Decoded Payload Duration	The stream duration, in seconds (s)
Interarrival Jitter	The interarrival jitter *J* is defined as the mean deviation (smoothed absolute value) of the difference *D* in packet spacing at the receiver, as compared to the sender, for a pair of packets. It is a measure of sudden delay variation, an estimate of the statistical variance of the RTP data packet interarrival time, measured in the timestamp unit.
Delay Variation Jitter	The sum of all the delays corresponding to all the received packets.
R Factor	The *R factor* is a voice quality metric describing the segment of the call that is carried over this RTP session. It is expressed as an integer in the 0 to 100 range.

Table 8-2. RTP Statistics in RTP Stream Viewer (Continued)

Statistic	Description
MOS	In voice telephony, especially when codecs are used to compress the bandwidth requirement of a digitized voice connection from the standard 64 kilobit/second PCM modulation, the Mean Opinion Score (MOS) provides a numerical indication of the perceived quality of received human speech over the connection. The MOS is expressed as a single number in the 1 to 5 range, where 1 is the lowest perceived quality, and 5 is the highest perceived quality.
Impairments, if present	The number of network impairments (for example, packet loss, latency, and so on)

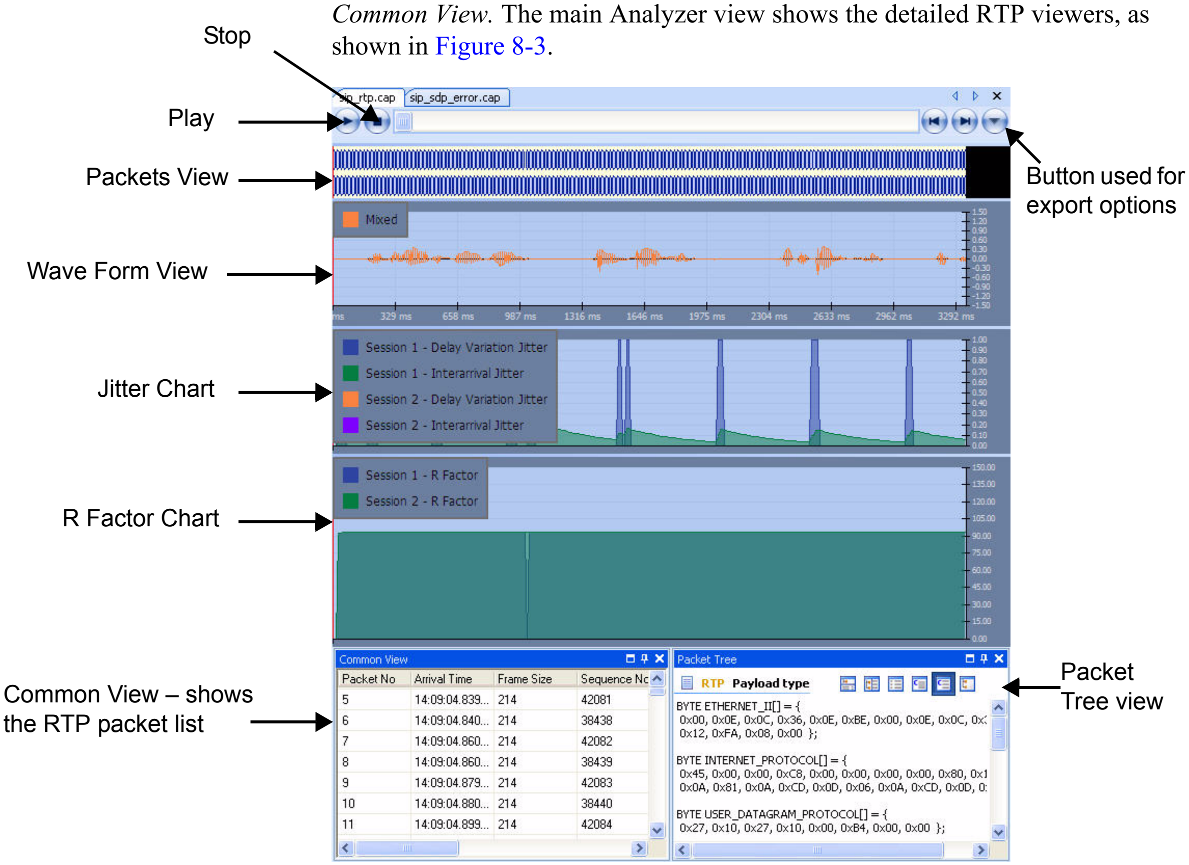
You can also export the selected audio stream in a wave file as PCM 16 Bit 8kHz mono by using the right-click options, as described in Table 8-3.

Table 8-3. Right-Click Options in the RTP Stream Viewer

Option	Action Description
Sessions	Allows you to select the RTP sessions to show in the chart.
Show Legend	If checked, displays the legend of the sessions shown in the wave-form chart.
Export as...	Exports the selected stream to a wave file saved on disk.
Export selection as...	Exports the selected part of the RTP stream to a wave file saved on disk.

Detailed RTP Viewers

You can access the detailed RTP viewers by following the **Click here for in-depth Media Analysis** link in the top-right corner of the *RTP Stream* panel in the *Common View*. The main Analyzer view shows the detailed RTP viewers, as shown in Figure 8-3.



Packet No	Arrival Time	Frame Size	Sequence Nc
5	14:09:04.839...	214	42081
6	14:09:04.840...	214	38438
7	14:09:04.860...	214	42082
8	14:09:04.860...	214	38439
9	14:09:04.879...	214	42083
10	14:09:04.880...	214	38440
11	14:09:04.899...	214	42084

```
BYTE ETHERNET_II[] = {
 0x00, 0x0E, 0x0C, 0x36, 0x0E, 0xBE, 0x00, 0x0E, 0x0C, 0x:
 0x12, 0xFA, 0x08, 0x00  };

BYTE INTERNET_PROTOCOL[] = {
 0x45, 0x00, 0x00, 0xC8, 0x00, 0x00, 0x00, 0x00, 0x80, 0x1
 0x0A, 0x81, 0x0A, 0xCD, 0x0D, 0x06, 0x0A, 0xCD, 0x0D, 0:

BYTE USER_DATAGRAM_PROTOCOL[] = {
 0x27, 0x10, 0x27, 0x10, 0x00, 0xB4, 0x00, 0x00  };
```

Figure 8-3. RTP In-Depth Media Analysis

This section describes the RTP charts and statistics provided by these RTP detailed viewers.

Packets View

The *Packets View* provides a graphical representation of the RTP packets, being able to show multiple RTP streams in the same view, as shown in Figure 8-4.

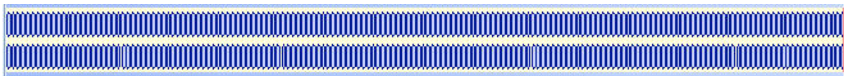


Figure 8-4. RTP Packets View

The right-click options are described in Table 8-3 on page 8-5.

Wave Form Viewer

The wave form viewer shows a graphical representation of the wave form, providing the capability to represent multiple streams in the same view, as shown in Figure 8-5.

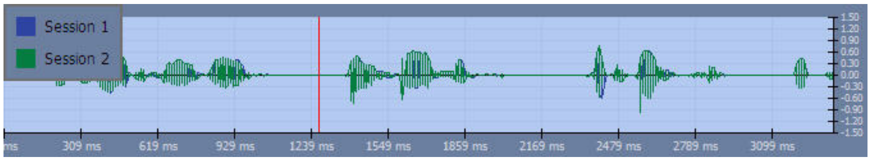


Figure 8-5. RTP Wave Form Viewer

To select the statistics to show in the *Packet Tree* view, right-click and choose one of the following options:

- **Show Packet Details** – shows detailed information about the selected packet.
- **Show Window FFT** – shows a graphical representation of the energy/frequency in a 2D chart.
- **Show QoS** – shows QoS measurements in the stream at the offset of the selected packet.

All the other right-click options, except for the ones listed above, are described in Table 8-3 on page 8-5.

Jitter Chart

To open or close the Jitter chart for the selected RTP stream, enable or disable the **RTP Charts > Jitter** option from the main menu or use the corresponding tool bar button.

The chart provides a graphical representation of **Delay Variation Jitter** and **Interarrival Jitter** evolutions, as shown in Figure 8-6.

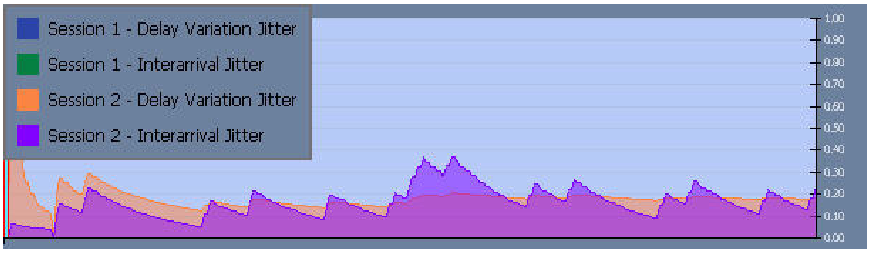


Figure 8-6. Jitter Chart

The available right-click options are the same as those described for the *Wave Form Viewer* on page 8-7.

R Factor Chart

To open or close the R factor chart for the selected RTP stream, enable or disable the **RTP Charts > R Factor** option from the main menu or use the corresponding tool bar button.

The R Factor chart provides a graphical representation of the R Factor evolution, as shown in Figure 8-7.

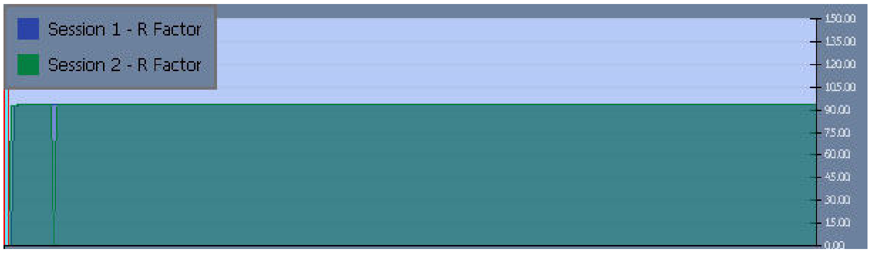


Figure 8-7. R Factor Chart

The available right-click options are the same as those described for the *Wave Form Viewer* on page 8-7.

FFT Viewer

To show the FFT viewer in the *Packet Tree* view, right-click one of the *Wave Form*, *Jitter*, or *R Factor* charts and select **Show Window FFT**.

The FFT viewer provides a graphical representation of the energy/frequency in a 2D chart, as shown in Figure 8-8.

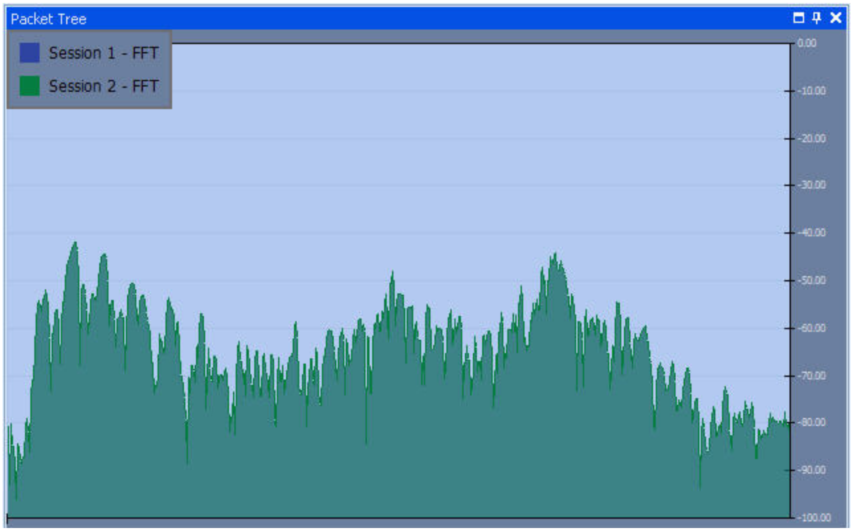
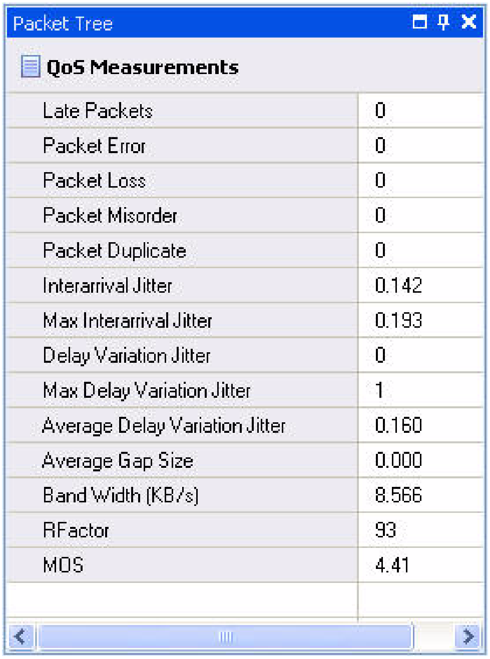


Figure 8-8. FFT Viewer

QoS Viewer

To show the QoS viewer in the *Packet Tree* view, right-click one of the *Wave Form*, *Jitter****,*** or *R Factor* charts and select **Show QoS**.

The QoS viewer shows quality parameters for the selected stream, as shown in Figure 8-9. For a description of the statistics, see Table 8-1 on page 8-2.



QoS Measurements

Late Packets	0
Packet Error	0
Packet Loss	0
Packet Misorder	0
Packet Duplicate	0
Interarrival Jitter	0.142
Max Interarrival Jitter	0.193
Delay Variation Jitter	0
Max Delay Variation Jitter	1
Average Delay Variation Jitter	0.160
Average Gap Size	0.000
Band Width (KB/s)	8.566
RFactor	93
MOS	4.41

Figure 8-9. RTP QoS Viewer

RTP Specific Errors

The following list describes the RTP errors in Analyzer:

- RTP Internal Error – Execution internal error
- Invalid RTP Version – Invalid RTP Version
- Unknown RTP Payload Type – Unknown RTP Payload Type
- RTP Padding Bit Error – Padding bit is set, but the last octet contains an invalid octet count
- RTP Extension Bit Error – Extension bit Error
- RTCP Invalid Version – Invalid RTCP Version
- RTCP Unknown Payload Type – Unknown RTCP Payload Type
- RTP Invalid Frame Size – Invalid frame size
- RTCP Padding Bit Error – The padding bit of the first packet of a compound RTCP packet is not zero.

Index

A

Application Conversations 4-13
Application Endpoints 4-14
Application Expert Log 4-16
Application Layer Views 4-11
Application Summary 4-11

C

Common View 4-23
Conversation Statistics 6-3
Customizing the Main View 4-29

D

Decode as MPEG 7-1
Decoding 4-31

F

FFT Viewer 8-8
Filtering the Information 4-29
Flow Summary 4-26

I

In-depth Media Analysis 8-6
IRU 3-2
Ixia registration utility (IRU) 3-2

J

Jitter Chart 8-7

L

Ladder Diagram 4-24

M

Main Window 4-1
Merging Captures 4-32
MGCP 6-1
MGCP Call Types 6-1
MGCP Conversations 6-1
MGCP Endpoint Statistics 6-5
MGCP Errors 6-5
MGCP Statistics 6-3
MPEG 7-1

N

Navigation Toolbox 4-10
Network Connections 4-20
Network Hosts 4-21
Network Packets 4-18
Network Views 4-18

O

Opening a Capture 4-29
Options in the RTP Stream Viewer 8-5
Options Menu 4-2

P

Packet Tree View 4-27
Packets Filter 4-32
Physical View 4-23
PRBS 4-35
Protocols 4-22

R

R Factor Chart 8-8

registering licenses 3-2

RTP 8-1

RTP Application Conversations View 8-1

RTP Errors 8-9

RTP Packets View 8-6

RTP Statistics in Common View 8-2

RTP Stream Viewer 8-4

RTP Wave Form Viewer 8-7

S

SIP Call Control 5-3

SIP Call Types 5-2

SIP Conversation Statistics 5-4

SIP Conversations 5-1

SIP Endpoint Statistics 5-6

SIP Errors 5-7

SIP Registration 5-2

SIP Statistics 5-4