



PACKETSCAN™

All-IP Analyzer

RTP, RTCP, Fax (T.38), Video Analysis

User's Manual

Document No-PKV100-3.11.22-03

Version 3.11.22

January 2014

GL Communications Inc.
818 West Diamond Avenue - Third Floor
Gaithersburg, MD 20878
Voice 301-670-4784
Fax 301-670-9187
Web page: <http://www.gl.com/>
E-mail: gl-info@gl.com

(Intentional Blank Page)

TABLE OF CONTENTS

Section 1.0 Overview	1
1.1 Introduction.....	1
1.2 Supported Protocols & Specifications.....	2
1.3 Main Features	8
1.4 Pre-requisites.....	10
1.5 VoIP Testing	11
Section 2.0 Installation Instructions	13
2.1 Installation Procedure	13
2.2 Dongle License Installation	13
2.3 PacketScan™ Installation.....	14
2.3.1 WinPcap Installation	15
Section 3.0 Getting Started with PacketScan™	19
Section 4.0 Performing Analysis using PacketScan™ – an Overview	21
4.1 Performing Real-time Analysis.....	21
4.2 Performing Offline Analysis	21
4.3 Packet Data Analysis (PDA).....	21
Section 5.0 File Menu Options	23
5.1 Start Real-time	23
5.2 Stop (Pause).....	23
5.3 Open a Trace for Off-line Analysis.....	24
5.4 Close Trace.....	24
5.5 Import	24
5.6 Save As and Close	25
5.7 Save As.....	25
5.8 Export Details	26
5.9 Export Summary	27
Section 6.0 Display Options	29
6.1 Define Views to Display	29
6.2 Summary View.....	30
6.2.1 Setting a Relative Time	30
6.2.2 Summary Column Selection.....	31
6.2.3 Column Resizing and Reordering	32
6.2.4 Repositioning Summary View	32
6.2.5 Summary Colors	33
6.2.6 Define Views.....	33
6.3 Detail View (Selecting Individual Frame)	34
6.3.1 Detail View – SIP Capture.....	35
6.3.2 Detail View – Megaco Capture.....	36
6.3.3 Detail View – H.323 Capture	37
6.3.4 Detail View – SS7 SIGTRAN Capture	38
6.3.5 Detail View – ISDN SIGTRAN Capture	39
6.3.6 Detail View – GSM A IP Capture	40
6.3.7 Detail View – UMTS IP Capture.....	41
6.3.8 Detail View – LTE Capture	42
6.3.9 Detail View – Diameter Capture	43
6.3.10 Detail View – Skinny Client Control Protocol (SCCP)	44
6.4 Hex Dump View.....	44
6.5 Statistics Views	44
6.6 Protocol Standard and User-Network Side Specifications.....	44
6.7 Time Display Formats.....	45
6.7.1 Relative Time.....	45
6.7.2 System Time	45
6.7.3 Date and Time	45

6.7.4 Difference Time	45
6.8 Latest	46
6.9 View Filtering Criteria	46
6.9.1 Setting Filtering Criteria	47
6.10 Activate Filter	48
6.11 Deactivating Filter	48
6.12 Example - View Filter	49
6.13 Searching for Specific Frames	50
6.14 Forward Search and Backward Search.....	51
6.14.1 Searching Towards the End of the Trace (Forward Search)	51
6.14.2 Searching Towards the Beginning of the Trace (Backward Search)	51
6.15 Display Trace File Name	51
6.16 Default Summary Columns	52
6.17 Invoke Packet Data Analysis	52
Section 7.0 Capture Menu Features	53
7.1 Periodic Trace Saving Options	53
7.2 Setting Capturing Options	55
7.2.1 In Memory for High Traffic Capture Rate	55
7.2.2 Circular Capture Buffer	55
7.3 Stream / Interface Selection.....	56
7.4 Setting Capture Filter.....	57
7.4.1 MAC Layer	58
7.4.2 IP	59
7.4.3 TCP	61
7.4.4 UDP	62
7.4.5 SCTP	63
7.4.6 SIP.....	64
7.4.7 RTP	65
7.4.8 MGCP	66
7.4.9 MEGACO	67
7.4.10 H323	68
7.5 GUI and Protocol Options	68
Section 8.0 Statistics.....	69
8.1 Steps to Display Statistics	70
8.1.1 Selecting Field Names (Step 1)	71
8.1.2 Defining Use Type (UT) and Statistics Type (Step 2).....	72
8.1.3 Update Selected Statistics Information List (Step 3)	73
8.1.3.1 Example 1 – Statistics with a Key UT.....	74
8.1.3.2 Example 2 – Statistics with a Total and a Key.....	76
8.1.3.3 Example 3 – Statistics Total and Field UT.....	78
8.1.4 Ranges, Wildcards and Enumerated Value Sets.....	79
8.1.5 Modifying and/or removing configured statistics.....	81
8.2 Opening and Closing Statistics View.....	81
8.3 Loading Statistics	82
8.4 Load and Edit Statistics.....	82
8.5 Save Statistics	82
8.6 Export Statistics.....	83
Section 9.0 Configuring for Call Detail Records	85
9.1 Build Call Detail Record.....	85
9.2 Active Calls Only	86
9.3 Open Call Detail Record	86
9.3.1 Active and Completed Calls	87
9.3.2 Call Duration	87
9.3.3 Find CDR	88
9.4 Select Call Detail Columns to Display	89

9.4.1 Call Detail Records View	90
9.5 Display Selected Call Summary	90
9.6 Display Entire Summary	90
9.7 Closing Call Detail Record	90
9.8 Export Call Detail Records.....	91
Section 10.0 Protocol Analyzer Configuration.....	93
10.1 Select summary columns to display.....	94
10.2 Menu Checked Options	95
10.3 Protocol Standard Selection	95
10.4 Network / User Side Selection	96
10.5 Time Format	96
10.6 Filtering Criteria.....	96
10.7 View Search	96
10.8 Connecting to Remote Database	97
10.9 Periodic Trace Saving Options.....	101
10.10 Startup Options	101
10.11 View Font Size	102
10.12 Decode Customization Options in PacketScanProt.INI	102
10.12.1 SIGTRAN	103
10.12.2 GSM A, UMTS IuCs.....	104
10.12.3 GPRS Gb.....	105
10.12.4 SIP, RTP, T.38 PDA Configurations	106
10.12.5 Skinny.....	106
10.12.6 Megaco.....	106
10.12.7 LTE Diameter Configurations	107
10.12.8 General	107
10.12.9 IPCapt.ini File.....	108
10.13 Define Summary Columns	110
10.14 Capture Options.....	113
Section 11.0 Status Indicators	115
11.1 Capture Rate.....	115
11.2 Trace File Name.....	115
11.3 Filtered and Total Frame Count.....	115
11.4 Missed Frames.....	115
Section 12.0 Packet Data Analysis – Traffic Analyzer Summary View	117
12.1 Overview	117
12.2 Summary View	118
12.2.1 Call Summary	118
12.2.2 Graphs	121
12.2.2.1 Active Calls Graph	121
12.2.2.2 Average Jitter Distribution	122
12.2.2.3 E-Model	122
12.2.2.4 RTP Packets Graph	124
12.2.2.5 Analysis of Fax over IP (T.38)	124
12.2.2.6 Call Graph	126
Call Summary – Signaling, Audio, & Video QoS Parameters.....	129
12.2.2.7 Signaling Parameters	129
12.2.2.8 Audio Parameters	130
12.2.2.9 Video QoS Parameters	130
12.2.3 Counters (Call Quality Parameters)	132
12.2.3.1 SIP	133
12.2.3.2 H323	134
12.2.3.3 MEGACO	135
12.2.3.4 RTP	136
12.2.3.5 GSM A	137

12.2.3.6 IuCS.....	138
12.3 File Menu Options.....	139
12.3.1 Export Displayed Summary	139
12.3.2 Export Terminated Calls	140
12.4 View Menu Options	140
12.4.1 Toolbar/Status Bar	140
12.4.2 Find.....	141
12.4.3 Call Detail View.....	142
12.4.4 Go To Analyzer	142
12.5 Call Summary Menu Options	142
12.5.1 Protocols.....	142
12.5.2 Filters	147
12.5.3 Save Call.....	149
12.5.4 Reports.....	151
12.5.5 Extract Fax Image.....	152
12.5.6 Play Audio	153
12.5.7 Write to File.....	154
12.5.8 Record Video	158
12.5.8.1 Video Codecs.....	159
12.5.8.2 Procedure	160
12.6 Additional Settings.....	160
12.6.1 E-Model Parameters	160
12.6.2 VQMon Settings	161
12.6.3 Payload Map Table.....	162
12.6.3.1 Codec Type	162
12.6.4 Codec Parameter Settings	163
12.6.5 Triggers and Action Settings	166
12.6.5.1 Trigger List.....	166
12.6.5.2 Filter Selection.....	167
12.6.5.3 Save Call to File	169
12.6.5.4 Audio Recording.....	169
12.6.5.5 User Defined	170
12.6.5.6 Send e-mail.....	170
12.6.5.7 Alert Summary	170
12.6.5.8 Call Detail Record.....	171
12.6.5.9 Extract Fax Image.....	174
12.6.5.10 File Menu Options.....	174
12.6.5.11 Example – Using Triggers and Action Feature	175
12.6.6 PDA Startup Options.....	176
12.7 Alert Summary.....	177
Section 13.0 Packet Data Analysis-- Detail View (RTP Diagnostic View)	179
13.1 Overview.....	179
13.2 Columns in Detail View.....	180
13.2.1 Functions Invoked By Right Click.....	182
13.3 Statistics and Graphs	183
13.3.1 RTP Statistics.....	183
13.3.2 RTCP Statistics.....	184
13.4 Graphs.....	186
13.4.1 Gap Graph.....	186
13.4.2 Jitter Graph	187
13.4.3 Gap Distribution Graph	188
13.4.4 Jitter Distribution Graph	189
13.4.5 MOS Graph (Mean Opinion Score)	190
13.4.6 Inband Events	191
13.4.7 RTP Events (Outband Events)	193

13.4.8 Wave Graph.....	193
13.4.9 Spectral Display	194
13.4.10 R-Factor Statistics.....	195
13.4.10.1 Quality Metrics based on E-model	195
13.4.10.2 Degradation Factor	199
13.4.10.3 Burst Metrics.....	199
13.4.10.4 Jitter Buffer Stats	200
13.5 File Menu Options	201
13.5.1 Export Displayed Summary	201
13.5.2 Export Terminated Calls	202
13.6 View Menu Options	202
13.6.1 Find	202
13.6.2 Call Summary View.....	202
13.6.3 Go To Analyzer.....	202
13.7 Detail View Menu Options	202
13.7.1 Save Call	202
13.7.2 Reports	202
13.7.3 Play Audio	202
13.7.4 Write To File	202
13.7.5 Inband Options	203
13.7.5.1 User Options.....	203
13.7.5.2 Parameters.....	203
13.7.5.3 User Defined Tones	204
13.8 Additional Settings.....	204
Section 14.0 Packet Data Analysis – Registration Summary	205
Note: This feature is applicable only for SIP calls.	205
14.1 Overview	205
14.2 Registration Summary	206
14.3 Registration Filters.....	206
14.4 Registration Statistics.....	207
14.5 Graphs	207
14.5.1 Active Registration Graph	207
14.5.2 Registration Trace	207
Appendix A: Glossary of Protocol Fields.....	209
Appendix B: Call States.....	215
Appendix C: SIP Registration States.....	217
Appendix D: Graphs.....	219
<input type="checkbox"/> Summary View Graphs	219
<input type="checkbox"/> Detail View Graphs	219
<input type="checkbox"/> Registration Summary Graphs.....	219
Appendix E: Additional Utilities	221
<input type="checkbox"/> HDL File Conversion Utility	221
<input type="checkbox"/> Advanced Excel Add-in for Call Detail Record (CDR) Analysis.....	223
<input type="checkbox"/> Advanced Excel Add-in for Reports.....	224

(Intentional Blank Page)

TABLE OF FIGURES

Figure 1: PacketScan™ Main Image.....	1
Figure 2: Testing networks components with PacketScan™	11
Figure 3: Dongle Installation	13
Figure 4: Welcome Screen	14
Figure 5: Choose Destination Location	14
Figure 6: Setup Status.....	15
Figure 7: WinPcap Installation Wizard.....	15
Figure 8: WinPcap Welcome Screen.....	16
Figure 9: WinPcap License Agreement Screen.....	16
Figure 10: WinPcap Installation Wizard –Screen4.....	17
Figure 11: WinPCap Installation Completion Wizard.....	17
Figure 12: Microsoft Visual C++ 2005 Redistributable.....	18
Figure 13: PacketScan™ Installation Complete	18
Figure 14: User Interface	19
Figure 15: Starting Real-time Analysis.....	23
Figure 16: Saving the trace file.....	23
Figure 17: Open a Trace from a File for Off-line Analysis.....	24
Figure 18: HDL File Conversion Utility.....	24
Figure 19: Save Trace as File Name and Close.....	25
Figure 20: Save As.....	25
Figure 21: Exporting Trace to an ASCII File	26
Figure 22: Exporting Summary to an ASCII File	27
Figure 23: Define Views to Display	29
Figure 24: Set Relative Time	30
Figure 25: Select Columns to Display	31
Figure 26: Column Resizing and Reordering	32
Figure 27: Repositioning the Summary View.....	32
Figure 28: Set Summary Colors	33
Figure 29: Selecting Individual Frame.....	34
Figure 30: Detail View of SIP.....	35
Figure 31: Detail View of MEGACO	36
Figure 32: Detail View of H323	37
Figure 33: Detail View of SS7 SIGTRAN	38
Figure 34: Detail View of ISDN SIGTRAN.....	39
Figure 35: Detail View of GSM A over IP	40
Figure 36: Detail View of UMTS over IP.....	41
Figure 37: Detail View of LTE.....	42
Figure 38: Detail View of Diameter.....	43
Figure 39: Detail View of Skinny Client Control Protocol	44
Figure 40: Time Format	45
Figure 41: Auto Screen Refresh during Real-time Analysis.....	46
Figure 42: Setting Filtering Criteria	47
Figure 43: Activating Filter	48
Figure 44: Deactivating Filter	48
Figure 45: Example - Filter Option to filter Error Frames Only.....	49
Figure 46: Setting Search Criteria	50
Figure 47: Searching Forward.....	51
Figure 48: Trace File Name	51
Figure 49: Default Summary Columns	52
Figure 50: Traffic Analyzer	52
Figure 51: Periodic File Saving Specifications.....	53
Figure 52: Capturing Options.....	55
Figure 53: Setting the Capturing option	56
Figure 54: Specifying Stream/Interface Selection.....	56
Figure 55: Capture Filter.....	57
Figure 56: MAC Layer	58
Figure 57: MAC Address.....	58
Figure 58: IP Layer	59
Figure 59: IP Address	59
Figure 60: ANY IP Address	60
Figure 61: TCP Layer	61
Figure 62: TCP Source and Destination Port	61
Figure 63: UDP Layer	62

Figure 64: UDP Source and Destination Port.....	62
Figure 65: SCTP Layer.....	63
Figure 66: SCTP Source and Destination Port	63
Figure 67: SIP Layer	64
Figure 68: SIP Source and Destination Port.....	64
Figure 69: RTP Layer.....	65
Figure 70: RTP Port.....	65
Figure 71: MGCP Layer.....	66
Figure 72: MGCP Port.....	66
Figure 73: MEGACO Layer.....	67
Figure 74: MEGACO Binary	67
Figure 75: H.323 Layer	68
Figure 76: H.323 Ports	68
Figure 77: Protocol Analysis with Statistics View	69
Figure 78: Statistics Definition Dialog.....	70
Figure 79: Selecting Filed Names.....	71
Figure 80: Field Types.....	71
Figure 81: Selected Statistics Information List.....	73
Figure 82: Define Statistics with a Key UT	74
Figure 83: Statistics Field set as Key UT	75
Figure 84: Define Statistics with a Total & Key UT.....	76
Figure 85: Statistics with Total and Key.....	77
Figure 86: Define Statistics with a Total and Field UT	78
Figure 87: Statistics with a Total and a Field	79
Figure 88: Range List for Numeric Fields.....	79
Figure 89: Wildcards for String fields.....	80
Figure 90: Specifying Value Sets	80
Figure 91: Modify/Remove some or all statistics	81
Figure 92: Opening and Closing Statistics View.....	81
Figure 93: Loading Statistics	82
Figure 94: Save Statistics as Filename	82
Figure 95: Export Statistics as Filename	83
Figure 96: Call Detail Records View	85
Figure 97: Build Call Detail Record.....	85
Figure 98: Display Active Calls Only	86
Figure 99: Open Call Detailed Record	86
Figure 100: Warning Message	87
Figure 101: Call Duration.....	87
Figure 102: Find CDR.....	88
Figure 103: Specify CDR criteria	89
Figure 104: Select Call Trace Columns to Display.....	89
Figure 105: Close Call Detailed Record	90
Figure 106: Export Trace File	91
Figure 107: Protocol and GUI option	93
Figure 108: Save As.....	94
Figure 109: Load Option	94
Figure 110: Menu Checked Options.....	95
Figure 111: Protocol Standard Selection	95
Figure 112: Network/User side Selection	96
Figure 113: Time Format	96
Figure 114: TCP Connection Options	97
Figure 115: Startup Options.....	101
Figure 116: View Font size.....	102
Figure 117: INI Decode Options	103
Figure 118: PacketScanProt.ini File	103
Figure 119: IPCapt.ini File	108
Figure 120: Warning Message	109
Figure 121: Define Summary Column.....	110
Figure 122: Popup Message	111
Figure 123: Adding the Summary Field to Display Summary Column.....	112
Figure 124: Added summary field	112
Figure 125: PacketScan™ Status Indicators	115
Figure 126: Packet Data Analysis – Traffic Analyzer Summary View	117
Figure 127: Call Summary Entry of SIP Call	118
Figure 128: Call Summary Entry of MEGACO Call.....	118

Figure 129: Call Summary	118
Figure 130: RTD Calculation	120
Figure 131: Active Calls Graph.....	121
Figure 132: Average Jitter Distribution	122
Figure 133: R-Factor	122
Figure 134: Mean Opinion Score	123
Figure 135: Packets Discarded.....	123
Figure 136: RTP Packets Graph.....	124
Figure 137: Fax analysis over IP (T.38) Ladder Diagram	124
Figure 138: Decode PacketScan™ Captured Fax files in GLInsight™	125
Figure 139: Call Flow Ladder Diagram for SIP Call.....	126
Figure 140: MEGACO Call Flow Ladder Diagram	127
Figure 141: H.323 Call Flow Ladder Diagram	127
Figure 142: GSMA Call Flow Ladder Diagram	128
Figure 143: IuCS Call Flow Ladder Diagram.....	128
Figure 144: Signaling, Audio and Video Parameters.....	129
Figure 145: Video QoS Statistics.....	130
Figure 146: Counter Type	132
Figure 147: SIP Counters.....	133
Figure 148: H.323 Counters	134
Figure 149: MEGACO Counters	135
Figure 150: RTP Counters	136
Figure 151: GSMA Counters	137
Figure 152: IuCS Counters.....	138
Figure 153: Export Displayed Summary	139
Figure 154: Export Summary Calls Summary	140
Figure 155: Play Sound Toolbar	140
Figure 156: Find Dialog.....	141
Figure 157: Protocols	142
Figure 158: SIP Calls.....	143
Figure 159: H.323 Calls	144
Figure 160: Auto Detected RTP Calls	145
Figure 161: MeGaCo Calls	146
Figure 162: GSM A Calls	146
Figure 163: IuCS Calls.....	147
Figure 164: Sessions.....	148
Figure 165: Save Call	149
Figure 166: Call Summary File.....	149
Figure 167: PCAP Option Selected	150
Figure 168: Selection of RTP Headers	151
Figure 169: Packetscan Call Summary Report in PDF Format.....	152
Figure 170: Extract Fax Image from Call.....	152
Figure 171: Play Jitter Options.....	153
Figure 172: Write to File	154
Figure 173: Write to File with Separate Option Selected.....	156
Figure 174: Invoke Adobe Audition after Write	157
Figure 175: Summary View Displaying Video Calls	158
Figure 176: Record	160
Figure 177: Record Video.....	160
Figure 178: E-model Parameters.....	161
Figure 179: VQMon Settings.....	161
Figure 180: Dynamic Payload Mapping Table	162
Figure 181: G726 Codec Type	163
Figure 182: AMR Codec Type.....	164
Figure 183: EVRC Codec Type	164
Figure 184: G722.1 Codec Type.....	164
Figure 185: AMR_WB Codec Type	165
Figure 186: EVRCB Codec Type.....	165
Figure 187: EVRC_C Codec Type.....	165
Figure 188: G726_VAD Codec Type.....	166
Figure 189: Triggers and Action Settings.....	166
Figure 190: Save Call Options	169
Figure 191: Audio Recording	169
Figure 192: Send e-mail	170
Figure 193: Alert Message.....	170

Figure 194: Call Detail Record	171
Figure 195: Call Side Record	171
Figure 196: Call Master Record	172
Figure 197: Call Event Record	173
Figure 198: Extract Fax Image	174
Figure 199: File Menu	174
Figure 200: Enable Triggers	175
Figure 201: Enabling Startup Options.....	176
Figure 202: Loading tgr Profile File	176
Figure 203: Trigger and Action Profile Path in sipProt.ini.....	176
Figure 204: Alert Summary.....	177
Figure 205: Detail View	179
Figure 206: Detail View Columns	180
Figure 207: Show Latest.....	182
Figure 208: Column Resizing and Reordering	182
Figure 209: Call Information	183
Figure 210: RTCP.....	184
Figure 211: RTCP Details of Sender Report	184
Figure 212: RTCP Details of Receiver Report	184
Figure 213: SDES Item	185
Figure 214: Bye Packet	185
Figure 215: 3D Gap Graph.....	186
Figure 216: 2D Gap Graph.....	186
Figure 217: 3D Jitter Graph	187
Figure 218: 2D Jitter Graph	187
Figure 219: 3D Gap Distribution Graph.....	188
Figure 220: 2D Gap Distribution Graph.....	188
Figure 221: 3D Jitter Distribution Graph	189
Figure 222: 2D Jitter Distribution Graph	189
Figure 223: 3D MOS Graph	190
Figure 224: 2D MOS Graph	190
Figure 225: Inband Events.....	191
Figure 226: Digits Only	191
Figure 227: All Events	192
Figure 228: Export to File	192
Figure 229: RTP Events Screen.....	193
Figure 230: Wave Graph.....	193
Figure 231: Offline Analysis	194
Figure 232: Spectral Display	194
Figure 233: Quality Metrics	195
Figure 234: Degradation Factor	199
Figure 235: Burst Metrics	199
Figure 236: Jitter Buffer Stats	200
Figure 237: Export Displayed Summary.....	201
Figure 238: User Options.....	203
Figure 239: Parameters.....	203
Figure 240: User Defined Tones.....	204
Figure 241: Registration Summary	205
Figure 242: Summary Columns	206
Figure 243: Registrations.....	206
Figure 244: Counter Type.....	207
Figure 245: Active Registration Graph	207
Figure 246: Registration Trace Ladder Diagram	208
Figure 247: Summary View.....	215
Figure 248: Marker Bit	216
Figure 249: Registration Status	217
Figure 250: Ethernet PCAP Trace File to HDL.....	221
Figure 251: Packet over IP CDR Analysis System	223
Figure 252: SIP CDR Analysis using Excel® Addin	223
Figure 253: Import PacketScan™ Text (*.txt) Sample Files	224
Figure 254: No. of Calls Per Day (CPD) graph.....	225
Figure 255: Calls per Day Table.....	225

Warranty Information

One Year Hardware Limited Warranty

GL Communications Inc. warrants the hardware products against defects in material and workmanship for a period of one year from receipt of the product to the recipient. If GL receives notice of defects during the warranty period, GL will either replace or repair the product and its components. In the event that GL is unable to repair or replace the product (After receipt of the defective product from the customer) within a reasonable period, the customer shall be entitled to refund of the purchase price.

One Year Software Limited Warranty

GL Communications Inc. warrants the licensed software products to perform in substantial conformance to the applicable GL software specifications for a period of one year from receipt of the product to the recipient. If GL receives notice of defects during the warranty period, GL will either replace or repair the product and its components. In the event that GL is unable to repair or replace the product (After receipt of the defective product from the customer) within a reasonable period, the customer shall be entitled to refund of the purchase price.

Extended 1 Year (total 2 years) Hardware Warranty at the time of sale is also available. Please contact GL Communications Inc for purchasing extended hardware warranty.

The basic 1-year hardware warranty is provided with the initial purchase price. The customer may renew this warranty service on a yearly basis and enjoy the benefits of first year service for the additional years. The basic and extended service includes the following:

All hardware (excluding PC) is warranted for one year from the date of purchase. GL will assist the customer to troubleshoot the purchased equipment to determine if hardware or software is defective. If hardware is determined to be defective, customer is required to send the defective equipment at their cost. GL will bear the return cost. Replacement equipment will be sent if necessary to reduce downtime to the customer.

Extended 1 Year (total 2 years) Software Warranty at the time of sale is also available. Please contact GL Communications Inc for purchasing extended software warranty.

The basic 1-year software upgrades and comprehensive support is provided with the initial purchase price. The customer may renew this warranty service on a yearly basis and enjoy the benefits of first year service for the additional years. The basic and extended service includes the following:

- Telephone, e-mail, IM, and Skype based technical support during regular GL business hours with prompt and courteous problem resolution.
- Assistance to the customer to troubleshoot the purchased equipment to determine if hardware or software is defective. If software is determined to be at fault, GL will expeditiously debug and repair the software at no cost to the customer. E-mail, FTP, and priority FedEx or equivalent will be used to send the repaired software to the customer.
- GL will maintain problem record tracking of all customer issues.

Software upgrades, bug fixes, and patches shall be provided at no cost to the customer during the warranty period

Warranty Exclusions and Limitations

The above warranty shall not apply to defects resulting from improper operation, inadequate maintenance, or unauthorized use or modification by the customer of the GL hardware & software. The warranty service and service beyond the warranty period described herein is the customer's sole remedies. In no event shall GL be liable for any direct or indirect or consequential damages.

Obtaining Service During and Beyond Warranty Period

To obtain warranty service, the customer shall return the product to GL Communications with proof of purchase and an explanation of the problem. The customer shall pay for shipping charges and shall pay for return shipping. For service beyond the warranty period, contact GL for details of available service.

GL's return policy:

GL Communications Inc. accepts returns or exchanges within 30 days from the original purchase. All returns and exchanges must be in original condition and include all accessories. All returns, exchanges and price adjustments will be made in the country of original purchase. GL Communications Inc reserves the right to request identification and to deny any return.

Software Support/Upgrade

Customer Support

GL Communications provides quality support for all users of the GL software. If you require technical assistance or have problems getting started with the software, please contact our support team using the following:

GL Communications Inc.
818 West Diamond Avenue - Third Floor
Gaithersburg, MD 20878
Voice 301-670-4784
Fax 301-670-9187
Web page: <http://www.gl.com/>
E-mail: gl-info@gl.com

Software Upgrade

The GL software will be upgraded on a periodic timeframe (usually once every three months). However the interim software releases may also be available on a routine basis. Please contact customer support for information concerning interim software releases.

All software upgrades are available on the GL Communications web site (www.gl.com). Download the latest upgrade (available id devices are covered under warranty). If additional licenses are required, contact GL Communications (using voice or email). Please note that before upgrading the any GL software, the existing installation directory should be backed-up to another location. This will allow the user to revert to the previous software in case a problem arises during upgrading

Section 1.0 Overview

1.1 Introduction

GL's **PacketScan™ - an All-IP Network Monitoring** software offers powerful features to capture and monitor live signaling and traffic over IP (version 4 and 6). It captures, segregates, monitors and collects statistics on all IP calls. Almost all VoIP and Wireless protocols over IP transport layer, as listed below, can be captured and decoded for troubleshooting network problems.

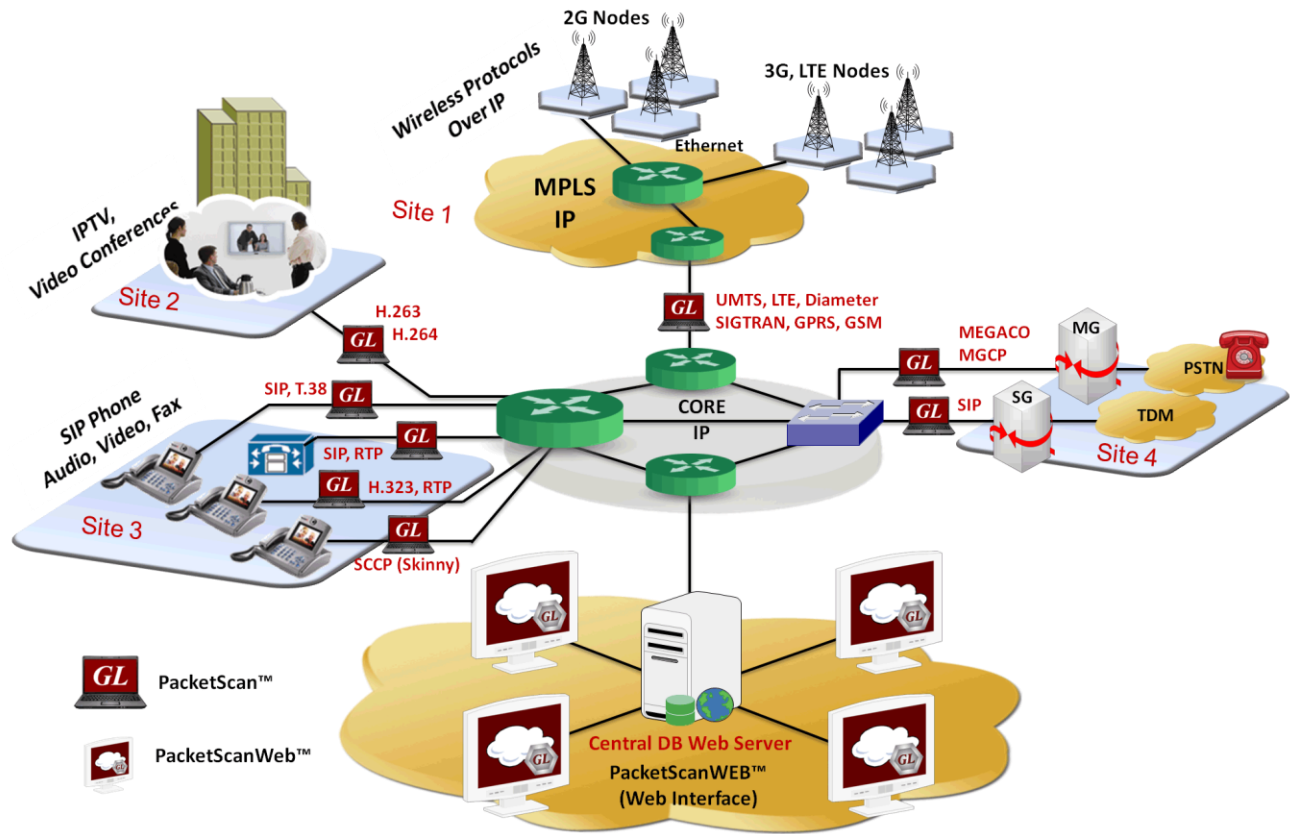


Figure 1: PacketScan™ Main Image

Some of the important applications of PacketScan™ are:

- Supports decoding of almost all industry standard signaling protocols – See [Protocol List](#)
 - SIP, SIP-I, SIP-T, H323, MEGACO, MGCP, Diameter, SCCP (Skinny)
 - LTE
 - SIGTRAN – SS7, ISDN
 - GSM A and Abis over IP
 - GPRS Gb and Gn over IP
 - UMTS IuCs and IuPs over IP
 - T.38 and Video calls
- All traffic supported – Digits, Tones, Voice, Video, Fax
- Live monitoring Ipv4 and IPv6 (version 4 and version 6) networks
- Segregates, captures, and collects statistics on VoIP and Wireless calls
- Monitors QOS (quality of service) on voice and video calls
- Permits analysis of adherence to protocol standards for the system under test or observation
- Provides graphical presentation of analysis, including ladder diagrams of protocols

Hundreds of calls can be monitored in real-time including detailed analysis of selected voice band streams. Applications include testing of IP phones, Gateways, IP Routers and Switches, and Proxies.

Users can **listen/record audio and video data** of a session in real-time; perform power, frequency, spectral, tone and digit analysis, and video analysis with ease and precision; get an exact picture of QoS (quality of the service).

Its ability to monitor / record audio and video data of a session to files (in QuickTime *.qt format), allows user to perform powerful video analysis. The captured VoIP calls with video can be played back using 3rd party VLC Viewer application.

The application is capable of displaying **Video QoS Statistics** such as Source/Destination Video Channels, Media Type, SSRC, Total Packet Counts, Missing Packets, Duplicate Packets and Out of sequence Packets, Average Delay/Gap, Video Frame Count, Frame rate, Media Delivery Index (MDI-(Delay Factor : Media Loss Rate)), and Average MDI for each video session.

PacketScan™ with Video QoS capability addresses customers long felt need of Video Call Quality in IP networks.

Detail call statistics such as packet loss, gap, jitter, delay, RTP performance statistics, R-Factor & MOS scores, and unparalleled voice band statistics can be monitored simultaneously. Sophisticated filters permit zooming and recording of specific calls of interest.

PacketScan™ further supports the following three views in **Traffic Analysis or Packet Data Analysis (PDA)** window:

- **Summary View** (Call Quality Matrix) displays complete summary of SIP/RTP/Megaco/H.323 call information in graphical format, along with a summary of alerts
- **Detail View** (RTP Diagnostic View) displays packet by packet statistics for particular call information in tabular format

These interfaces allow users to define parameters such as E-Model based MOS and R-Factor score, VQMon settings, & Dynamic Payload Mapping. It supports real-time digit capturing like DTMF, MF and user-defined digits/tones.

- **Registration Summary View** displays statistics and status of the SIP registration process, an active registration graph, and registration trace graph of each SIP registration.

What sets apart PacketScan™ or VPA (Virtual Packet Analysis) is its ability to collect vital statistics about calls for theoretically infinite time. The ability of VPA to capture data is limited only by the hard disk capacity of the PC. It can work with [PacketScanWEB™](#), a central monitoring system for a comprehensive view of network performance. It features rich graphics, ladder diagrams and CDRs (Call Detail Records).

PacketScan™ can be run on any PC with Windows® XP 32 bit, / Windows® Vista 32 bit, Windows® 7 32 bit and 64 bit OS, an Ethernet card and a sound card. All the features can be accessed through a user friendly GUI.

1.2 Supported Protocols & Specifications

All-IP PacketScan™ supports IP signaling and traffic analysis with the support for the following listed protocols:

- **SIP - RFC 3261**

SIP is an application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences). These sessions include Internet multimedia conferences, Internet (or any IP Network) telephone calls and multimedia distribution

SIP is normally used in conjunction with other protocols in order to provide complete services to the users.

- **MEGACO – RFC 3525 and 3015**

Megaco is also known as H.248 is a signaling protocol, is used between Media Gateway and Media Gateway Controller (Call Agent). Megaco/H.248 uses a series of commands to manipulate terminations, contexts, events, and signals. Megaco/H.248 is architecturally quite similar to MGCP; however, Megaco/H.248 supports a broader range of networks.

- **Media Gateway Control Protocol (MGCP) - RFC 2705/3435 (3991)**

MGCP is a protocol for controlling Voice over IP Gateways (or Call Agent endpoints) from external call control elements. It assumes a call control architecture where the call control "intelligence" is outside the gateways and handled by external call control elements. The Call Agent can create, modify and delete connections in order to establish and control media sessions with other multimedia endpoints. Also, the Call Agent can instruct the end points to detect certain events and generate signals. The endpoints automatically communicate changes in service state to the Call Agent.

- **H323**

H.323 provides the foundation for audio, video and data communication on packet based IP network. H.323 is not a single protocol rather a protocol suite, which performs all the functions necessary to establish and maintain real time audio/video/data conferencing sessions over IP data networks.

- **SDP**

SDP is a session description protocol for multimedia sessions. SIP generally uses SDP to convey session information. SDP is carried as the message body in a SIP message.

- **RTP/RTCP**

The RFC 1889 defines RTP as the service, which provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Those services include payload type identification; sequence numbering, time stamping and delivery monitoring. RTP is mostly used in conjunction with RTCP, the protocol used to monitor the quality of service and to convey information about the participants in an on-going session.

- **SCTP - RFC 2960**

In computer networking, the **Stream Control Transmission Protocol** (SCTP) is a Transport Layer protocol. It provides some of the same service features of both: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP.

The protocol was defined by the IETF Signaling Transport (SIGTRAN) and RFC 4960 defines the protocol.

- **COTP**

Connection Oriented Transport Protocol (COTP, ISO 8073). COTP transports *packets of data* from one user to the other, so the receiver will get exactly the same data boundaries as the sender transmitted.

- **SS7 SIGTRAN**

Capable of capturing and decoding SS7 over IP (ISUP, MAP, TCAP, INAP, CAMEL and more)

- **ISDN-SIGTRAN**

Capable of capturing and decoding Q.931, DASS2, DPNSS over IUA (ISDN Q.921-User Adaptation Layer)

- **GSM A over IP**

Capable of capturing and decoding GSM A over IP (BSSAP, CC, MM, RR, GCC, BCC, and more)

- **GPRS over IP**

Decodes GPRS-GB interface (BSSGP, LLC, SNDSCP, GMM, SMG, and more)

- **UMTS over IP**

It can decode UMTS over IP (RANAP, RNSAP, NBAP, CC, MM, RR, and more)

- **LTE**

Capable of capturing and decoding (S1AP, X2AP, NAS, Diameter)

- **Diameter**

The Diameter protocol is intended to provide a framework for Authentication, Authorization and Accounting (AAA) applications such as network access, roaming, and IP mobility. Diameter protocol supports decoding of following Diameter interfaces S6a, S6d, Cx, Dx, Zn, Zh, Wx, Gq, Gy, Sh, Dh, Gx, Rf, RO, Wg, Wm, Pr, Wa, Wd, Rx interfaces

- **Skinny Client Control Protocol (SCCP)**

The Skinny Call Control Protocol (SCCP), also referred to as "Skinny," is a Cisco Systems proprietary signaling and control protocol used to communicate between IP devices and Cisco Unified Communications Manager.

Apart from these, protocols supported by PacketScan™ are listed along with the specifications in the table below.

Supported Protocols		Standards / Specifications Used
SIP-3261	MAC	IEEE 802.3
Megaco3525	IP	RFC 791
Megaco3015	TCP	RFC 793
MGCP	UDP	RFC 768
H323	ICMP	RFC 792
	SIP 3261	RFC 3261
	RTCP	RFC 3550
	RTP	RFC 2833
	MEGACO	RFC 3525
	MEGACO	RFC 3015
	MGCP	RFC 3435
	H.245	H.245
	RAS	H.225
	ISDN H.225	H225 Q.931 Layer
	STUN	RFC 3489
	DNS	RFC 1035
	DHCP	RFC 1533, 2131
	SMTP	RFC 2821
	POP3	RFC 1939
	HTTP	RFC 2616
	FTP	RFC 959
	SNMP	RFC 1157,1155,1902,3416,2863,2578,3418,2011,2012 etc
	T38	ITU-T T.38
	ARP	RFC 826
	RARP	RFC 903
	RIP	RFC 2453
	SCTP	RFC 2960
	COTP	RFC 905 - ISO Transport Protocol specification ISO DP 8073
	CLNP	RFC 994 - Final text of DIS 8473
	H450	ITU-T Recommendation H.450.1 to H.450.12
	USPS	USPS Specification
	RIEP	RFC 995
	RFC 2833	RFC 2833 / RFC 4733
	H.263	ITU-T H.263
	STP	IEEE Std 802.1D-2004
	NBNS	RFC 1002
	DECnet RP (Routing Protocol)	DECnet DIGITAL Network Architecture Routing Layer Functional Specification Version 2.0.0 May 1983

	DECnet MOP (Maintenance Operation Protocol)	DECnet DIGITAL Network Architecture Maintenance Operations Functional Specification Version 3.0.0 September 1983
	DECnet NSP (Network Service Protocol)	DECnet DIGITAL Network Architecture NSP Functional Specification Phase IV Version 4.0.1 July, 1984
	DECnet SCP (Session Control Protocol)	DNA FS SESSION CONTROL
	DECnet DAP (Data Access Protocol)	Decnet Digital Network Architecture Data Access Protocol (Dap) Functional Specification Version 5.6
	DECnet CTERM (Command Terminal)	Digital Terminal Software Architecture Network Command Terminal Specification Version 1.4
	DECnet LAT (Local Area Transport)	Proprietary
	DECnet STP (Spanning Tree Protocol)	
	DECnet LAVC (Local Area VAX Cluster)	
	SNAP	RFC 1042
	SMB	ftp://ftp.microsoft.com/developr/drg/CIFS/SMB.TXT
	IPMReg	RFC 3220
	IPMAgentAdv	RFC 3220
	IDP	
	SPP	
	DDP	RFC 1742 (AppleTalk Management Information Base II)
	ATP	RFC 1742 (AppleTalk Management Information Base II)
	VinesIP	
	VinesSPP	
	VinesIPC	
	VinesRTP	
	RFC1006	RFC 1006 (ISO Transport Service on top of the TCP Version: 3)
	NetBIOS	
	Bootstrap	RFC 951
	IGRP, LAP, RTMP	
	SNA	Systems Network Architecture Formats - GA27-3136-20
	RPCall	RFC 1050 / RFC 1831
	NetIPX	
	NFS	RFC 1094
	NSAP	
	NRIP	
	NCP	RFC 801
	IPv6	RFC 2460, RFC 2402, RFC 2406
	ICMPv6	RFC 2463, 2461, 1885, 2894, 3122, 3810, 3775, 3971, 4286, 4066
	OSPF	RFC 2328

	PIMSMDM	PIM-SM : RFC 4601 / Obsolete 2362 PIM-DM: RFC 3973
	MPEG2	RFC 2250
	PIM_IP (IP layer comes above PIM-SM/DM)	RFC 791
	WiMAX	WiMAX Forum Network Architecture Stage3 Detailed Protocols and Procedures (Release1.0.0)
	GRE	RFC 2784 / RFC 1701
	SMPP	Short Message Peer-to-Peer Version 5.0 19-February-2003.
	ISUP ITU	ITU - Q.761, Q.762, Q.763 and Q.764
	LDP	RFC 5036
	MPLS	RFC 5036
	RSVP	RSVP : RFC-2205, RFC-2210 RSVP-TE : RFC-3209
	EIGRP	
	PPPoE	RFC 2516
	IGMP	RFC 3376, RFC 2236, RFC 1112
	NTP	RFC 1305
	Skinny	
	LLC	IEEE 802.2
	CLTP	T-REC-X.234
	SDP	RFC 4566
	RTSP	RFC 2326
SS7 SIGTRAN*	ISUP ITU	ITU - Q.761, Q.762, Q.763 and Q.764
	ISUP ETSI	EN 300 356 -1 V3.2.2(1998-08)
	ISUP ANSI	ANSI - T1.113.1 to T1.113.4
	IUA	RFC 4233 / RFC 5133
	BICC	BICC pl-080r1, T-REC-Q.1902.2-07/2001, T-REC-Q.1902.3-07/2001
	TUP ITU	T-REC-Q.723-11/1988
	SCTP	RFC 2960
	SCCP ITU	ITU-T Q.711-Q.714
	SCCP ANSI	ANSI rec. T.112 (1996), T1.116.2 (1996)
	SCCP ETSI	EN 300 009 -1, sept 1996, 3rd edition
	SUA ITU	RFC 3868
	SUA ANSI	Internet Engineering Task Force: Draft 2026 (sec.10)
	M2UA	RFC 3331
	M2PA	RFC 4165
	SUA ITU	RFC 3868
	SUA ANSI	Internet Engineering Task Force: Draft 2026 (sec.10)
	M3UA ITU	RFC 3332
	M3UA ANSI	RFC 3332
	MTP2- ITU	ITU-T Q.703
	MTP3 ITU	ITU-Y Q.701-Q.705 / ITU-T Q.782
	MTP3 ANSI	T1.111.4-1996
	MTP2, MTP3 ANSI	T1.111.4-1996
	ICMP	RFC 792
	MAP R99	3GPP TS 09.02 V7.14.0 (2003-09)
	MAP R4	3GPP TS 29.002 V4.18.0
	TCAP ITU	ITU-T Q.771 - Q.775
	TCAP ANSI IS-41	TIA/EIA, IS41.1-C, IS41.5

	INAP CS1 ITU / ETSI	Q1218 and ETS 300 374 1, Sept, 1994
	INAP CS2 ITU	INAP - Capability Set 2. (Q.1228)
	INAP CS2 ETSI	INAP - Capability Set 2. (EN 301 140-1-v1.3.4-1999-06)
	CAMEL V3	3GPP TS 29.078 V3.15.0
	CAMEL V6	3GPP TS 29.078 6.3.0 (2004-09)
	Test & Network Management Messages (ITU)	ITU-T Q.703, Q.704
	Test & Network Management Messages (ANSI)	ANSI T1.111.4 - 1996
ISDN-SIGTRAN*	Q.931	ITU-T Q.931 / Q.932(Facility IE) / Q.955.3 (MLPP Procedures)
	DASS2	BTNR 190:June 1992
	DPNSS	ND1301:2001/03
GSMA over IP*	BSSAP+	3GPP TS 29.018 V6.0.0
	BSSAP-LE (BSSMAP-LE/DTAP-LE)	3GPP TS 49.031 V7.3.0
	CC	3GPP TS 04.08 V7.17.0
	MM	3GPP TS 04.08 V7.17.0
	GCC (Group Call Control)	3GPP TS 44.068 V9.0.0
	BCC (Broadcast Call Control)	3GPP TS 44.069 V9.0.0
	RR	3GPP TS 04.08 V7.17.0
GPRS over IP*	BSSGP	3GPP TS 08.18 V8.10.0
	LLC	3GPP TS 04.64 V8.7.0
	GMM	3GPP TS 04.08 V7.19.0
	SMG	3GPP TS 04.08 V7.19.0
	SNDPCP	3GPP TS 04.64 V8.7.0
UMTS over IP*	RANAP	3GPP TS 25.413 V6.3.0 (2004-09)
	RNSAP	3GPP TS 25.423 V6.4.0 (2004-12)
	NBAP	3GPP TS 25.433 V6.3.0 (2004-09)
	CC	3GPP TS 04.08 V7.17.0
	MM	3GPP TS 04.08 V7.17.0
	RR	3GPP TS 04.08 V7.17.0
LTE*	S1AP	3GPP TS 36.413 V9.0.0
	X2AP	3GPP TS 36.423 V9.0.0
	NAS	3GPP TS 24.301 V9.0.0
Diameter	S6a, S6d, S13	3GPP TS 29.272 V10.3.0
	Rx	3GPP TS 29.214-b10
	Cx/Dx	3GPP TS 29.228 & TS29.229
	Gx	3GPP TS 29.212 & TS 23.203
	Zn/Zh	3GPP TS 29.109 & TS 33.220
	Wx	3GPP TS 29.234
	Gx	3GPP TS 29.212 & TS 23.203
	Gy	3GPP TS 32.29, TS 32.251 & RFC 4006
	Gq	3GPP TS 29.209
	Sh/Dh	3GPP TS 29.328 & TS 29.329
	Rf/RO	3GPP TS 32.225, 3GPP TS 32.299 3GPP TS 29.061
	Wg/Wm/Wa/Wd/Pr	3GPP TS 29.234

* Requires Additional License

1.3 Main Features

Capacity	<ul style="list-style-type: none"> • Monitor progress of up to 2000 simultaneous calls with bidirectional RTP traffic • Circular buffer with capture and view filters • Long-Term Activity Reporting
Supported Protocols	<ul style="list-style-type: none"> • SIP RFC 3261- MAC, IP, IPv6, UDP, TCP, SMPP • SIP-I, SIP-T • Megaco- RFC 3525, RFC 3015 • MGCP – RFC 3991 • H.323/H.225 • RTP - RFC 3550, RTCP, T.38, Video, and more. • SS7 SIGTRAN - SS7 over IP (ISUP, MAP, CAP, TCAP, INAP, CNAM, CAMEL) • SIGTRAN ISDN over IP - Q.931, DASS2, and DPNSS over DUA (ISDN Q.921-User Adaptation Layer) • GSMa over IP - BSSAP+, BSSMAP, CC, MM, RR, GCC, BCC, SMS • GSM Abis over IP - BTSM, CC, MM, RR, GCC, BCC, SMS • GPRS - GPRS-Gb interface (BSSGP, LLC, SDCP, GMM, SMG) • GPRS – GPRS-Gn interface (GTPv2, GTP-IP, GTP-TCP, GTP-UDP) • UMTS IuCS and IuPS over IP - RANAP, RNSAP, NBAP, CC, MM, RR • LTE - S1AP, X2AP, NAS, eGTP • Diameter – S6a, S6d, Cx, Dx, Zn, Zh, Wx, Gq, Gy, Sh, Dh, Gx, Rf, RO, Wg, Wm, Pr, Wa, Wd, Rx interfaces • Skinny Call Control Protocol (SCCP)
Supported Codecs	Almost all industry standard codec supported. For more comprehensive information on these codecs visit "Estimating Speech Quality of Packets" link
As a stand-alone tool	<ul style="list-style-type: none"> • Capture calls in real-time for infinite time, • Monitor adherence to protocol standards, report, and • Flexibility to add any protocol field to the summary view, filtering, and search features • Analyze with rich graphics, ladder diagrams, call trace • Complex Filtering and Search capabilities to record all or filtered traffic into a trace file • Consolidated interface allows access to all the important settings and auto-startup actions
As a Probe with Central Monitoring System - PacketScanWEB™	A central monitoring system for a comprehensive view of network performance. It features rich graphics, ladder diagrams, CDRs (Call Data Records), and user-defined Filter Views.
As a Single Point Analysis System	PacketScan™ has been enhanced to work with GL's VoiceBand Analyzer (VBA) and Call Data Records (CDR) applications to provide useful call detail records for further analysis using built-in tool in Excel® .
Packet Data Analysis	<ul style="list-style-type: none"> • RTP packet statistics for each direction of a call • A host of counters gives the user an instantaneous snapshot of the VoIP traffic on the network • Pictorial representation of the statistics including ladder diagrams for the calls of various protocols. • Ability to export PDA summary and detail reports of selected or all calls in PDF file format. • Ability to export completed calls summary report of PDA in CSV file format, and analyze the reports using custom Excel® addins.

Performance Metrics	<ul style="list-style-type: none"> • Signaling, audio, and video QoS parameters for each call • Minimum, maximum, and average Round Trip Delay (RTD) • Inband (DTMF & MF) events, RFC 2833 events, RTP/RTCP packet count and reports per direction
QoS Parameters	<ul style="list-style-type: none"> • E-model (G.107) based MOS/R-Factor scores • Media Delivery Index (Delay Factor: Media Loss Rate) for video calls • H.263, H.264 codec support • Jitter, Delay, and Gap for Audio and Video traffic
Triggers and Actions	Filter the captures based on any signaling parameters followed by a set of actions for the completed calls.
Traffic (Digits, Audio, Video, Fax) Handling	<ul style="list-style-type: none"> • Segregation of IP traffic, VoIP, and Fax calls • Extracts fax images in TIFF format for Fax calls • Audio capture/playback - Listen and Record RTP (Audio) streams • Record Video and Video QoS Statistics
SIP Registration Details	Registration statistics and trace messages depicted graphically.
Utilities	<ul style="list-style-type: none"> • Provides HDL File Conversion utility to convert ethereal format file (*.PCAP, *.CAP, and *.PCAPNG) to GL's file format (*.HDL) and vice-versa • Includes Excel® Addins to import CDRs into Excel® to analyze using Pivot Table, and Pivot Charts.

1.4 Pre-requisites

Package Contents

Verify if you have received the following as part of the GL product package:

- GL software installation CD containing PacketScan™ installation software
- Documentation (User's Manual, Quick Start Guide, Release Notes, Help)
- USB Hardware Dongle with required licenses

System Requirements

Following are the computer requirements for a computer equipped with the **PacketScan™** software.

- PC with Windows® XP, Vista, 7 (32-bit and 64-bit), or 8 (32-bit and 64-bit)
- Processor Minimum Requirements- P4 processor, or Dual Core processor; Recommended - Quad Core processor (i7 processor for high performance).
- RAM Minimum Requirements - 512 MB RAM; Recommended - 4 GB RAM

License Requirements for Optional Software

- **PKV100** – PacketScan™ Base License (includes SIP, Megaco, MGCP, Diameter, Skinny)
- **PKV105** – SIGTRAN Analyzer Software, requires PKV100
- **PKV103** – IP Based GSM and UMTS Analyzer, requires PKV100
- **PKV107** – LTE (Long Term Evolution) Analyzer, requires PKV100
- **PKV104** – FaxDDT38™ - Decodes Fax images in TIFF format from PCAP files
- **PCD103** - Optional Codec – AMR
- **PCD104** - Optional Codec - EVRC
- **PCD105** - Optional Codec – EVRC-B
- **PCD106** - Optional Codec – EVRC-C

1.5 VoIP Testing

Typically in the real world, a VoIP endpoint that supports SIP or H.323 (such as SIP phone or H.323 Phone) makes use of the SIP/H.323, SDP and RTP/RTCP components to build a complete communication end point. SIP/H.323 is used to setup and teardown calls, SDP is used to exchange media information and RTP is used to actually transport media (such as voice), between endpoints. PacketScan™ captures packets pertaining to all the three components there by keeping track of a complete VoIP call and providing user with tools to analyze any call in great detail. PacketScan™ non-intrusively captures the packets between the communicating entities, sieves the VoIP packets, segregates them into calls, collects statistics and even stores the traffic 'as-is' for later retrieval.

A SIP based VoIP network has several components that need to be tested. The network components that can be tested using the PacketScan™ are as depicted in the following figure.

SIP end points: PacketScan™ can non-intrusively capture traffic between SIP end points and keep track of SIP calls and the RTP traffic between them. It can be used to test the correct protocol behavior as well as Voice quality.

SIP servers: SIP network servers perform a variety of crucial functions. All the servers (Proxy, Redirect and Registrar) functionality can be tested using PacketScan™ for their adherence to the protocol standard.

Signaling Gateways: SIP networks must work with already existing networks like PSTN and also with other VoIP networks like H323, MGCP etc. The interoperation between these networks involves Signaling Gateways, the most important being the PSTN Signaling Gateway. These devices can be stressed using the PacketScan™, again mostly for protocol correctness and Voice Quality – post conversion between the various audio formats.

Media Gateways: Media Gateways are edge devices that convert RTP based media traffic to TDM based bearer traffic in the PSTN world and vice versa. The PacketScan™ can be used to test the voice quality on these devices.

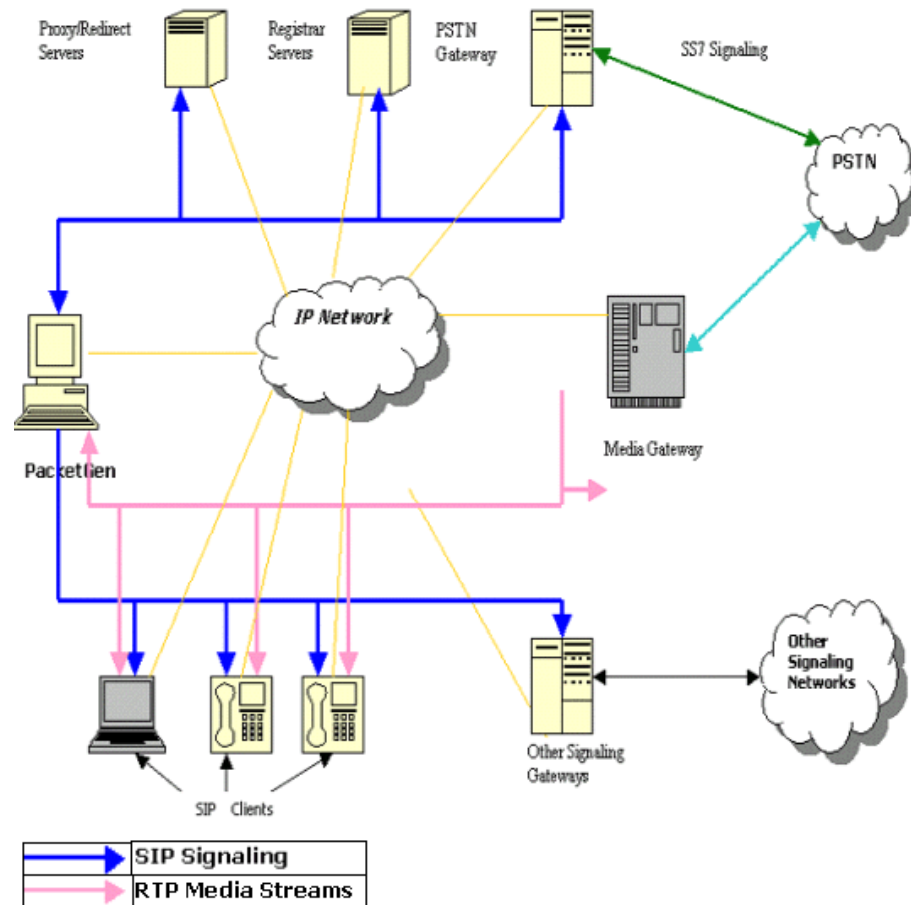


Figure 2: Testing networks components with PacketScan™

(Intentional Blank Page)

Section 2.0 Installation Instructions

2.1 Installation Procedure

The installation procedure for PacketScan™ is as follows:

- Dongle License Installation
- PacketScan™ Installation

2.2 Dongle License Installation

Hardware dongle containing the serial number and corresponding license is used to secure GL Communications software products. The PacketScan™ application requires the GL Dongle license and hardware be installed before installing PacketScan™. Click **setup.exe** in the dongle license installer directory to install the license. The dongle installs the license for the following applications as shown in the figure below:

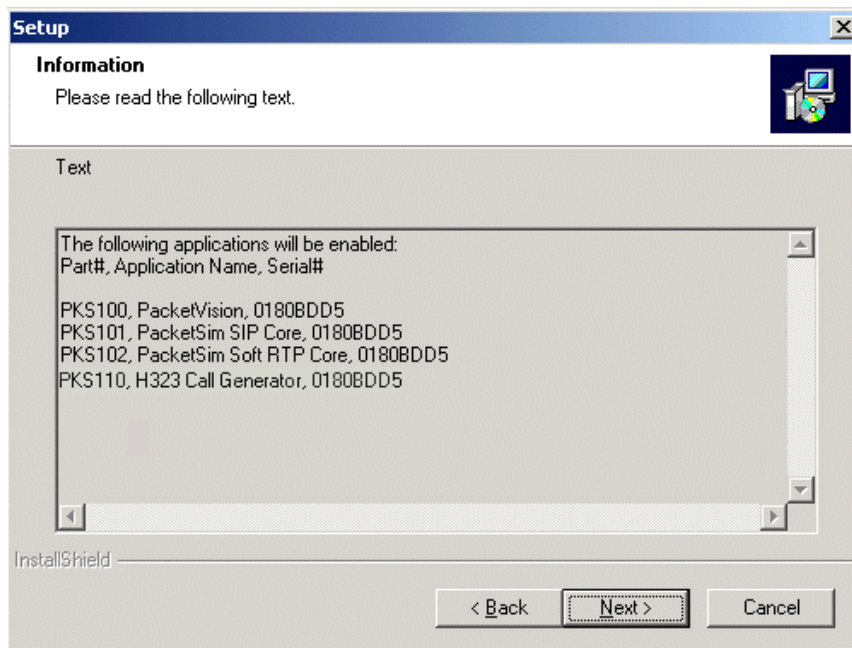


Figure 3: Dongle Installation

Click **Next** to begin copying of files on to the machine and click **Finish** to complete dongle installation.

2.3 PacketScan™ Installation

- 1) Click **setup.exe** (executable file) in the PacketScan™ installation disk. The following **InstallShield Wizard** appears.

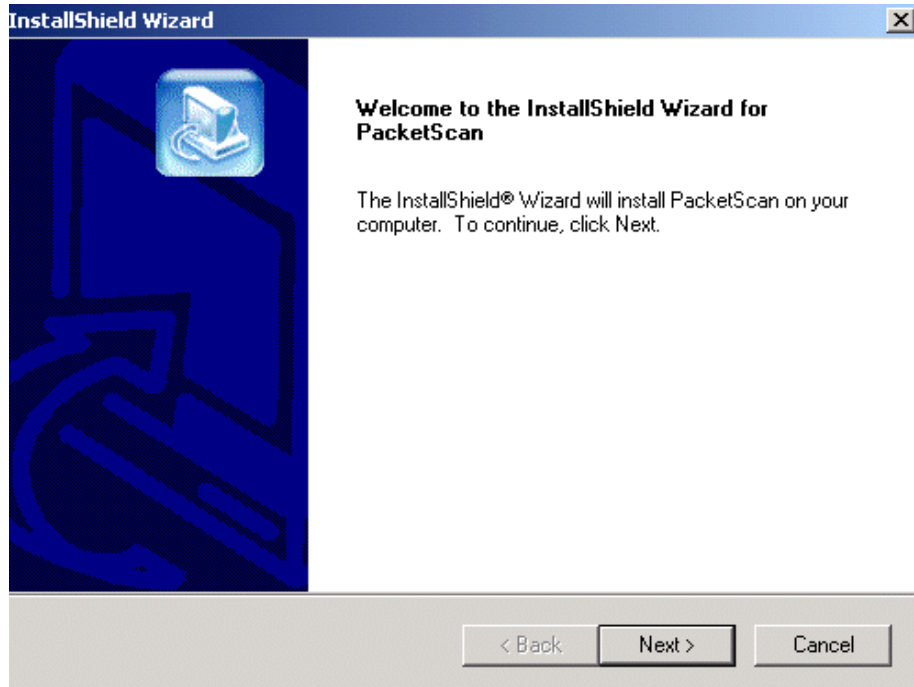


Figure 4: Welcome Screen

- 2) Click **Next** in the above wizard.
- 3) Select the destination folder to install (default folder is set to...\\Program Files\\GL Communications Inc\\PacketScan) shown in the following figure:

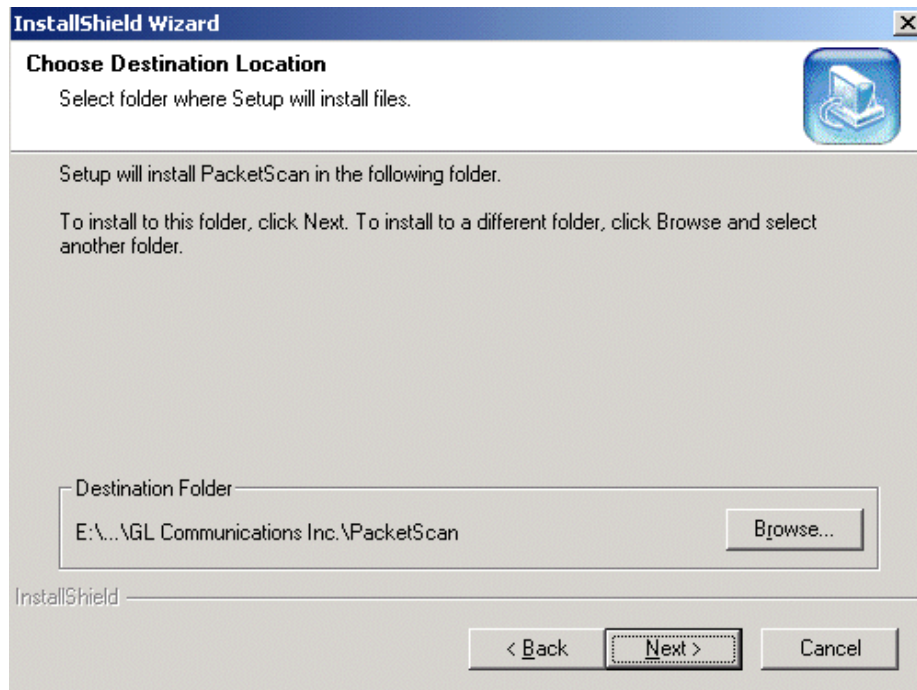


Figure 5: Choose Destination Location

- 4) Status of the installation process is as shown in the figure below.

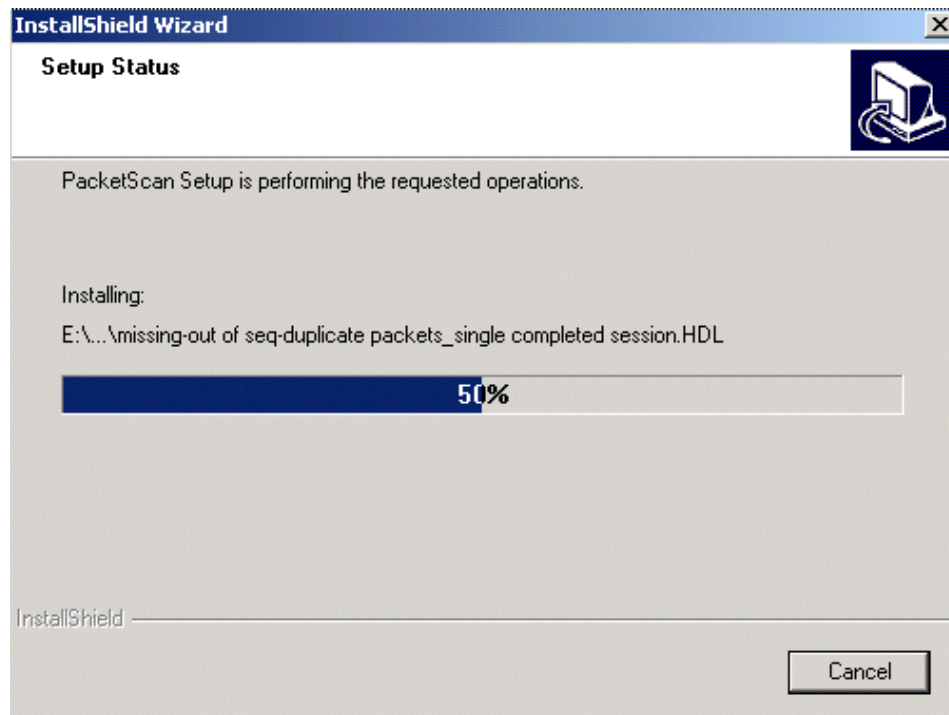


Figure 6: Setup Status

2.3.1 WinPcap Installation

WinPcap is a driver and library used for packet capture and network analysis for Win32 platforms. WinPcap functions allow packet capturing independent of the underlying network hardware and operating system. WinPcap must be installed to use PacketScan™ and is included as part of the PacketScan™ Installation.

- 1) If a previous version of WinPcap is installed the installation will remove it and install version 4.1.2. If this version is already installed, it will skip this step and continue on to completion. The WinPcap installation wizard appears as shown in the figures below:

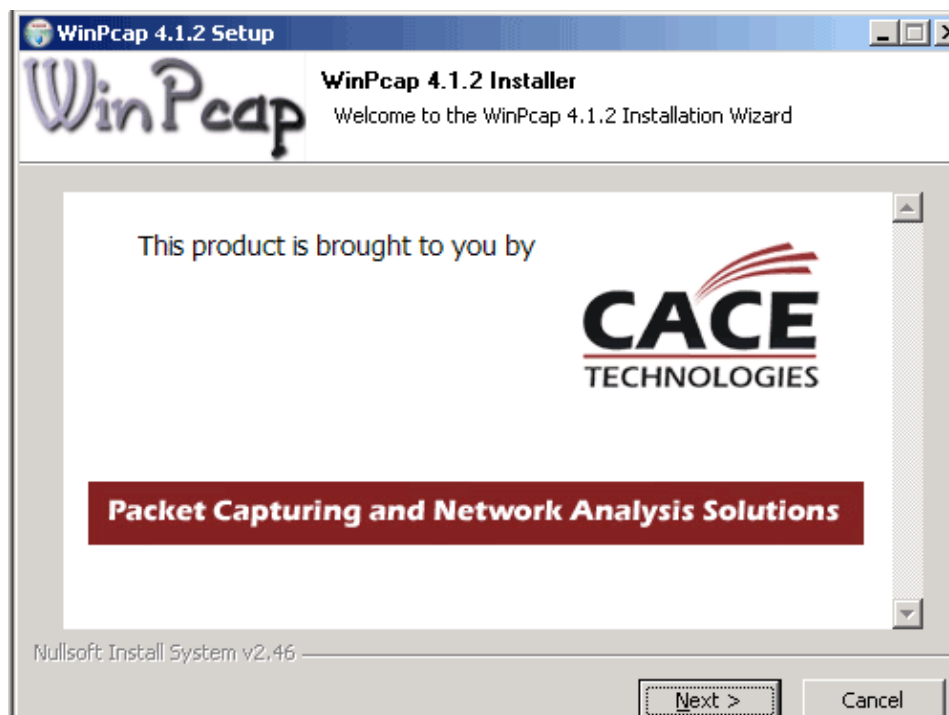


Figure 7: WinPcap Installation Wizard

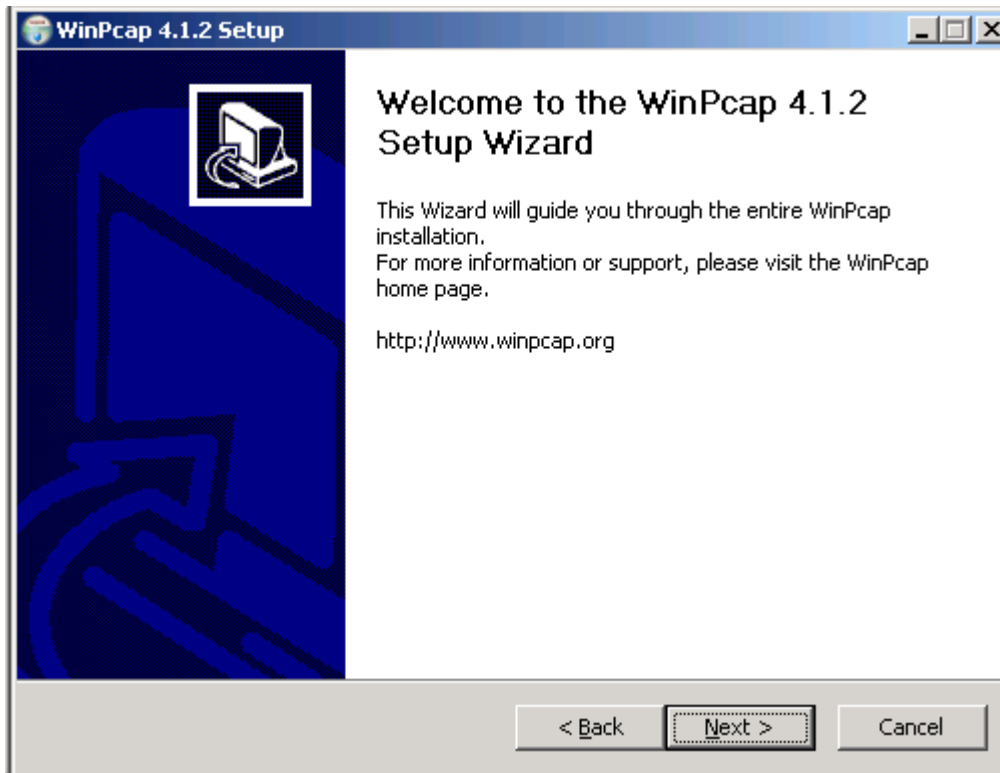


Figure 8: WinPcap Welcome Screen

2) Check the **License Agreement** for WinPcap as shown in the figure below:

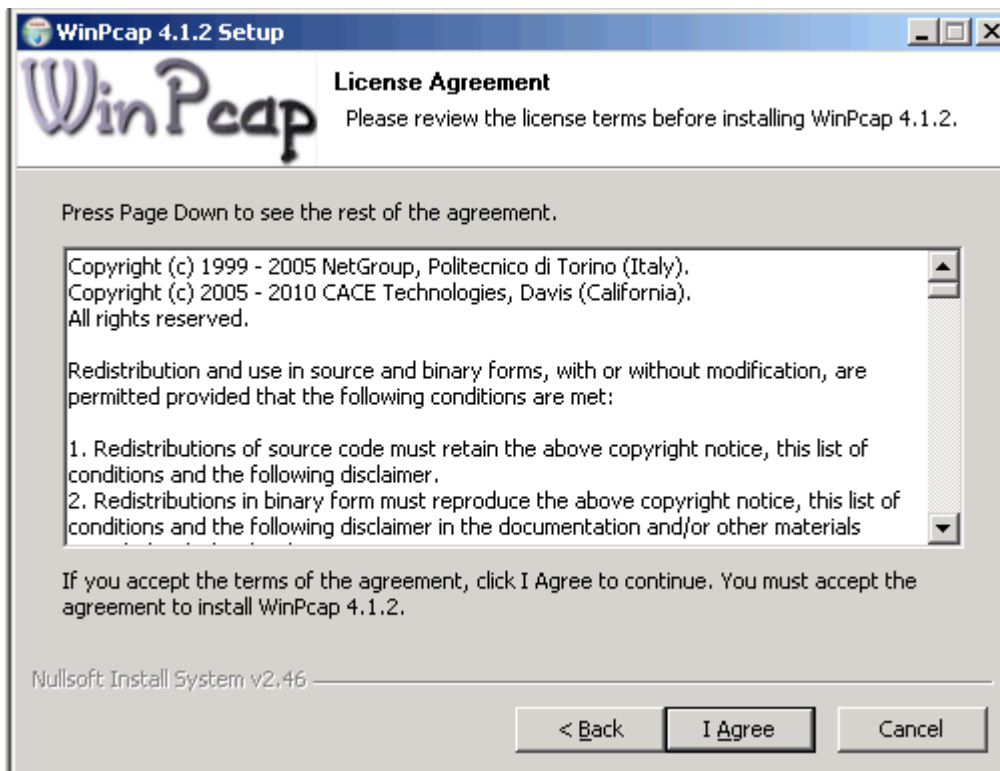


Figure 9: WinPcap License Agreement Screen

- 3) Select 'Automatically start the WinPcap driver at boot time' option and click 'Install' to install the software.

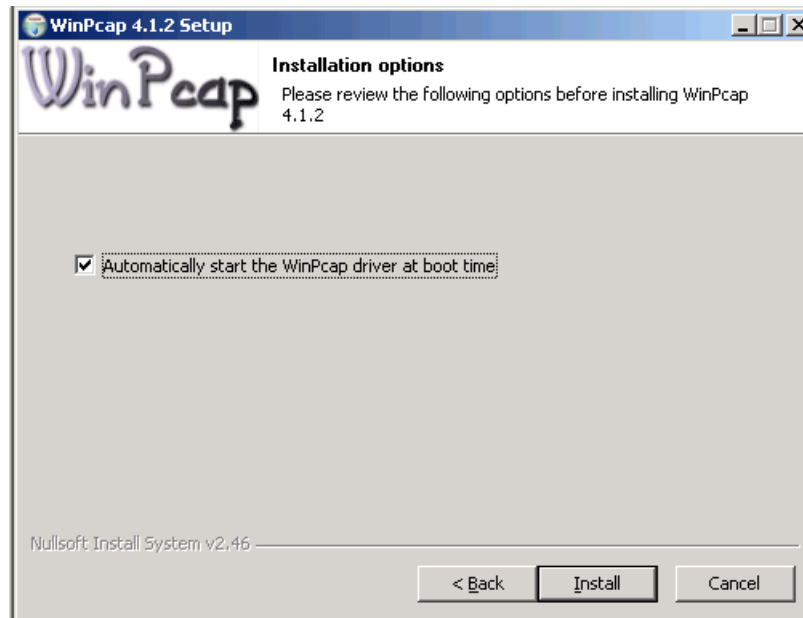


Figure 10: WinPcap Installation Wizard –Screen4

- 4) Click **Finish** to proceed with PacketScan™ installation process.

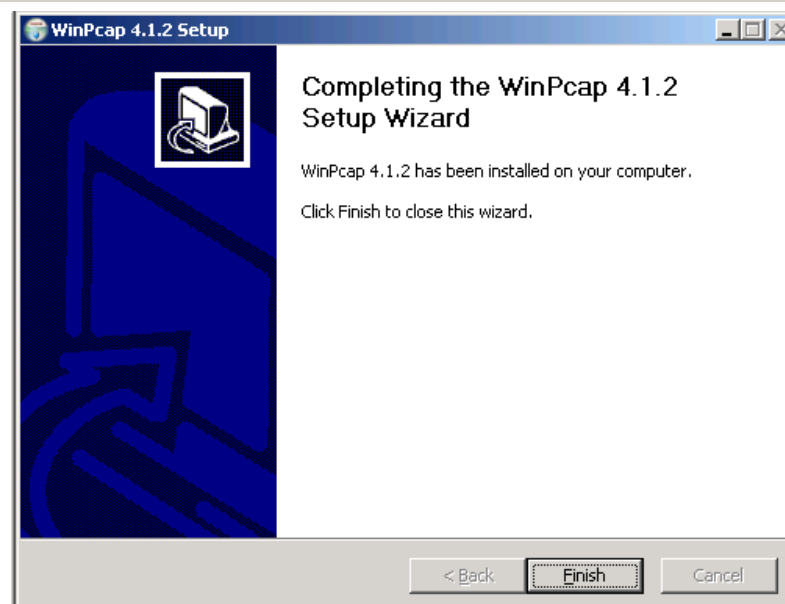
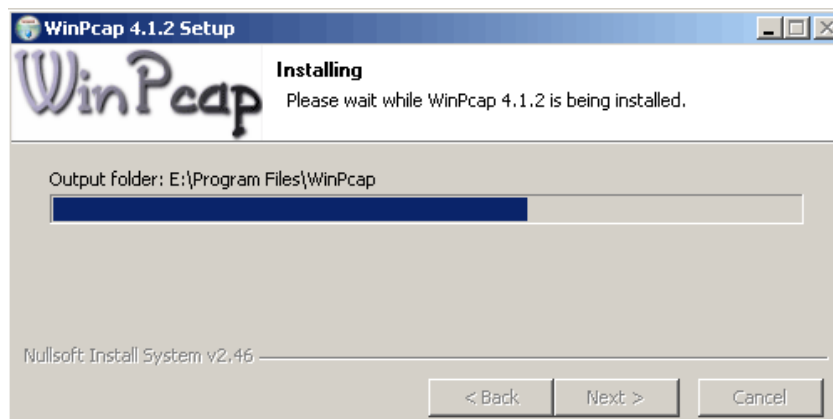


Figure 11: WinPCap Installation Completion Wizard

- 5) Microsoft Visual C++ 2005 Redistributable installation status

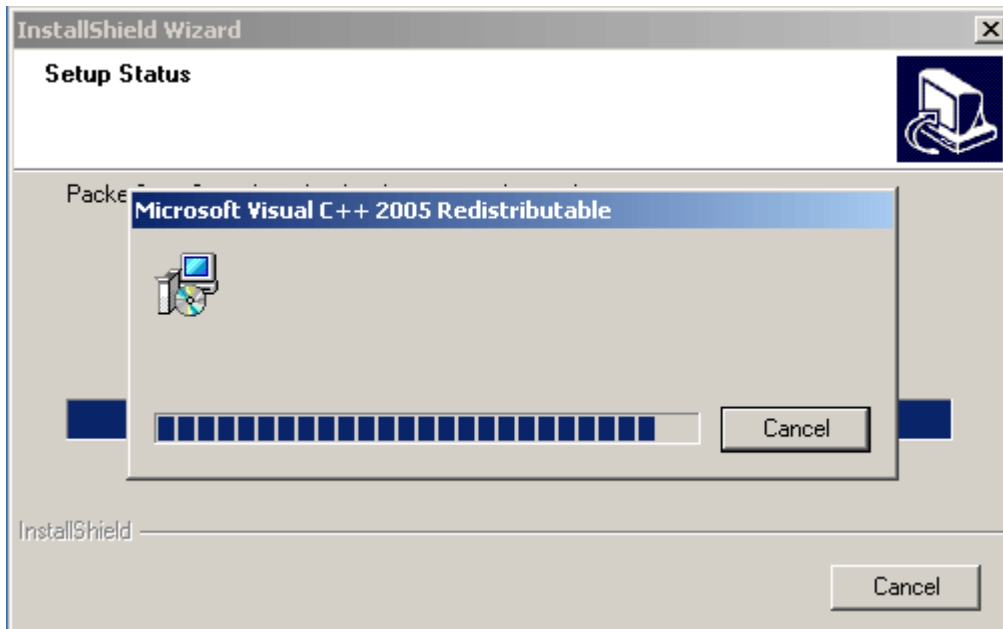


Figure 12: Microsoft Visual C++ 2005 Redistributable

- 6) Click **Finish** to complete the installation of software.

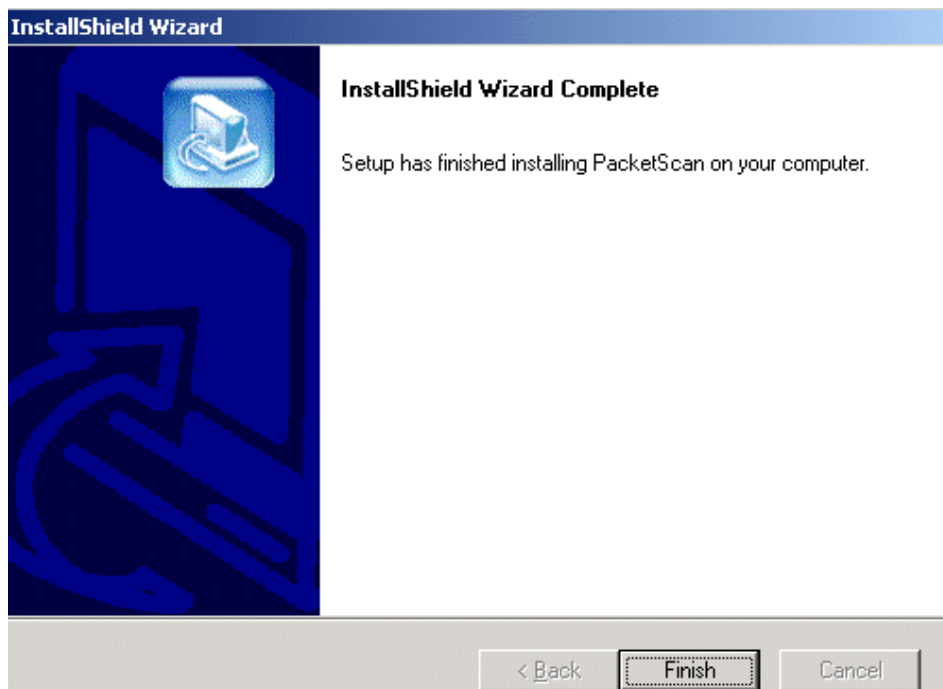


Figure 13: PacketScan™ Installation Complete

™

Section 3.0 Getting Started with PacketScan

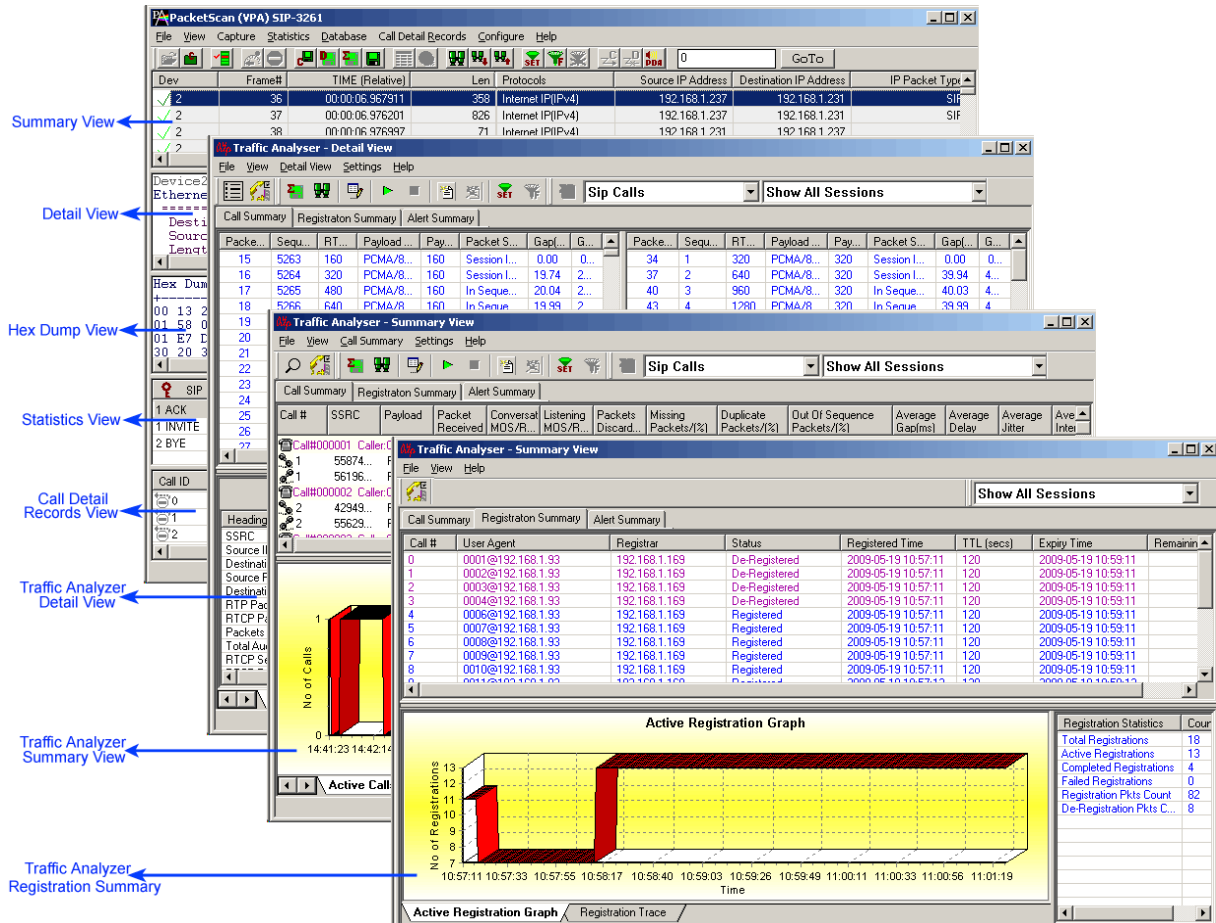


Figure 14: User Interface

PacketScan™ is comprised of following two GUIs –

Real-time Analysis

- Default panes – Summary, Detail, and Hex dump of the frame data views
- Optional panes – Statistics and Call Detail Views

Packet Data Analysis

- Summary View (Call Quality Matrix) displays call information in graphical format
- RTP diagnostic view displays call information in tabular format
- Registration Summary displays the SIP registration information in tabular as well as graphical format

The user interface of Real-time analysis GUI comprises of a main menu, toolbar and different views, which includes Summary View at the top, followed by the Detail, Hex Dump, Statistics and Call Detail View at the bottom as shown in the figure above.

The main menu tool bar comprises of File, View, Capture, Statistics, Database, Call Detail Records, Configure, and Help menu. The main menu and the tool bar are used to select an operation to perform. The status fields at the bottom of the window display miscellaneous status information. Most of the operations can be performed either using the main menu or the corresponding tool button.

The features under these menus are explained in detail later, in this document.

The analyzer opens with Summary, Detail and Hex Dump as default panes. Statistics and Call Detail are optional panes. The users have the options to set the desired views using **Views > Define Views**. The splitter separating the Summary, Detail and Hex dump Views can be adjusted according to user preferences. The Summary View columns can be resized and reordered.

- Summary View displays various columns such as, Dev#, Frame #, Time, LEN, Error, Packet Type, TCP/IP/UDP Source and Destination Port address, DHCP Message Type, HTTP and FTP Messages, SIP Method, SIP From and To, SIP Call ID and Cseq, RTCP Packet Type, and more.
- User selects a frame in the Summary View to get the detail protocol field information in the **Detail View**.
- Raw data for the selected Summary View frame is displayed in the **Hex-dump View** in HEX and ASCII format.
- Call Detail View displays Call ID, Call status, Source Address, Destination Address, Call Start Date and Time, Call duration, Device number (Dev No), SIP CallID, Release Cause, CRV, Conference ID, Call Type, Call Identifier, SrcIPAddr, and DestIPAddr.
- Statistics View displays statistics based on frame count, byte count, frames/sec, bytes/sec etc for the entire capture data.

At least one of the following views must be defined: Summary, Statistics, or Call Detail Record. The Detail and Hex Dump views can be displayed only when the Summary View is displayed.

In addition to the above, PacketScan™ includes the following interfaces (shown in figure) under Packet Data Analysis (PDA):

- **Summary View (Call Quality Matrix)** – This interface displays complete summary of SIP/H323/Megaco call information in graphical format in each direction. It includes statistical counts and graphical views to provide a complete analysis of the captured data.
- **Detail View (RTP Diagnostic View)** – This interface displays the entire call information (RTP sessions) in tabular format. Vital aspects of the RTP frame needed for close analysis are included in this table.
- **Registration Summary** – This interface displays the SIP registration information such as user agent, registrar, registered time, status, and more in a tabular format for each user agent. Also displays the active graph of the entire SIP registration and provides the trace display of each SIP registration.

Section 4.0 Performing Analysis using PacketScan™ – an Overview

4.1 Performing Real-time Analysis

The real-time analysis is used to capture data on the selected Ethernet board simultaneously during transmission. Follow the steps below to perform the real-time analysis:

Protocol/Decode Standard Selection

- 1) PacketScan™ supports four protocols SIP-3261, Megaco3525, Megaco3015, and H323. Select one of the decoding standards that should be used to parse and display information in VPA using **Protocol Standard Selection** under the **Configure-Protocol and GUI** menu. For further details refer to section [Protocol Standard Selection](#).

Capture Settings

- 2) The captured data is by default stored in a temporary file. Use Setting Capture Options under **Configure > Protocol and GUI** menu to specify a different file on which the transmission should be captured. This option also allows users to set the required file size, frame count, time limit and the path settings as per the requirements. The capturing settings are saved in the Windows registry when the user exits the application and does not require the users to enter them each time the application is started. For further details refer to section [Setting Capturing Options](#).
- 3) Select the required Ethernet boards using **Stream Interface Selection** option under the **Configure – Capture Options** menu to capture the data received on the selected boards. For more details on setting the Ethernet boards, refer to section [Stream / Interface Selection](#).
- 4) Additionally, the **Periodic Trace Saving Options** under **Configure – Protocol and GUI** menu can be used to save the capturing frames in the required format such as trace files with user-defined prefixes, user-specified directory, creating new trace files after a specified limit has reached, restrict or recycle after specified number of captured trace files. Select **Enable Periodic Saving** options before setting the periodic file saving specifications. For further details refer to section [Periodic Trace Saving Options](#).
- 5) To analyze only particular frames of interest, user can set real-time capture filter options using **Capture Filter** option under **Configure – Capture Options** menu. Filtering options can be set for layers such as MAC, IP, IPV6, TCP, UDP, SIP, RTP, SCTP, MEGACO, MGCP, and H.323 layer. For further details on this refer to section [Setting Capture Filter](#).
- 6) In addition, the filtering criteria may also be set after the completion of real-time analysis or during offline analysis using the **Filtering Criteria** option under the **Configure-> Protocol and GUI** menu. For further details on this refer to section [View Filtering Criteria](#).

Start/Pause/Stop Real-time Analysis

- 7) Start the real-time analysis using the Start/Pause menu options available under the file menu. For further details on this refer to section [Start Real-time](#) and [Stop \(Pause\)](#).
- 8) Users can save the current trace with a new file name using the option Save As and Close or save specific **Frames/Packets** in an existing file by overwriting it or append to an existing file. For further details refer to section [Save As and Close](#) and [Save As](#).
- 9) The captured information in detail and Summary View may also be exported to ASCII files for subsequent import into a database or spreadsheet. Follow the steps explained in [Export Details](#) and [Export Summary](#).

4.2 Performing Offline Analysis

An off-line analysis is equivalent to capturing a file in pre-defined channels, capture settings and decode standards. Here the captured file is opened using off-line option available under the File menu. For further details on this refer to section [Open a Trace for Off-line Analysis](#).

4.3 Packet Data Analysis (PDA)

Packet Data Analysis feature may be used for detail analysis of each session either during real-time (session is active) or during offline analysis (session is completed). For more details on this feature refer to sections [Packet Data Analysis – Traffic Analyzer Summary View](#), [Packet Data Analysis – Traffic Analyzer Detail View](#), and [Packet Data Analysis – Registration Summary](#).

(Intentional Blank Page)


Section 5.0 File Menu Options

5.1 Start Real-time


Note:

This feature is applicable to real time analyzer only.

Users can capture and analyze frames in real-time and record all or filtered traffic into a trace file. The recorded trace file can then be analyzed offline and exported to ASCII file, or printed. Performing any of the following steps can start the real-time analysis:

- Select **File > Start Real-time** as shown in the figure below
- Check **Start Real-time tracing** option provided under **Configure > Startup Options**, and then click Execute (For more details refer to [Startup Options](#)), Or
- Click **Start Real-time**  icon from the toolbar.

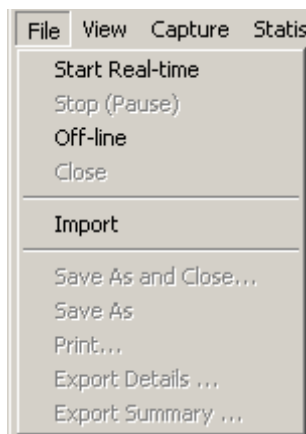


Figure 15: Starting Real-time Analysis

After you click the **Start Real-time** button, a warning message for overwriting the temporary trace file is displayed. If you want to overwrite click **Yes**, else, click **No** and save it as a new file in the desired location. This new file replaces the default specified in the capturing options dialog.

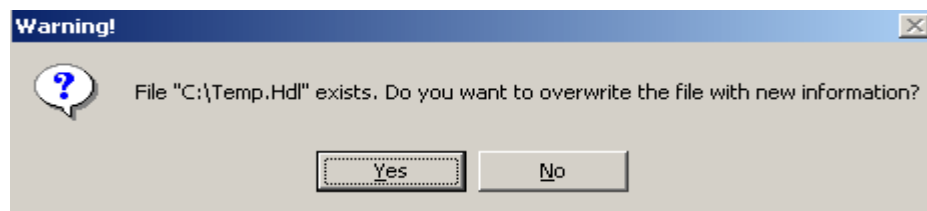



Figure 16: Saving the trace file

5.2 Stop (Pause)


Note:

This feature is applicable to real time analyzer only.


To suspend real-time capturing, perform any of the following steps given below:

- Select **File > Stop (Pause)** as shown in the figure below, Or
- Click **Stop**  from the toolbar

5.3 Open a Trace for Off-line Analysis

Off-line analyses are equivalent to transmitting/capturing a file in pre-defined channels and decode standards. During off-line analysis the users can analyze the pre-captured *.HDL files.

To open a captured trace file for offline analysis, perform any of the following steps given below:

- Select **File > Off-line** menu item or
- Click **Offline from a file**  from the toolbar

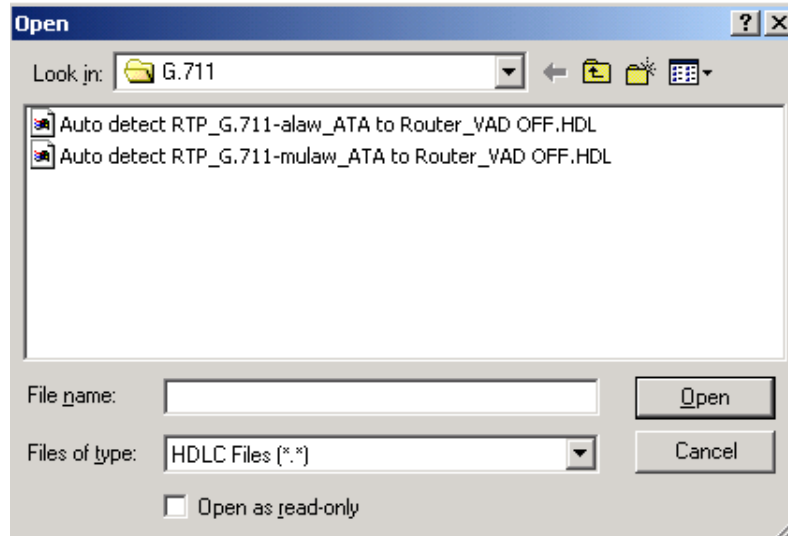



Figure 17: Open a Trace from a File for Off-line Analysis

5.4 Close Trace

To close the trace file opened for analysis, perform any of the following steps given below:

- Select **File > Close** as shown in the figure or
- Click **Close trace**  from the toolbar

5.5 Import

Import option invokes 'HDL File Conversion Utility'. It converts *.pcap or *.cap files into *.hdl file and it will open the converted *.hdl file in the PacketScan™ Analyzer.

To convert the pcap or cap files into hdl file, do the following:

- 1) Select **File > Import**, This displays HDL File Conversion Utility as shown in the figure below:

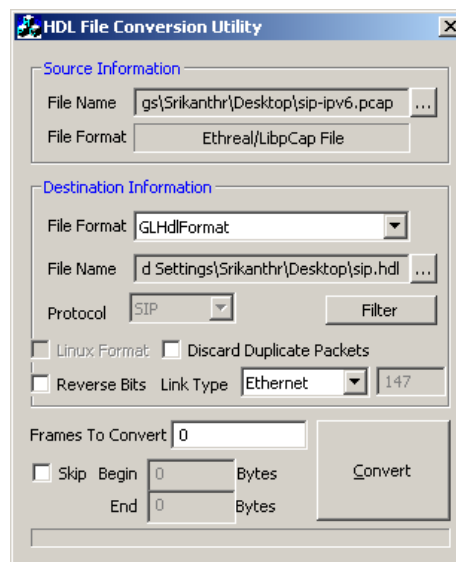


Figure 18: HDL File Conversion Utility

- 2) Browse and select the *.pcap or *.cap file from the Source Information
- 3) Select the File Format as GLHDFormat


- 4) Choose the destination path from the Destination Information to save the converted *.hdl file
- 5) Click Convert. It converts *.pcap file into *.hdl file and opens the converted file in the PacketScan Analyzer.

**Note:**

User can also execute HDL File Conversion utility from the PacketScan installation folder. For more information on HDL File Conversion Utility refer to the section [HDL File Conversion Utility](#)

5.6 Save As and Close

To save the current trace with a new file name and close the trace:

- Select **File > Save As and Close** menu item or
- Click **Save Trace to a Different File Name** and Close  from the toolbar

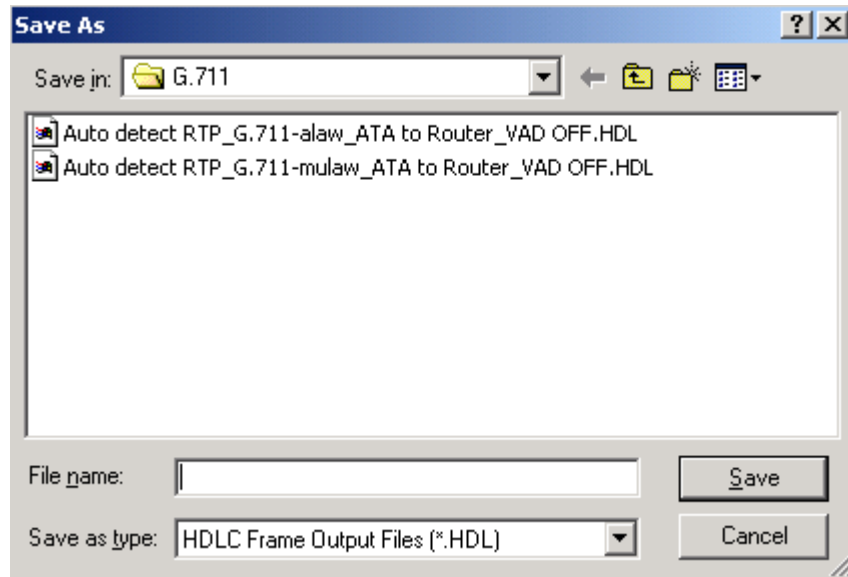


Figure 19: Save Trace as File Name and Close

This feature is usually used to make sure that trace is saved in a different file than temporary trace file and will not be overwritten by accident.

5.7 Save As

To save specific **Frames/Packets** in a new file or to append to an existing file, perform any of the following steps given below:

- Click **File > Save As** Or
- Click **Save As**  from the tool bar

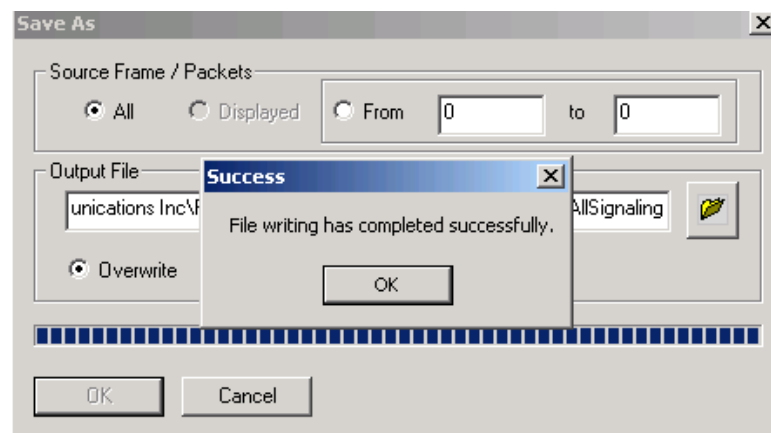


Figure 20: Save As

- Select **All** to save all the captured frames

- Select **From** to save all the frames whose frame length ranges within the specified values in 'min' to 'max' text boxes as shown in the above figure
- Select **Overwrite** to overwrite the existing *.HDL files in the directory with the new captured frames
- Select **Append** to append the frames/packets to the already existing *.HDL files in the directory.

Trace file remains open after the "**Save As**" operation is completed. Close the trace file and verify if the file has been successfully saved by opening the saved *.HDL file in offline mode.

5.8 Export Details

To export the Detail View information of frames to an ASCII file, perform any of the following steps given below:

- Click **File > Export Details** Or
- Click **Export Details**  from the tool bar

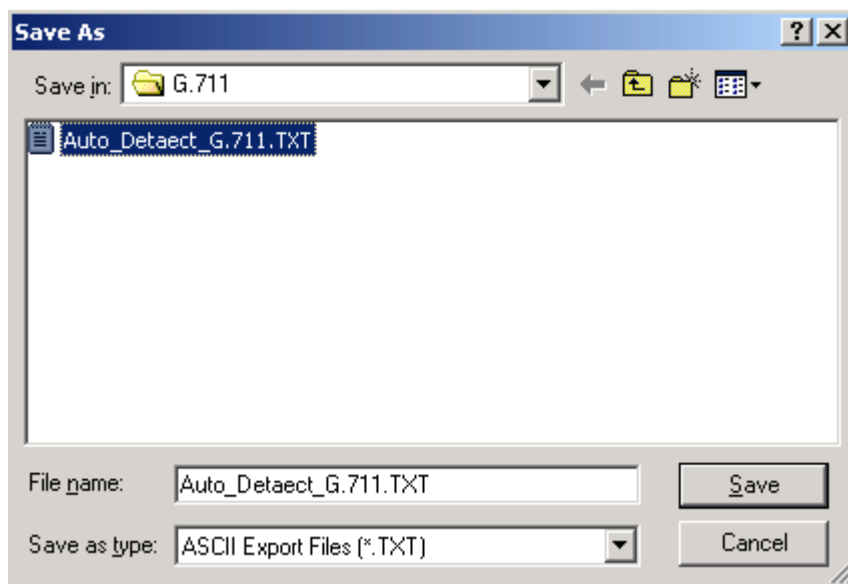


Figure 21: Exporting Trace to an ASCII File




Note:

In order to export details you must have Summary, Detail, and Hex Views

5.9 Export Summary

To export the summary information to a comma separated values (CSV) format, perform any of the following steps given below:

- Click **File > Export Summary** Or
- Click **Export Summary to a Comma Delimited File**  from the tool bar

Select the **Columns to Export** and save the export summary as text file. Select Export Headers to export a header line with column names preceding the summary data rows.

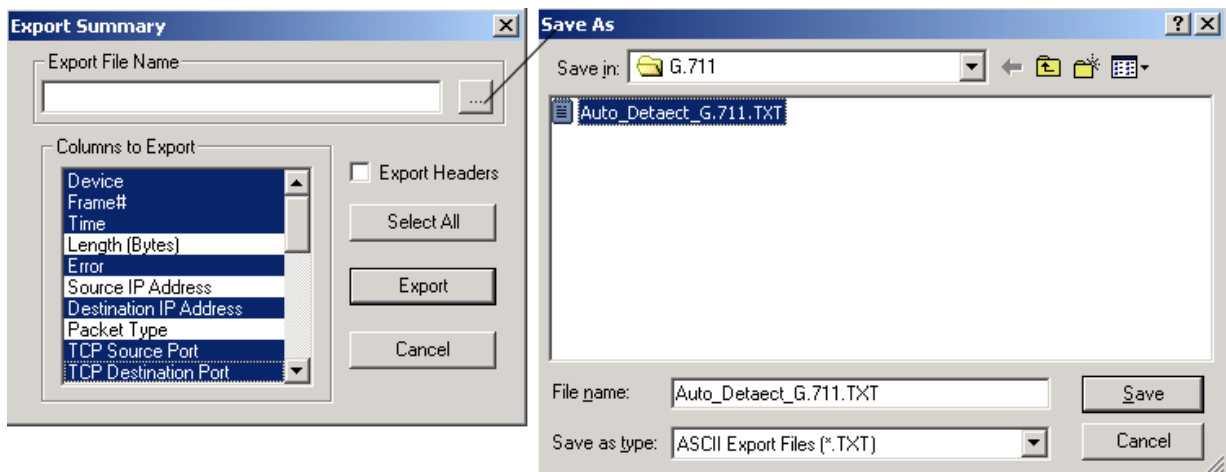


Figure 22: Exporting Summary to an ASCII File

(Intentional Blank Page)

Section 6.0 Display Options

The View menu includes:

- Define Views to Display – Summary View; Right-click options in Summary View; Detail View; Hex Dump View; Statistics View; Call Detail Records View
- Protocol Standard
- User/Network Side Specification
- Time Format
- Latest Frame
- Set filtering criteria
- Activate or Deactivate filter
- Search criteria
- Next, Prev
- Displays trace file name
- Default Summary column
- Invoke Packet Data Analysis

6.1 Define Views to Display

Select **View > Define Views** to select Summary, Detail, Hex-Dump, Statistics, and/or Call Detail View as shown in the figure below and click 'OK' to view the details.

**Note:**

Summary View should be selected to view the Detail and /or Hex Dump Views.

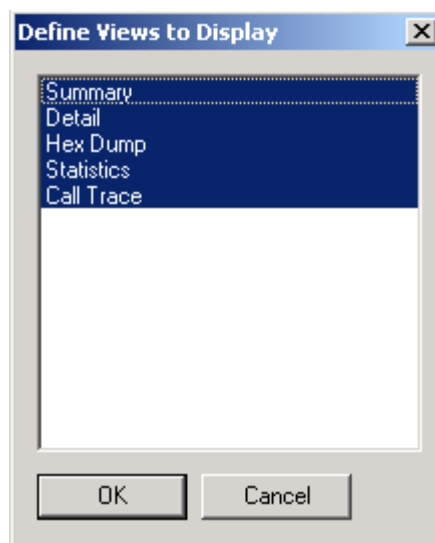


Figure 23: Define Views to Display

**Note:**

Summary View cannot be deselected.

6.2 Summary View

The Summary View displays various information such as Frame Number, Time, Length, Message Types, IP source and destination address and so on. Any field from the protocol headers can be added to summary view, i.e., summary fields are completely user-configurable. For more information refer [Define Summary Columns](#).

6.2.1 Setting a Relative Time

Select a particular frame in Summary View and right click to select **Set Relative Time**.

The relative capture time stamp of all other frames will be calculated relative to the selected frame as shown in the figure below. The selected frame becomes a baseline and the relative time above the selected frame shows that frames are captured before this frame. Also the relative time below this baseline shows that the frames are captured after this frame.

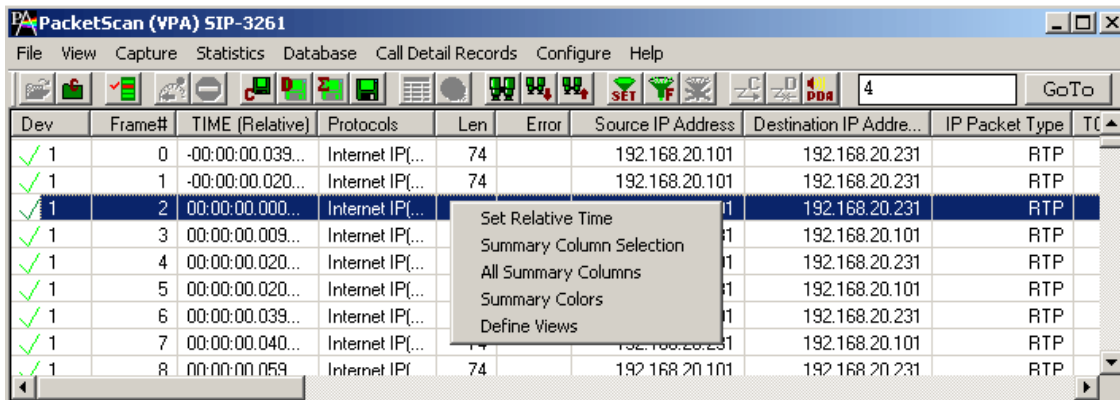



Figure 24: Set Relative Time

6.2.2 Summary Column Selection

Select a particular frame in Summary View and right-click to select **Summary Column Selection** or click on the  Select summary columns to display button from **Configure > Protocol and GUI Options** to open the **Analyzer GUI and Protocol Configuration** window as shown in the figure below.

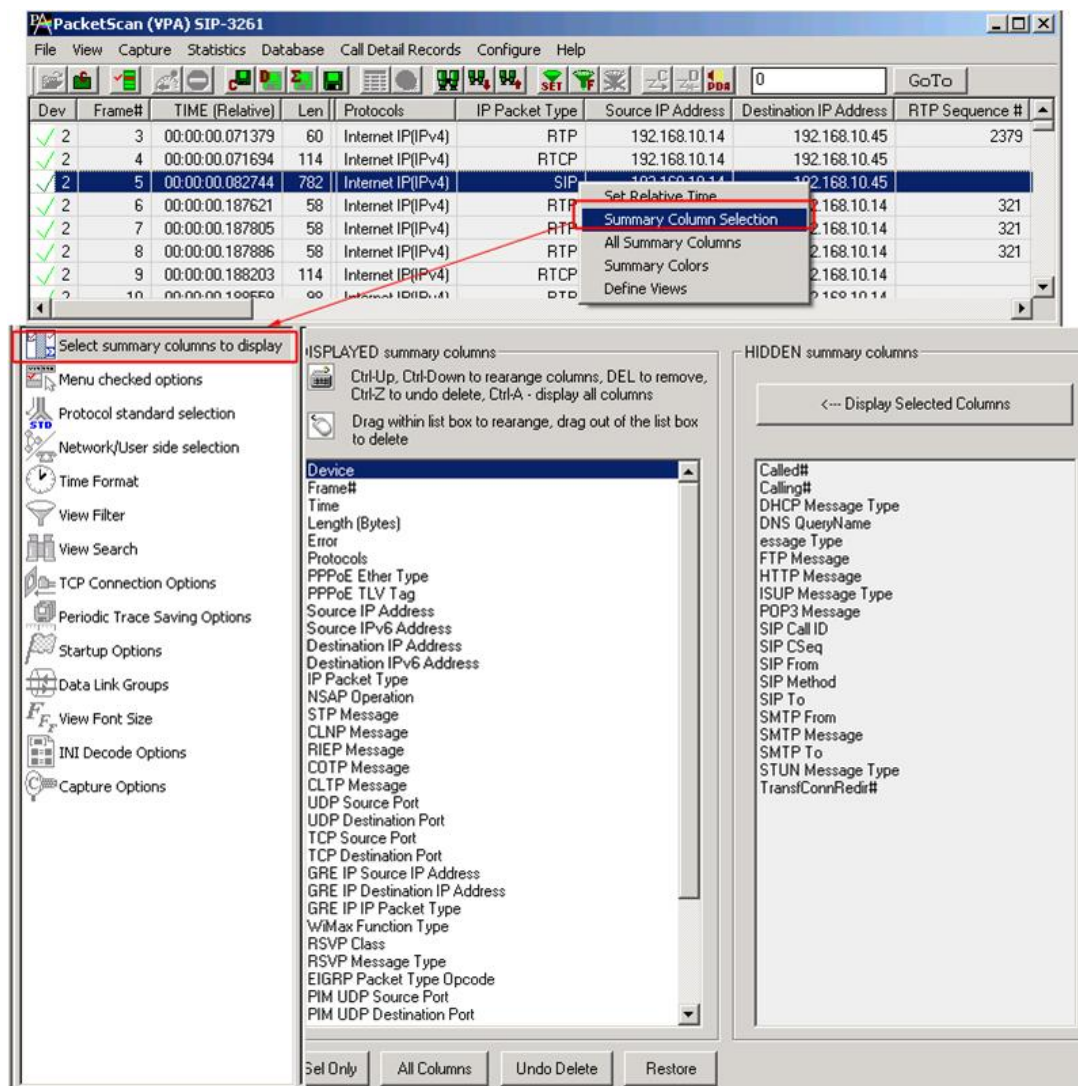


Figure 25: Select Columns to Display

This window is used to select the columns that are to be displayed in the Summary View.

Select the desired columns to be displayed from **DISPLAYED summary columns** pane to display the columns in the Summary View.

- Click **All Columns** to display all the columns in the Summary View.
- Click **Sel Only** to display a particular column in the Summary View.
- Click and drag columns up and down in the "DISPLAYED" summary column list to reorder them.
- Click and drag the columns to the right side of the pane to delete them or use the keyboard "Delete" key.
- Click **Undo Delete** or **Restore** to get the columns back to the left pane.
- Click **Display Selected Columns** from the HIDDEN summary columns pane to view the columns, which are hidden.

In addition to column selection, this window allows users to reorder the columns appearance that is displayed in the Summary View, which is explained in the section below.

6.2.3 Column Resizing and Reordering

The users can resize and/or reorder the columns in Summary View. From [Select Columns to Display](#) dialog in **Configure > Protocol and GUI Options**, click and drag the columns to different positions as shown in the figure below. The figure shows the **Frame #** and **IP Packet Type** columns are reordered and **TIME (Relative)** and **Len** columns are resized.

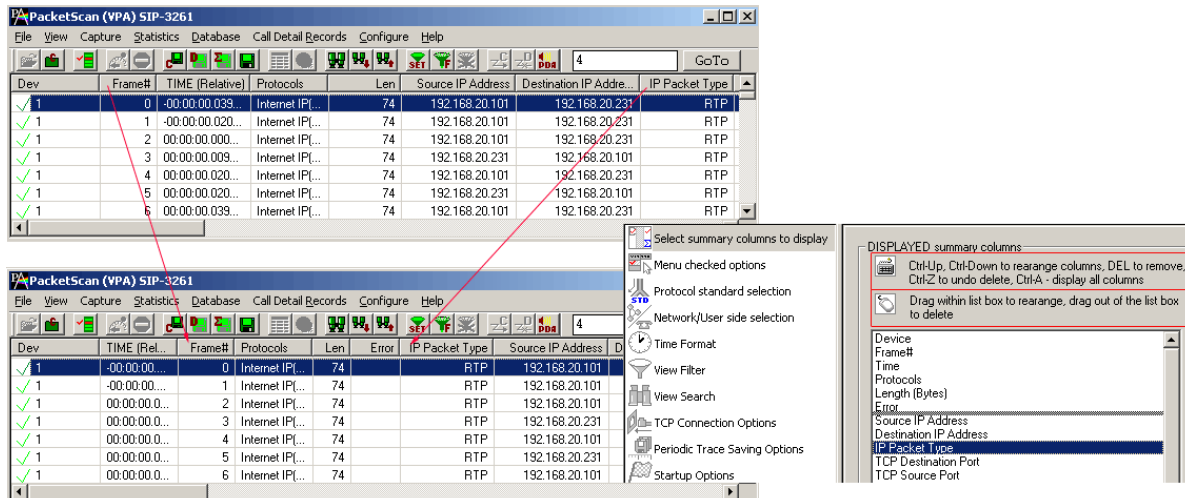


Figure 26: Column Resizing and Reordering

In addition to reordering, the Summary columns can be resized. Click and drag the Summary column headers to resize them.

6.2.4 Repositioning Summary View

Enter a new current frame number to position at the top of the Summary View and click **GoTo** button as shown in the figure below:

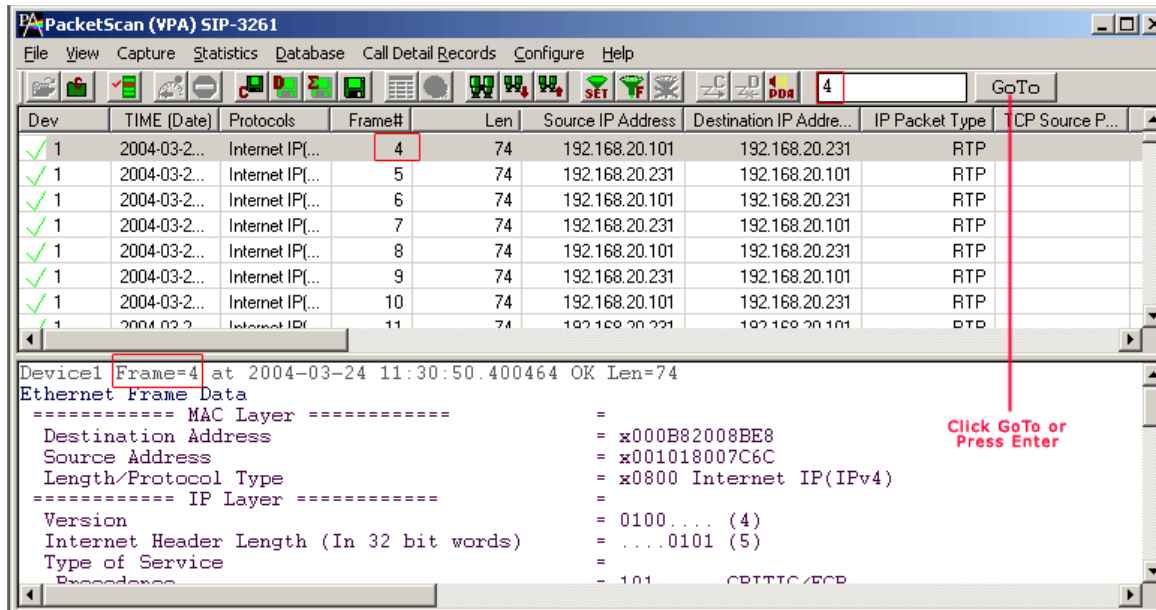


Figure 27: Repositioning the Summary View

This operation may be executed even during the real-time capturing. If a filter is active the frame number refers to displayed (filtered out) frames.

6.2.5 Summary Colors

Select a frame in Summary View and right-click to select **Summary Colors** as shown in the figure below. Summary View is shown in different colors based on the selected columns.

For example, select **Len** option and click **Ok**.

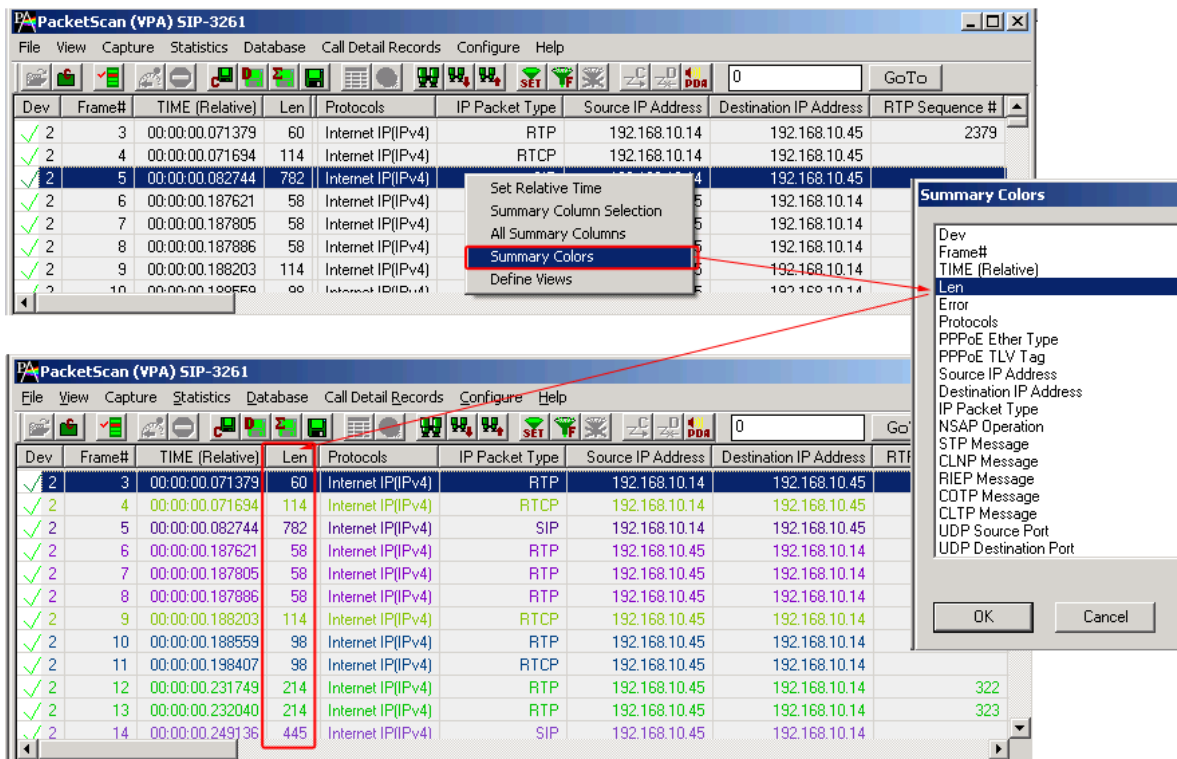


Figure 28: Set Summary Colors

Observe that different color is set based on the **Len** column, in other words, the frames having the same length values will have a unique color set for it as shown in the figure above.

6.2.6 Define Views

For detail information on this, refer to section [Define Views to Display](#).

6.3 Detail View (Selecting Individual Frame)

Click to highlight a frame in Summary View to display the frame-specific details in the **Detail View**.

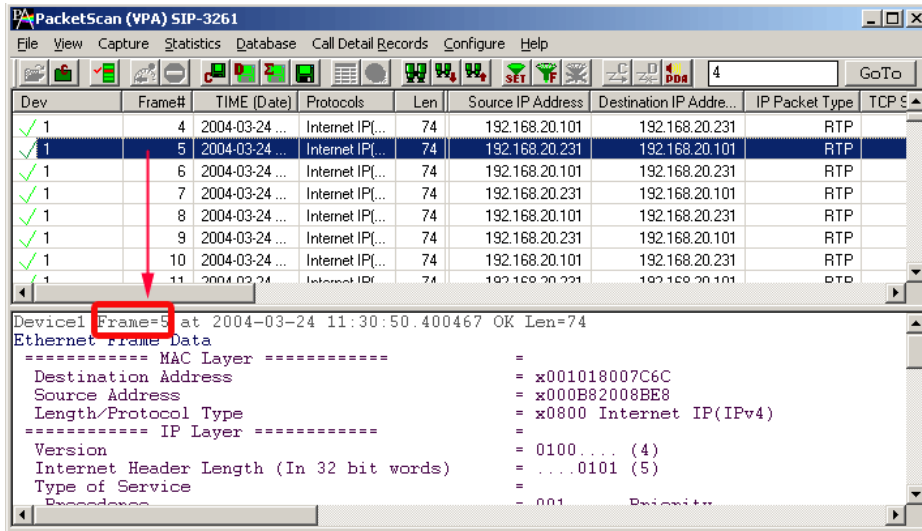


Figure 29: Selecting Individual Frame

The Detail View displays frame information in the following sequence

- Frame Summary Information
- MAC layer details
- IP / IPv6 Layer details
- UDP or TCP layer details
- Higher Layer Information includes –
 - SIP Layer information
 - MEGACO layer information
 - H.323 Layer Information
 - SMPP Layer Information
 - RTP Layer Information
 - RTCP Layer Information
 - MGCP Layer Information and other supported protocols

6.3.1 Detail View – SIP Capture

The detail decode view of SIP call displays the following

- MAC layer
- IPV6 (or IPV4) layer
- UDP Layer
- SIP 3261

```

Device2 Frame=30 at 17:57:26.956270 OK Len=889
Ethernet Frame Data
===== MAC Layer =====
Destination Address      = x001CC0A3F414
Source Address          = x0013208E1369
Length/Protocol Type    = x86DD IPv6
===== IPv6 Layer =====
Protocol Version        = 0110.... (6)
Traffic Class           = 0 (...0000 0000....)
Flow Label              = 0 (...0000 00000000 00000000)
Payload Length          = 835 (x0343)
Next Header             = 00010001 User Datagram Protocol (UDP)
Hop Limit               = 128 (x80)
Source Address          = 2001:ff01:21fd:fd0d:5606:3df0:2bfb:b056
Destination Address     = 0021:0918:0012:0001:0000:0000:0000:0054
===== UDP Layer =====
Source Port             = 5060 (x13C4)
Destination Port        = 5060 (x13C4)
Length (Header + Data)  = 835 (x0343)
Checksum                = 42923 (xA7AB)
===== Sip3261 Layer =====
HDR                     = INVITE sip:0001@[21:918:12:1::54] SIP/2.0
HDR                     = Via: SIP/2.0/UDP [2001:ff01:21fd:fd0d:5606:3df0:2bfb:b056]:5060;branch=z9hGz6
HDR                     = From: sip:0001@[2001:ff01:21fd:fd0d:5606:3df0:2bfb:b056];tag=FromTag_413786
HDR                     = To: sip:0001@[21:918:12:1::54]
HDR                     = Call-ID: ProtScriptId_4137846152-4497
HDR                     = CSeq: 1 INVITE
HDR                     = Max-Forwards: 70
HDR                     = Contact: sip:0001@[2001:ff01:21fd:fd0d:5606:3df0:2bfb:b056]
HDR                     = Content-Length: 300
HDR                     = Allow: INVITE,BYE,CANCEL,ACK,INFO,PRACK,OPTIONS,SUBSCRIBE,NOTIFY,REGISTER,UPDATE
HDR                     = Content-Type: application/sdp
BODY                     = v=0
BODY                     = o=0001 33852938 33852938 IN IP6 2001:ff01:21fd:fd0d:5606:3df0:2bfb:b056
BODY                     = s=-
BODY                     = c=IN IP6 2001:ff01:21fd:fd0d:5606:3df0:2bfb:b056
BODY                     = t=0 0

```

Figure 30: Detail View of SIP

6.3.2 Detail View – Megaco Capture

The detail decode view of Megaco call displays the following layers:

- MAC Layer
- IP Layer
- UDP Layer
- MEGACO Layer

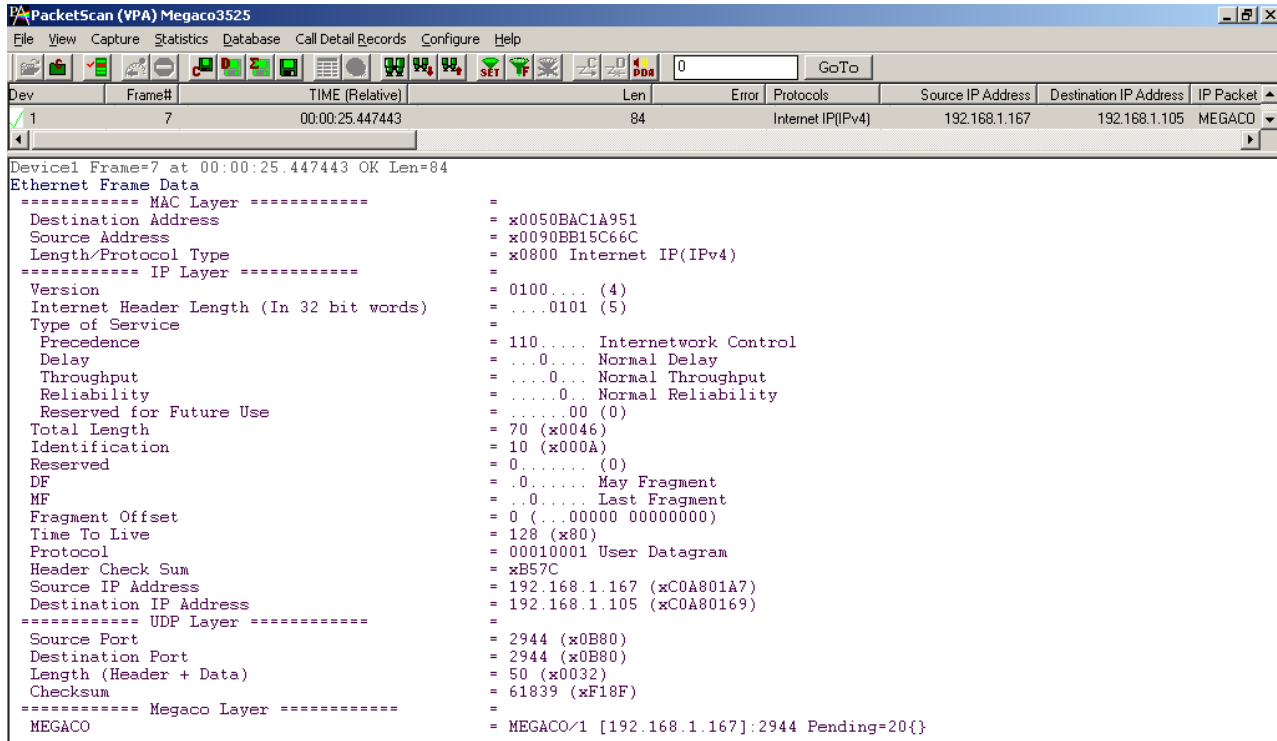


Figure 31: Detail View of MEGACO

6.3.3 Detail View – H.323 Capture

The detail decode view of H.323 call displays the following:

- MAC Layer
- IP layer
- TCP Layer
- TPKT Header Layer
- H225 Q.931 Call Signaling Layer
- H225 Call Layer
- H245 Layer.

PacketScan (VPA) H323

File View Capture Statistics Database Call Detail Records Configure Help

Dev	Frame#	TIME (Relative)	Len	Error	Protocols	Source IP Address	Destination IP Address	IP Packe
✓ 1	2	00:00:13.444104	380		Internet IP(IPv4)	192.168.1.151	192.168.1.232	H225

```

Urgent Pointer = x0000
===== TPKT Header Layer =====
TPKT Hdr
  Version = 3 (x03)
  Reserved = 00000000 (0)
  Length = 326 (x0146)
===== H225 Q.931 Call Signaling Layer =====
Protocol Discriminator = 00001000 Q931/I 451 user-network call control
Call Reference Length = ...0010 (2)
Call Reference Value = 30357 (.1110110 10010101)
Call Reference Flag = 1..... TO side that originated callref
Message Type = 00000001 ALERTING
IEI Display = 00101000 Display IE Identifier
IE Length = 9 (x09)
Display Information = x4E61676172616A7300
IEI User User = 01111110 User User IE Identifier
IE User User Length = 303 (x012F)
Protocol Discriminator(H323) = 00000101 X.680 and X.690 coded user information
===== H225 Call Layer =====
H323-UserInformation = SEQUENCE
Extensibility Marker = 0
Preamble = 0
h323-uu-pdu = SEQUENCE
Extensibility Marker = 1
Preamble = 0
h323-message-body = CHOICE
Extensibility Marker = 0
Choice Index = 3
  alerting = SEQUENCE
  Extensibility Marker = 1
  Preamble = 0
  protocolIdentifier = OBJECTIDENTIFIER
  Length Determinant = 6
  Contents = 0.0.8.2250.0.4
  destinationInfo = SEQUENCE
  Extensibility Marker = 0
  Preamble = 010001
  vendor = SEQUENCE
  Extensibility Marker = 0
  Preamble = 11
  vendor = SEQUENCE

```

Figure 32: Detail View of H323

6.3.4 Detail View – SS7 SIGTRAN Capture

The detail decode view of SS7 SIGTRAN call displays the following:

- MAC Layer
- IP Layer
- SCTP Layer
- MTP3 Layer
- ISUP Layer

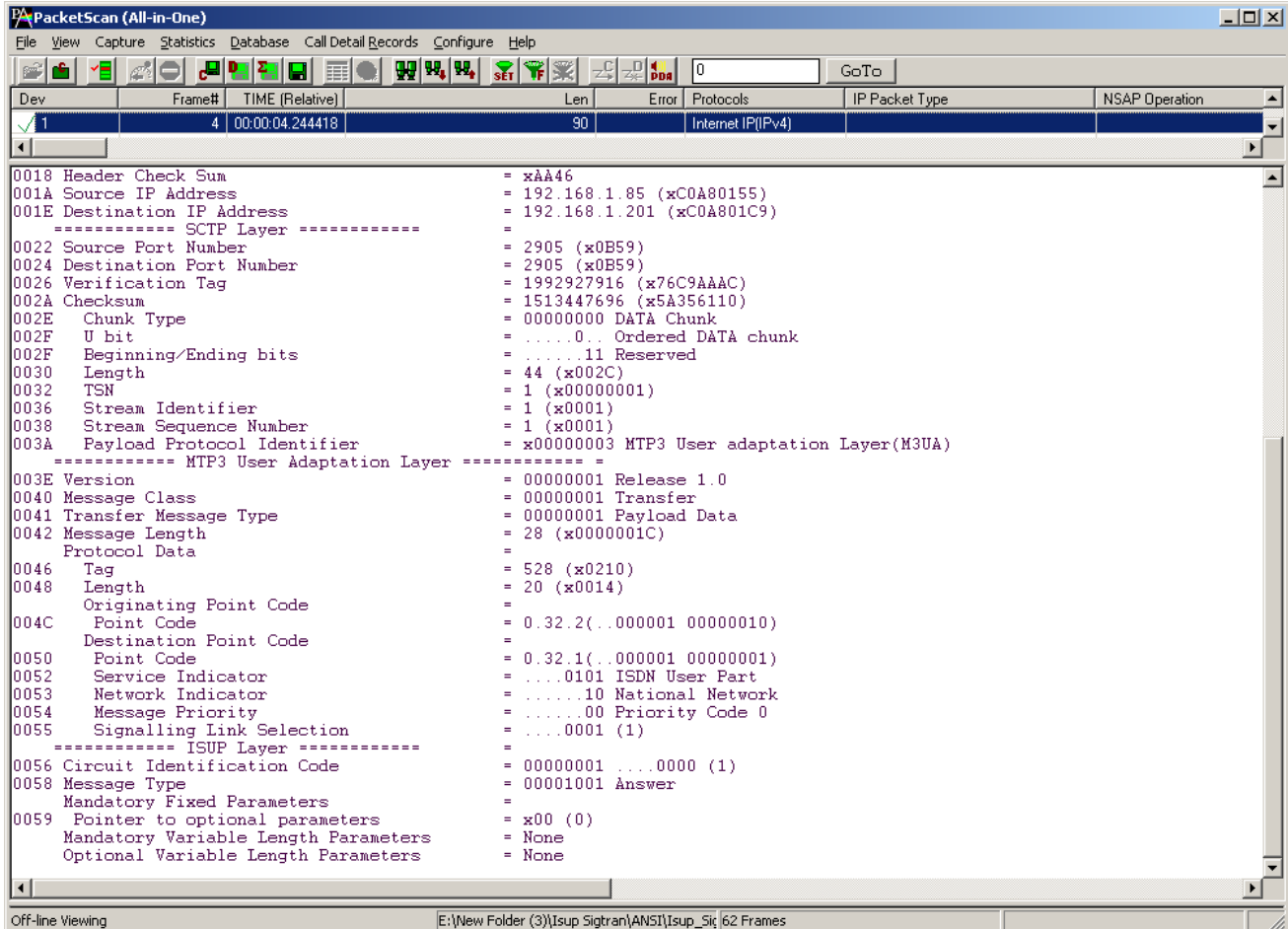


Figure 33: Detail View of SS7 SIGTRAN

6.3.5 Detail View – ISDN SIGTRAN Capture

The detail decode view of ISDN SIGTRAN call displays the following:

- MAC Layer
- IP Layer
- SCTP Layer
- ISDN Q.921 Layer
- Q.93x-Layer 3

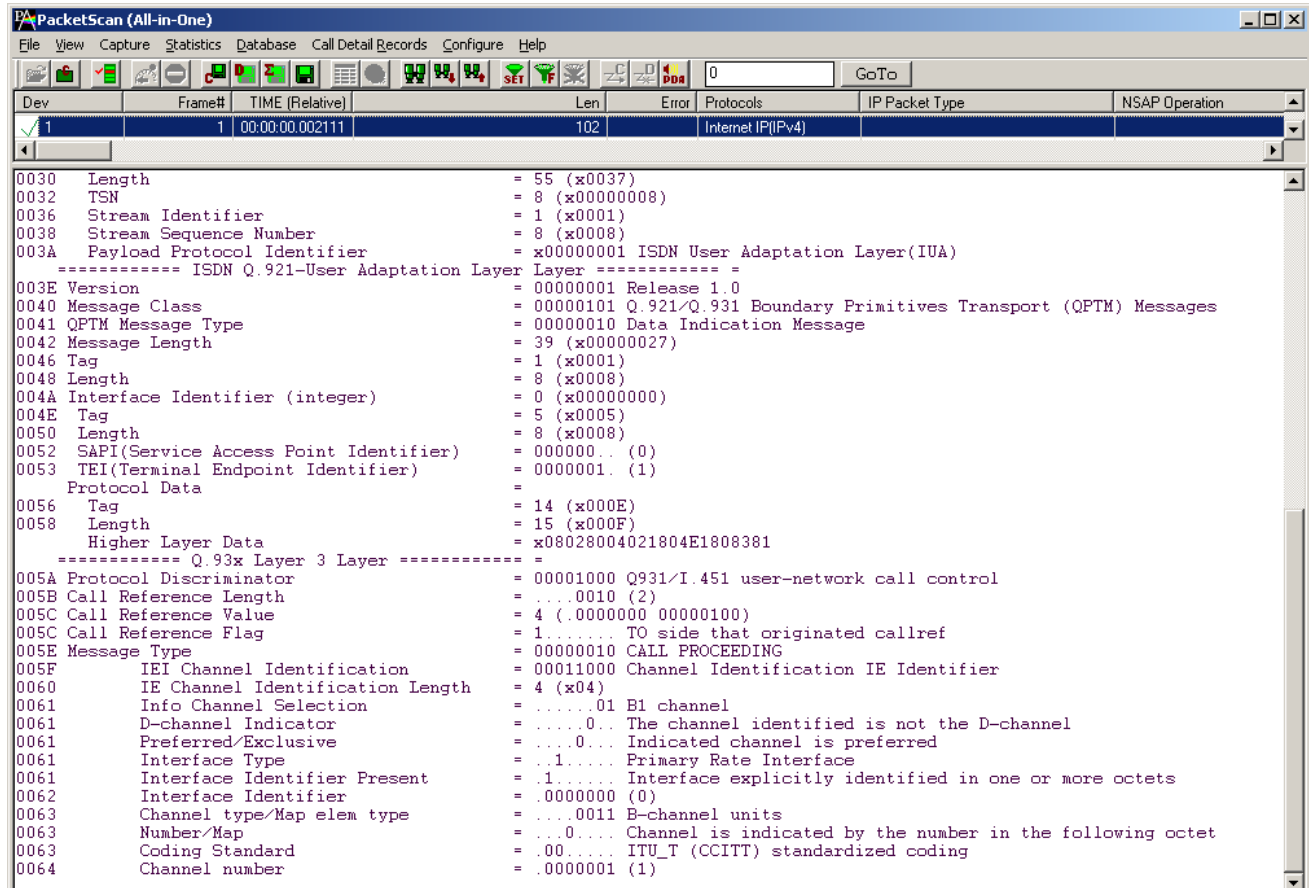


Figure 34: Detail View of ISDN SIGTRAN

6.3.6 Detail View – GSM A IP Capture

The detail decode view of GSM A over IP call displays the following:

- MAC Layer
- IP Layer
- SCTP Layer
- MTP3 Layer
- SCCP Layer
- GSM Phase 2 Layer
- MM Layer
- CC Layer

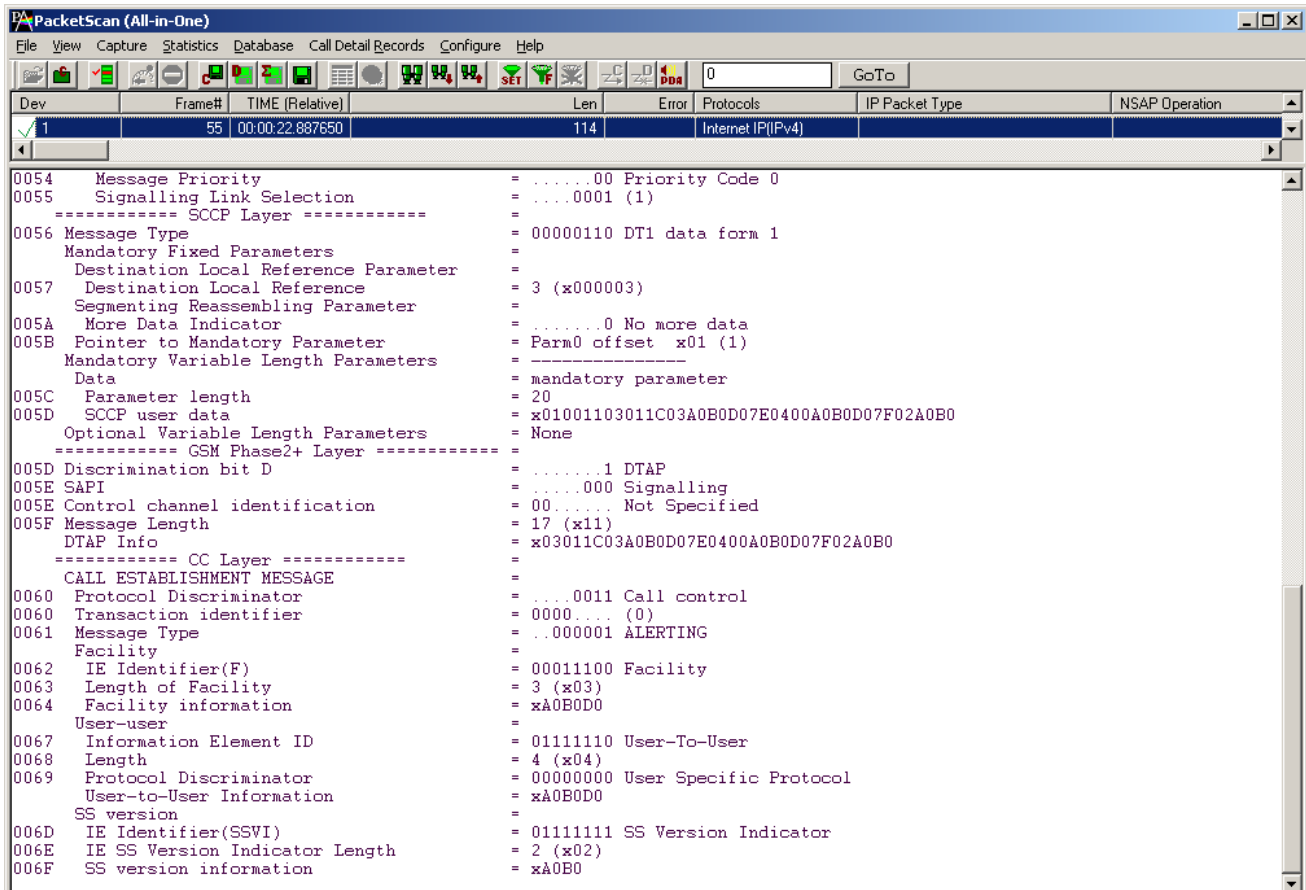


Figure 35: Detail View of GSM A over IP

6.3.7 Detail View – UMTS IP Capture

The detail decode view of UMTS over IP call displays the following:

- MAC Layer
- IP Layer
- SCTP Layer
- MTP3 Layer
- SCCP Layer
- RANAP Layer
- MM Layer
- CC Layer

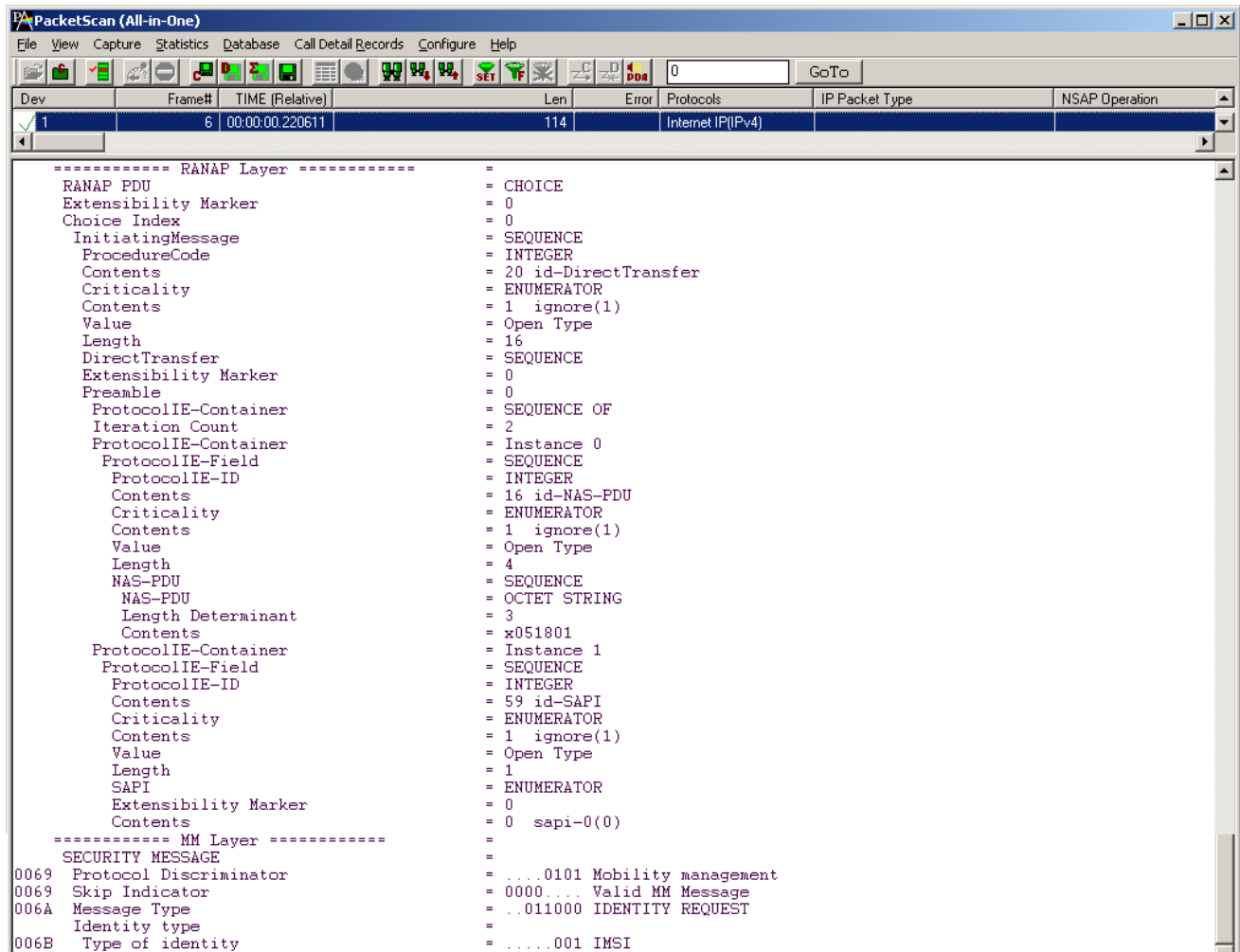


Figure 36: Detail View of UMTS over IP

6.3.8 Detail View – LTE Capture

The detail decode view of LTE call displays the following:

- MAC Layer
- IP Layer
- UDP Layer
- eGTP Layer
- S1AP Layer

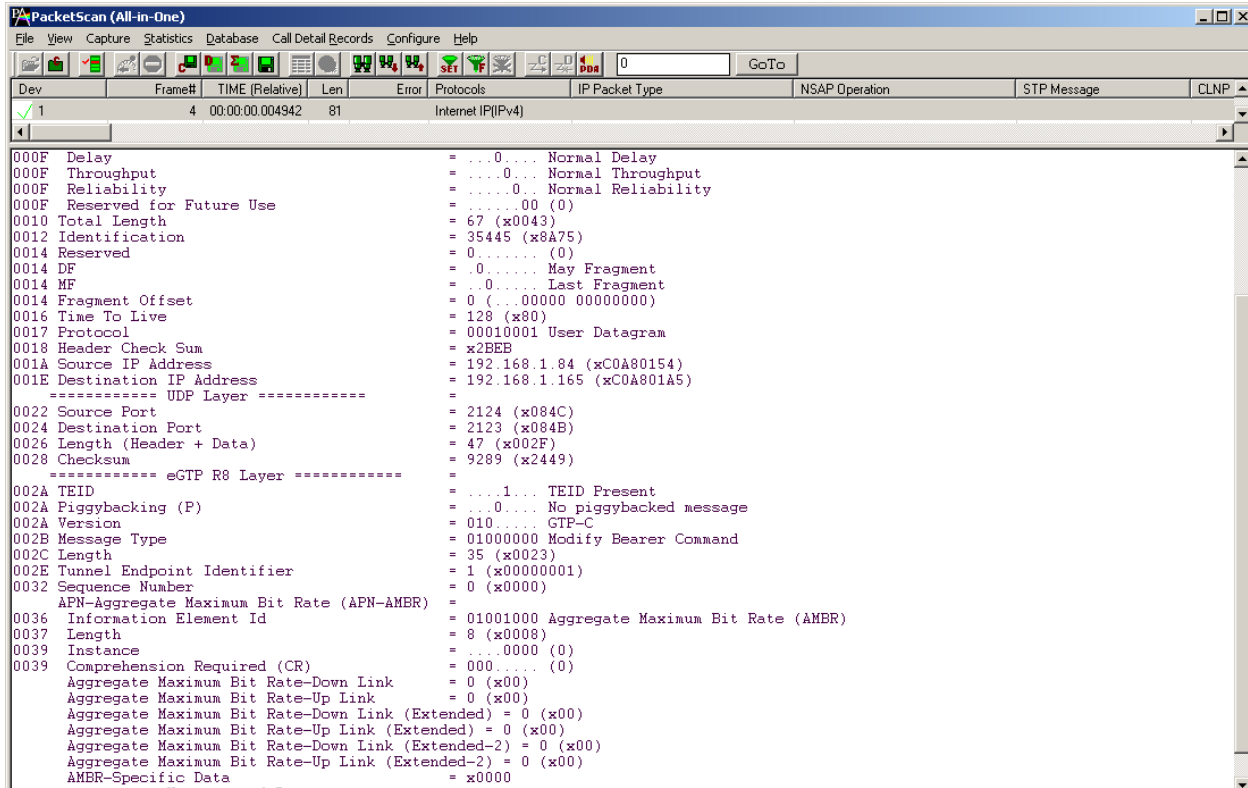


Figure 37: Detail View of LTE

6.3.9 Detail View – Diameter Capture

The detail decode view of Diameter call displays the following:

- MAC Layer
- IP Layer
- SCTP Layer
- Diameter Protocol Layer

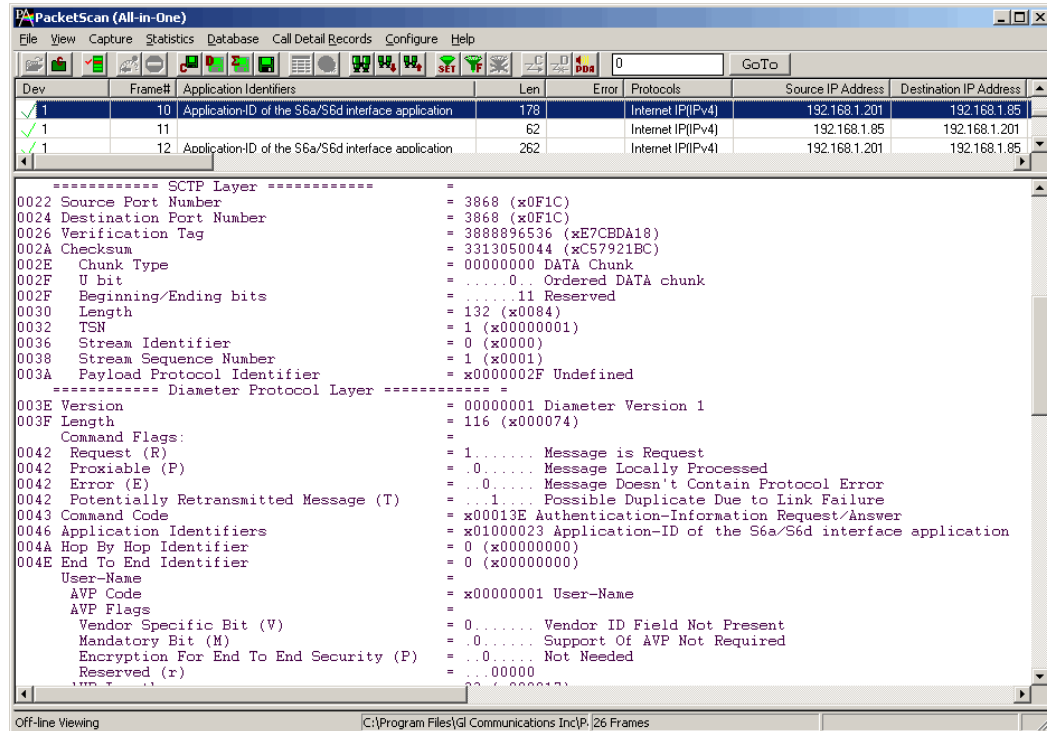


Figure 38: Detail View of Diameter

6.3.10 Detail View – Skinny Client Control Protocol (SCCP)

The detail decode view of SCCP (Skinny) call displays the following:

- MAC Layer
- IP Layer
- TCP Layer
- Skinny Client Control Protocol Layer

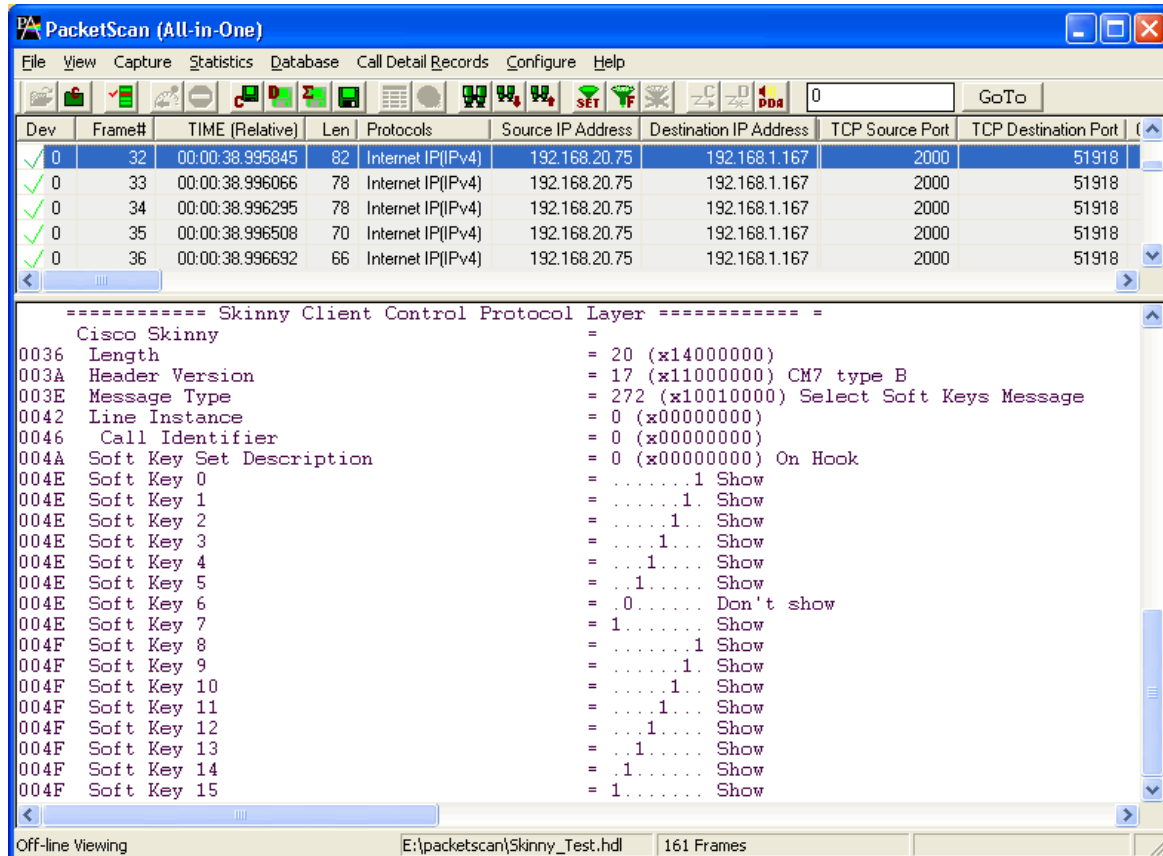


Figure 39: Detail View of Skinny Client Control Protocol

6.4 Hex Dump View

Hex Dump View displays raw frame data as a hexadecimal and an ASCII octet dump.

6.5 Statistics Views

Various statistics can be calculated based on the protocol fields. For more information refer to the Statistics section.

6.6 Protocol Standard and User-Network Side Specifications

The Protocol Standard option is used to select the required decoding standard, while the user-network side specifications is used to specify the network-side cards and is relevant when there are multiple analyzer cards. These options are required to be set before the analysis is started. For more details on configuring these options, refer to section [Protocol Standard Selection](#) and [Network / User Side Selection](#).

6.7 Time Display Formats

Four time formats are supported for both **real-time** and **offline** analysis. These time formats can be changed during both off-line and real-time operations by selecting the required time format either from **View > Time Format** menu item or by clicking on the time column header in the Summary View shown in the figure below.

- Select **View > Time Format** as shown in the figure below
- Click on the **Time** column header in the Summary View, Or
- Select **Time Format** under **Configure > Protocol and GUI** menu

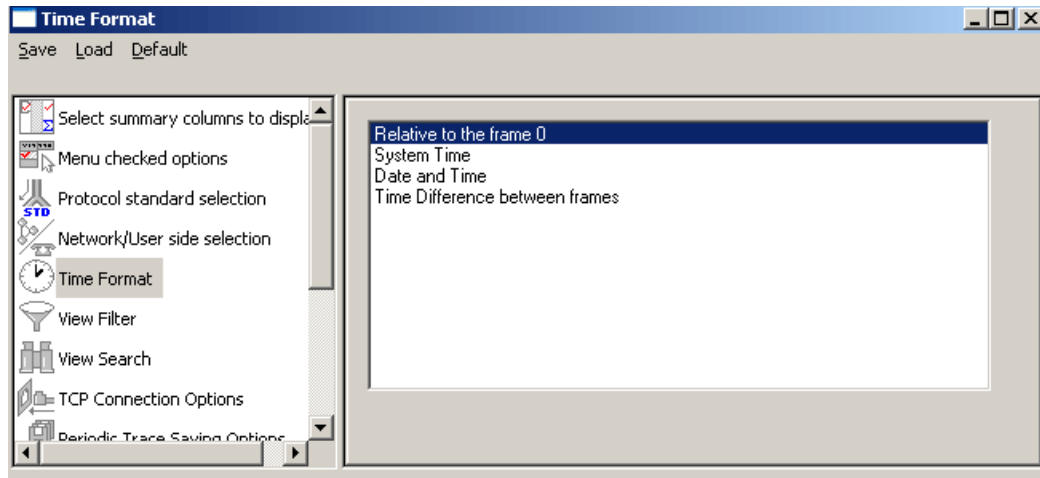


Figure 40: Time Format

6.7.1 Relative Time

In the **Relative Time** format, the time of capture of each frame is displayed relative to the time of a selected frame. In this format, time value of the selected frame when the option is activated is always 0:00:00:000000. Preceding frames have negative relative time and the following frames have positive relative time.

6.7.2 System Time

This option displays the system (local computer) time when frames were captured.

For instance, during real-time capture, if the capture time displayed for the first frame is 14:53:24:015411, it means that the first frame was captured at 2.53 P.M., 24 seconds, 015411 microseconds system time (PC).

6.7.3 Date and Time

Date and Time format shows local date and system (PC) time during the real-time capturing of the frames. For off-line analysis, the system time option shows the date and time when the trace was captured earlier. The display is in the form of year, month, day, hours, minutes, seconds and microseconds.

6.7.4 Difference Time

In Time Difference format displays, the time difference between consecutive frame capture times. For each frame it is this frame time minus the preceding frame time.

6.8 Latest

**Note:**

This feature is applicable to real-time analyzer only.

The **View > Latest** option enables/disables automatic screen refresh and repositioning of the Summary and Detail View to the latest captured frame. This option does not have any effect in the off-line analysis mode and is used only for real-time analysis to refresh screen approximately every two seconds. When the menu option is checked the automatic repositioning to the latest captured frame is enabled.

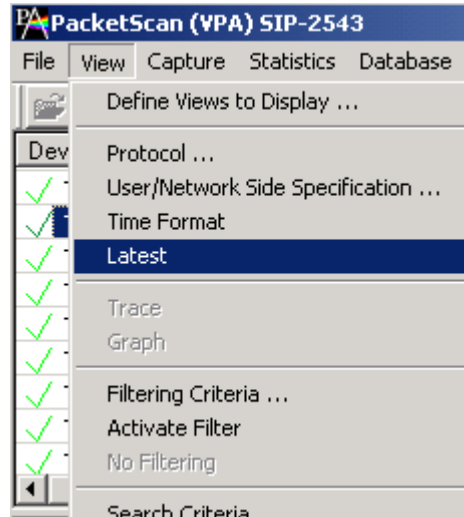


Figure 41: Auto Screen Refresh during Real-time Analysis

6.9 View Filtering Criteria



The View Filter is used real-time and offline to display and subsequently save, export and print a subset of frames satisfying a certain filtering criterion. The active filter is used as WYSIWYG (what you see is what you get). When filtering is active, the subsequent save as, export and or print will save only the filtered frames, else, all the frames will be affected by the operation.

All captured frames are preserved and will be displayed when filter is deactivated. The filtering criterion is effective till the criterion is changed, de-activated or analyzer is closed. After the filtering criterion has been specified the frame filtering can be activated or de-activated any time.

6.9.1 Setting Filtering Criteria

The filtering criteria are set for protocol fields and various parameters supported for the respective protocol standard. The parameters satisfying the conditions may be included or excluded from the result using the **Include** or **Exclude** options. All the selected criteria logically use **OR** or **AND** operations. A frame is filtered if at least one criterion matches (OR), or each criteria matches (**AND**).

Filtering Criteria can be set using any one of the following methods:

- Select **View > Filtering Criteria** menu item
- Click on the  View Filter button from **Configure > Protocol and GUI Options**
- Click **Filtering Criteria**  icon from the toolbar. The Filter selection dialog is displayed as shown in the figure below:

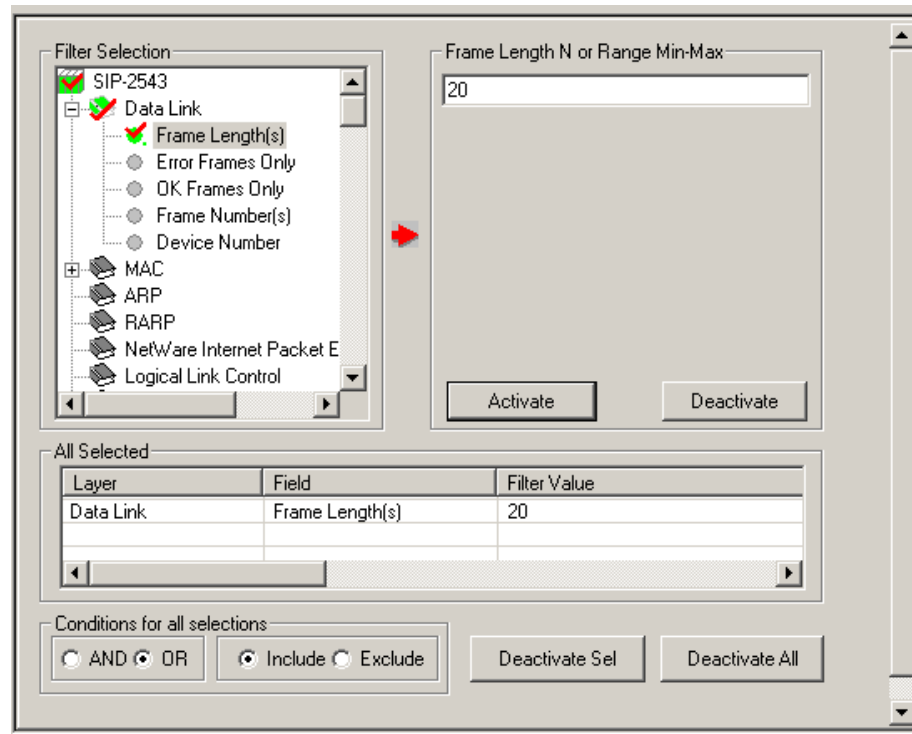


Figure 42: Setting Filtering Criteria

Just setting the filtering criteria is not sufficient to start filtering. After the filtering criteria have been set, activate filter as explained below.




Note:

For more information on the parameters provided in the filtering criteria, refer to [Appendix A: Glossary](#).

6.10 Activate Filter

Activate filter activates the filtering criterion and displays only filtered frames. To Activate filter perform any of the following steps:

- Select **View > Activate Filter** menu item as shown in the figure below or
- Click  from the toolbar Or
- Select Activate Filter option under **Configure > Protocol** and **GUI > Startup Options**

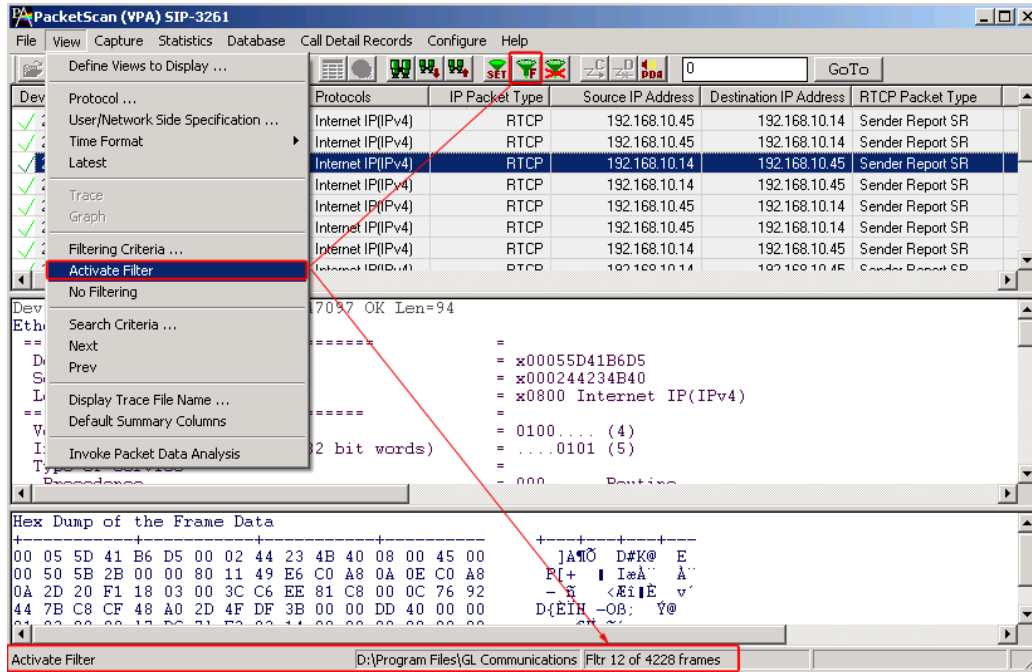


Figure 43: Activating Filter

If no filtering criterion is selected, then both **View > Activate Filter** menu item and the corresponding button are disabled. Therefore, setting filtering criteria must precede the filter activation.

The active filter affects subsequent save, export and print operations. It works as WYSIWYG (what you see is what you get).




Note:

Select Activate Filter option (provided under **Configure > Startup Options**) before setting the filter. For more details refer to [Startup Options](#).

6.11 Deactivating Filter

Deactivating filter removes filtering and displays all the frames in the trace.

- Select **View > No Filtering** menu item as shown in the figure below Or
- Click **Deactivate Filter**  from the toolbar.

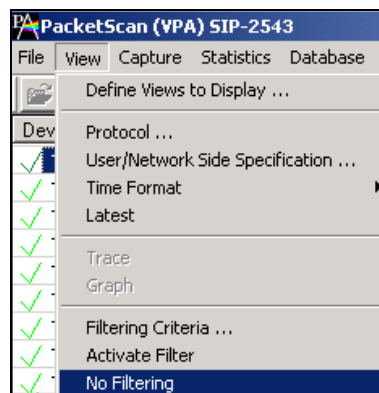


Figure 44: Deactivating Filter

6.12 Example - View Filter

To filter out frames with errors and display only the erred frames, follow the steps below:

- 1) Expand **Data Link Layer**. Select **Error Frames Only** option as shown in the figure below to filter all error frames.
- 2) Enter the character 'y' in the entry field and click **Activate** to apply the settings.
- 3) Select **Include** radio button and close the **View Filter** window to apply the settings.
- 4) If more than one filter condition is required, select the AND / OR option accordingly.

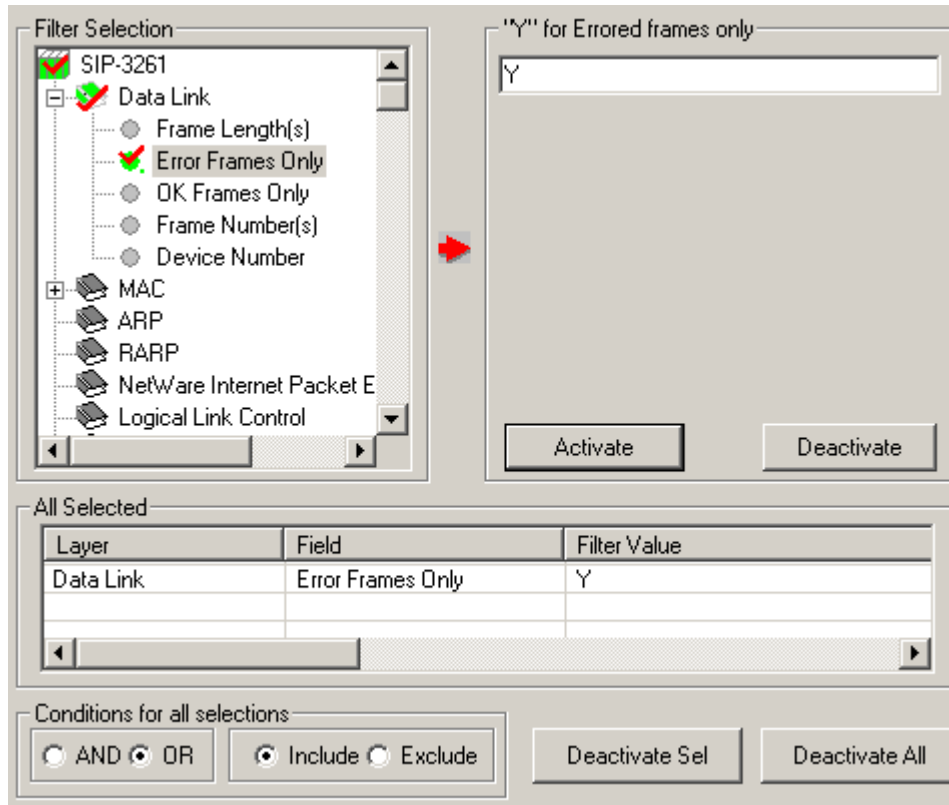




Figure 45: Example - Filter Option to filter Error Frames Only

6.13 Searching for Specific Frames

First, the search criterion has to be set and then 'Next' or 'Prev' function is invoked to search from the current record towards end of trace (next) or beginning of the trace (prev). If filtering is active the search operation is conducted among the already filtered frames.

Search Criteria can be set using any one of the following methods:

- Select **View > Search Criteria** menu item
- Click on the  View Search button from **Configure > Protocol and GUI Options** Or
- Click  from the toolbar to open search criteria window as shown in the figure below

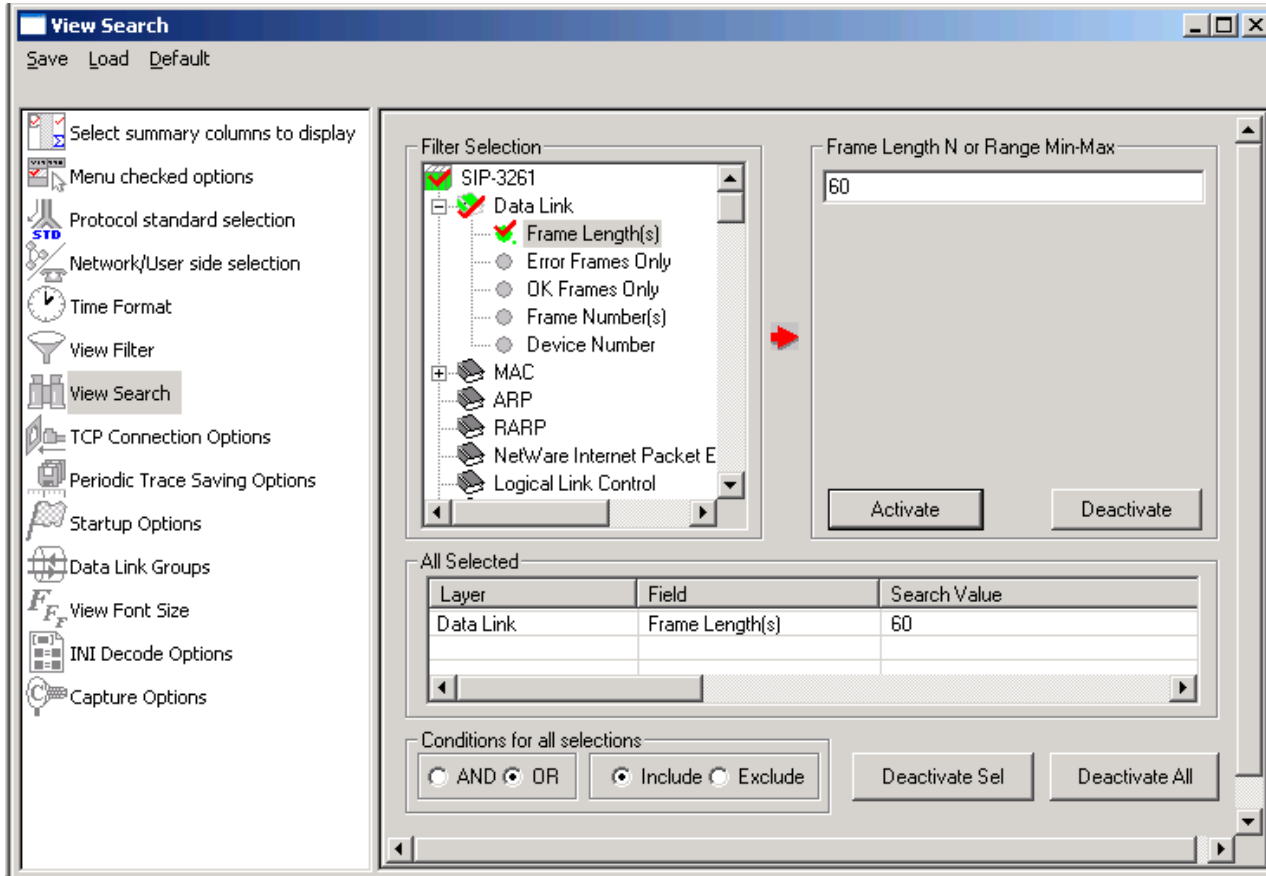


Figure 46: Setting Search Criteria

6.14 Forward Search and Backward Search

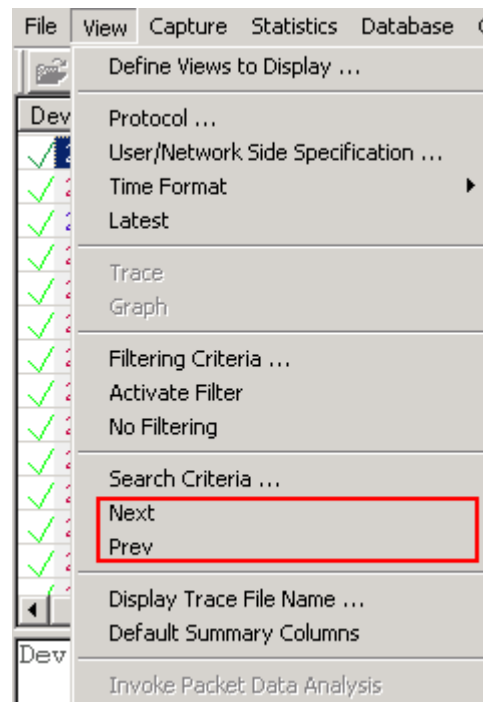



Figure 47: Searching Forward


6.14.1 Searching Towards the End of the Trace (Forward Search)

This operation will search from the current frame in the Summary View towards the end of the trace. To view next menu item:

- Select **View > Next** menu item or
- Click  from the toolbar

6.14.2 Searching Towards the Beginning of the Trace (Backward Search)

This operation will search from the current Frame in the Summary View towards the end of the trace. To invoke this operation, follow the steps given below:

- Select **View > Prev** menu item as shown in the figure below or
- Click  from the toolbar

6.15 Display Trace File Name

Select **View > Display Trace File Name** menu item to view the filename under which the analyzer capture frames during real-time or offline-trace as shown in the figure below. This option is useful when the file name is very long and is truncated in the status pane.

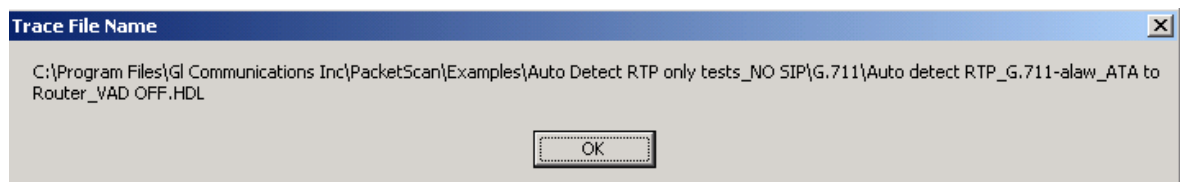


Figure 48: Trace File Name

6.16 Default Summary Columns

To return to the **Default Summary Columns** from resized/reordered columns, click the **View > Default Summary Columns** option as shown in the figure below:

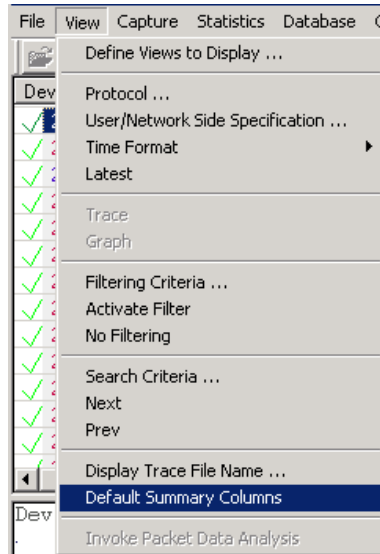



Figure 49: Default Summary Columns

6.17 Invoke Packet Data Analysis

In order to view the Traffic analyzer Summary or Detail View:

- Select **View > Invoke Packet Data Analysis** menu item, Or
- Click **Invoke Packet Data Analysis**  from the toolbar to open the window as shown in the figure below

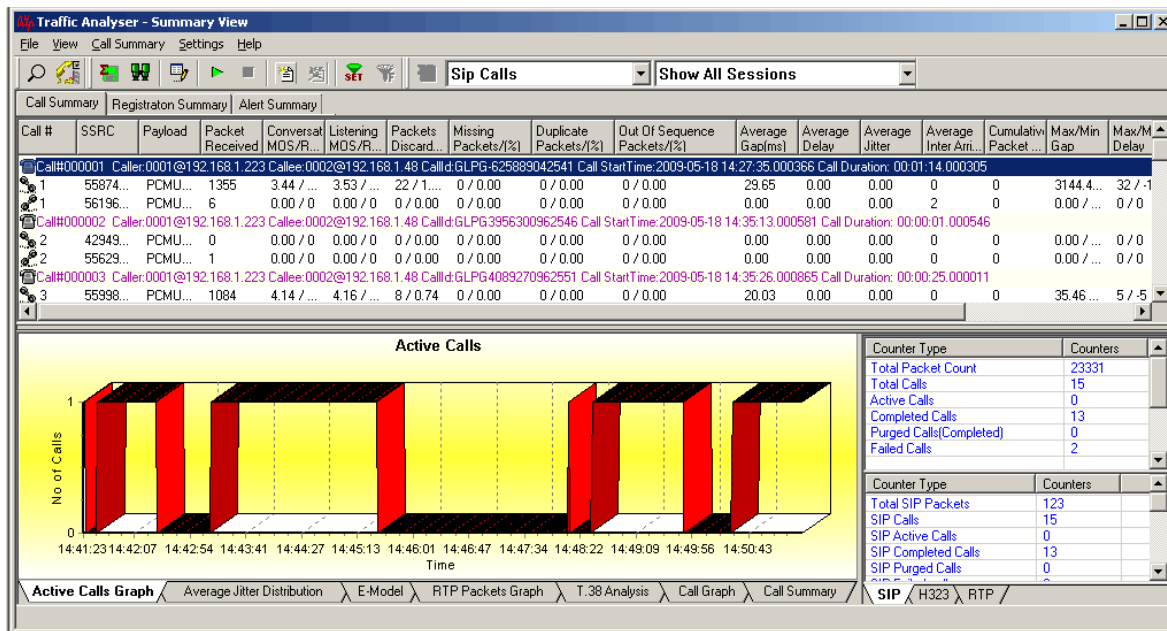


Figure 50: Traffic Analyzer

For more details on this, refer to section [Packet Data Analysis – Traffic Analyzer Summary View](#), [Packet Data Analysis – Traffic Analyzer Detail View](#), and [Packet Data Analysis – Registration Summary](#).

Section 7.0 Capture Menu Features



Note:

Capture Menu features are applicable to real time analyzer only.

7.1 Periodic Trace Saving Options

Periodic trace saving is used to preserve all real-time captured data. Frames are saved to separate trace files by size or time criteria and capture is limited only by the available amount of hard disk space.

Select, **Capture > Periodic File Saving Specifications**, to open the screen as shown in the figure below.

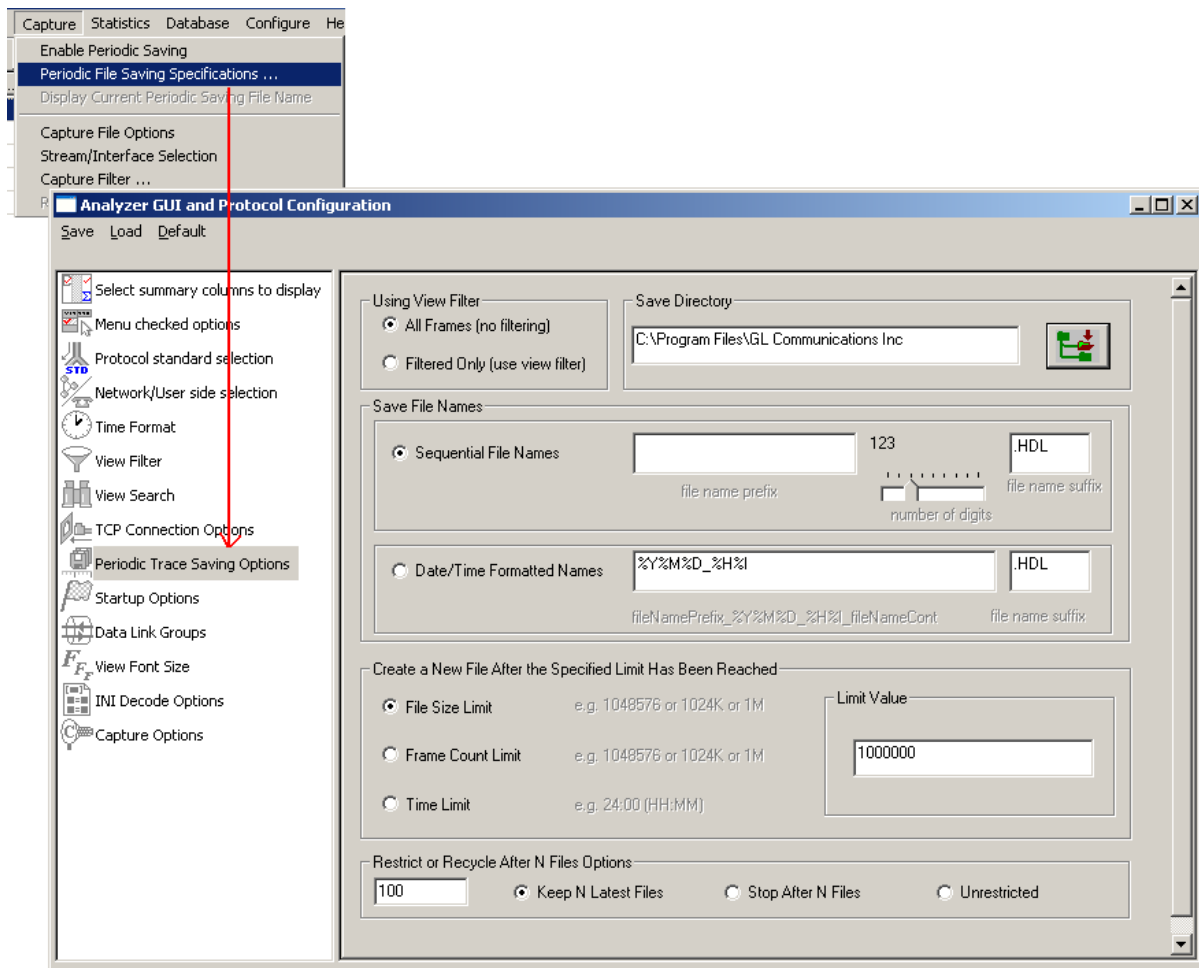



Figure 51: Periodic File Saving Specifications

Save Directory:

Click  browse button to select the path of the directory where the files will be saved.

Save File Names:

Sequential File Names

This file naming convention saves the trace files with user-defined prefixes along with the numbers indicating the sequence of the file. Select **Sequential File Names** radio button and enter a name in the **file name prefix** entry field. Use the slider control to indicate the total number of files to be saved. You can drag the slider handle to any position using the mouse or simply click to the left or right of the slider handle to move it. You can control the slider by number of digits.

Example: Enter the file name prefix as 'ff' and set the slider control to third position of the ruler in the number of digits slider box. Now the files will be saved from ff000 up to ff999 in the user-defined directory.

Date/Time Formatted Names:

This file naming convention saves the trace file with date-time prefixes. Select **Date/Time Formatted Names** radio button to obtain the file name saved with the year, month, date, and hour.

Example:

Enter the file name prefix as %Y%M%D_%H%I in the **Date/Time Formatted Names** text box. Verify that the trace files are saved in '20050531_0953.HDL' format in the user-defined directory. The formatting specification refers to the year, month, day, hour and minute (date and time stamp).

Create a New File After the Specified Limit has been Reached:

Select either **File Size Limit**, **Frame Count Limit**, or **Time Limit** option and specify the limit in the Limit Value entry field.

Restrict or Recycle After N Files Options:

Select **Keep N Latest files**, **Stop After N Files**, or, **Unrestricted** option to get the desired number of trace files.

Keep N Latest files – Restricts the file saving only for last 'N' number of files, where 'N' is the value set in the text box. When **N** is reached the older files will be overwritten by the most recent files keeping the total number of files equal to N.

Stop After N Files – Restricts the file saving only for first 'N' number of files, where 'N' is the value set in the text box. After the limit has been reached, the periodic saving stops.

Unrestricted – This option does not restrict the number of files being saved. This option limits the periodic saving to the available disk space only.

For Example:

Enter the value as 10(N=10) in the entry field and select **Keep N Latest files** radio button. Only ten files will be kept. They will contain the latest captured data.

Enter the value as 10(N=10) in the entry field and select **Stop After N Files** radio button. Initial 10 files are obtained and the process is stopped.



Note:

Select **Enable Periodic Saving** and **Start real-time tracing** options (provided under **Configure > Startup Options**) before setting the Periodic File Saving Specifications.

7.2 Setting Capturing Options

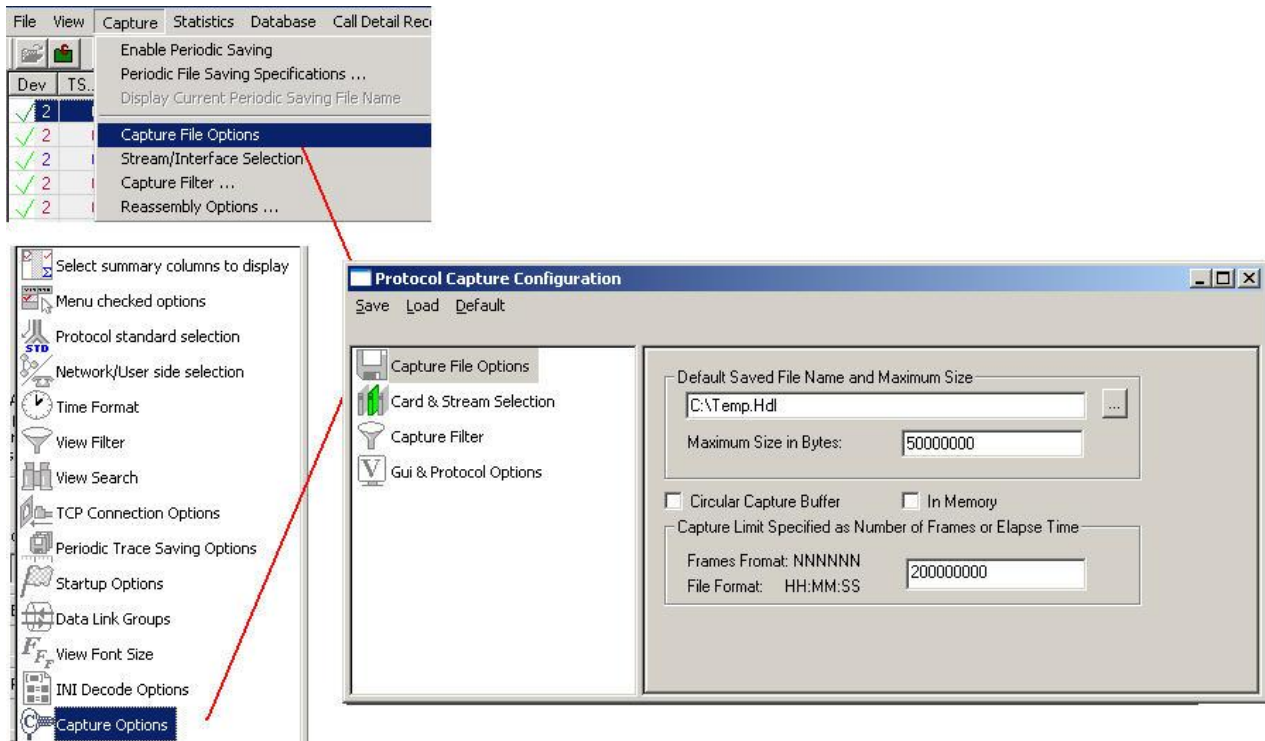


Figure 52: Capturing Options

From the main menu select **Capture > Capture File Options**. This dialog is used to specify a temporary file location, maximum file size in bytes, frame count or time limit as per the requirements. The capturing settings are saved in the Windows registry when the user exits the application. They do not need to be entered each time application is started.

Specific settings can also be saved using Save menu option and subsequently loaded when needed.

The file name can be either typed in the entry field or selected using the file dialog by clicking '...' button. The limit in frames should be specified as a positive number, 50000000 indicate that the maximum trace file size is 50Mb. If the limit is specified using the time format, for example, 12:22:20, then capturing stops after 12 hours, 22 minutes and 20 seconds.

The capturing settings are saved in the Windows registry when the user exits the application. They do not need to be entered each time application is started.

Capturing stops when either the maximum trace file size in bytes is reached or the capturing limit is exceeded when circular capturing is not used.

7.2.1 In Memory for High Traffic Capture Rate

In case of high traffic rate (>50 Mbps), select the **In Memory** check box to get better performance. This will store all the frames in primary memory instead of writing to trace file on the disk till the trace file is closed. Frames will be written to trace file only when analyzer is closed. This option is used when disk is not fast enough to keep with capturing speed but if in-memory file is large, say 500 MB it will take a while to close the trace file.

7.2.2 Circular Capture Buffer

For infinite capturing, select the **Circular Capture Buffer** check box. When end of the capturing buffer is reached, the capturing does not stop. Instead, the oldest trace records are purged from the buffer and the new ones are placed at the end of the circular buffer.


Various options are available for saving trace file, refer to the section [Periodic Trace Saving Options](#) for more details.



Note:

GL's PacketScan™ software is now designed to handle processing on 64 bit CPUs.

7.3 Stream / Interface Selection

- 1) Select **Capture > Stream/Interface Selection** as shown in the figure or
- 2) Click **Stream/Interface**  from the toolbar.

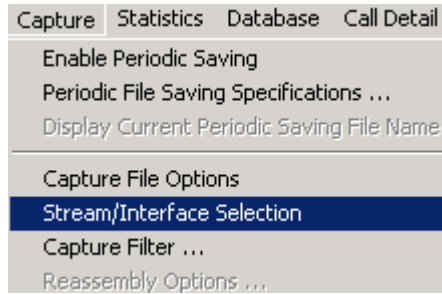


Figure 53: Setting the Capturing option

This helps the user to enable Ethernet boards so that data can be received on these boards. This option must be checked. If there are multiple Ethernet boards, user can select the desired ones.

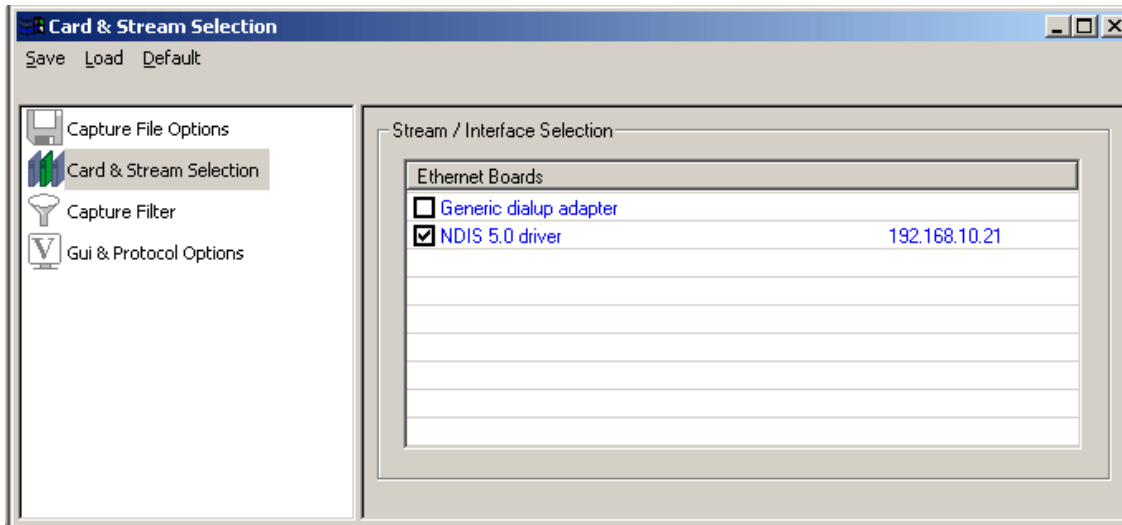


Figure 54: Specifying Stream/Interface Selection

7.4 Setting Capture Filter

From the main menu select **Capture > Capture Filter** option to open the screen as shown in the figure below.

This filter selection is used only in real-time and it's like a tree structure which has MAC layer, IP / IPV6 Layer, TCP Layer, UDP Layer, SIP layer, RTP layer, SCTP layer, MEGACO layer, MGCP layer and H.323 layer. Users can enter more than ten IP address and ports for each layer.

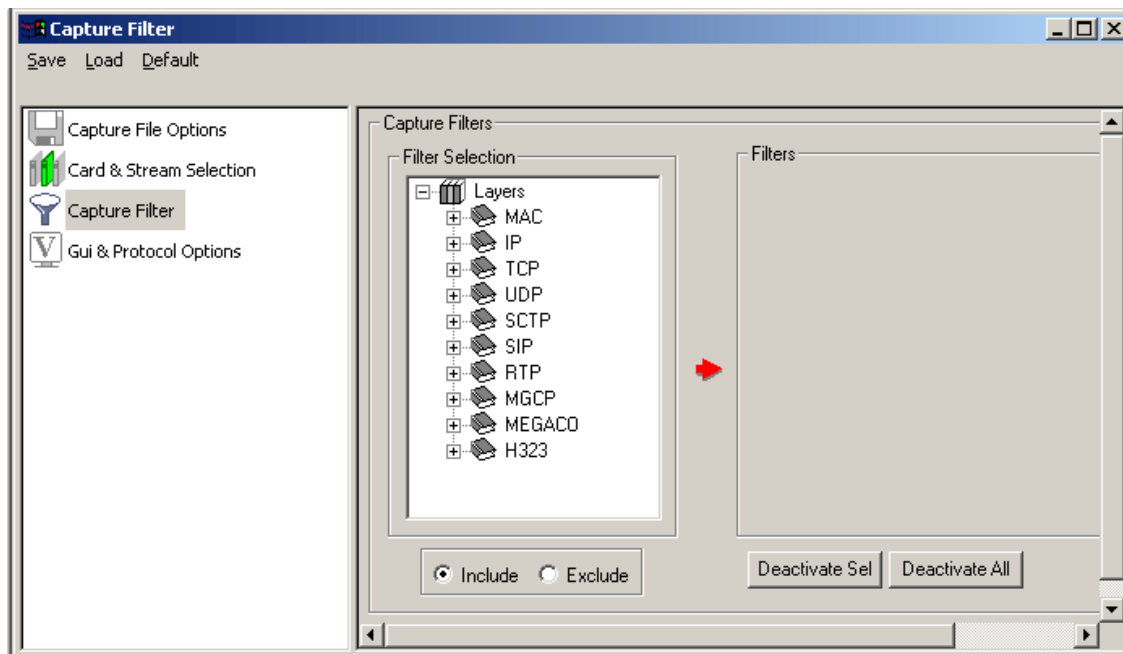


Figure 55: Capture Filter

The Capture Filters are set as shown in the figure above. Set the filtering selection.

- Click **Deactivate Sel** to deactivate the required selection in the Filter Selection list
- Click **Deactivate All** to deactivate all selections in the Filter Selection list
- Click **Include** to include the Filter Selections in real time capture
- Click **Exclude** to exclude the Filter Selections in real time capture

7.4.1 MAC Layer

Select **Filter All MAC data** option as shown in the figure below to capture all MAC data.

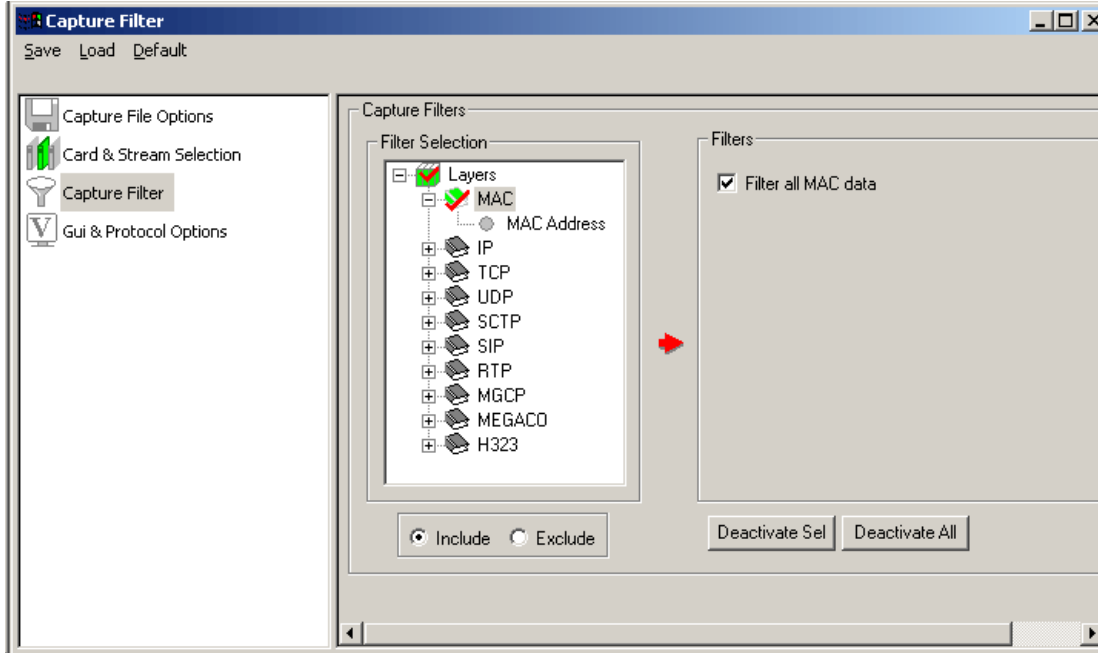


Figure 56: MAC Layer

If specific part of data is to be captured in MAC layer, user can specify the MAC Source address, direction and MAC destination address shown in the figure below. User can click **Add** to add the selection and **Delete** to cancel the selection.

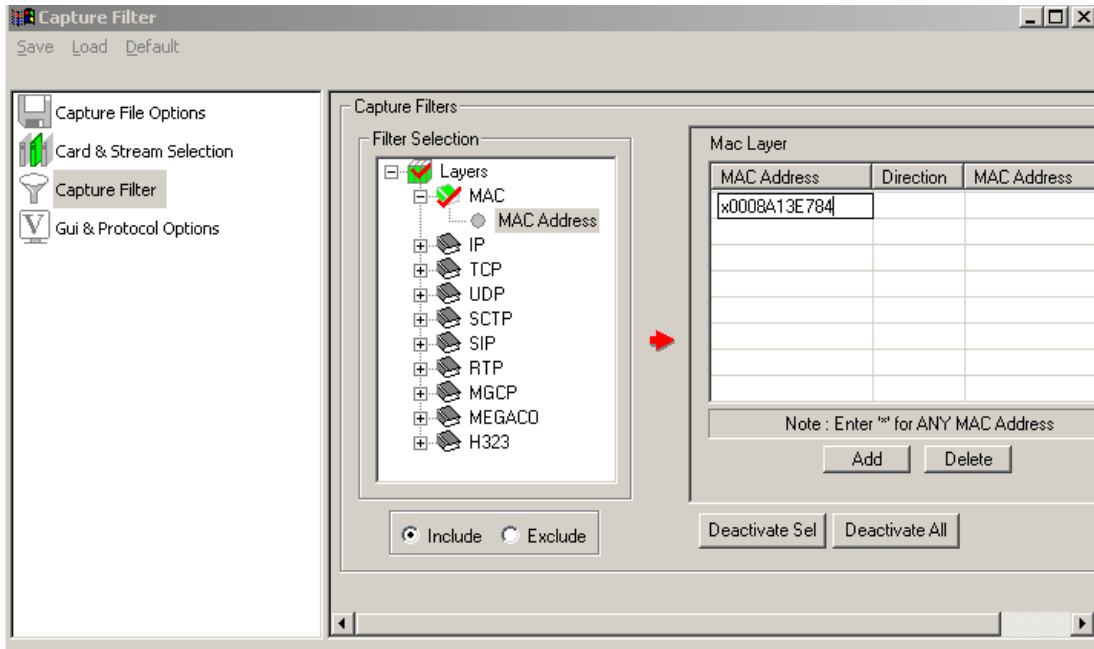


Figure 57: MAC Address

7.4.2 IP

Select **Filter All IP data** option shown in the figure to capture all IP data.

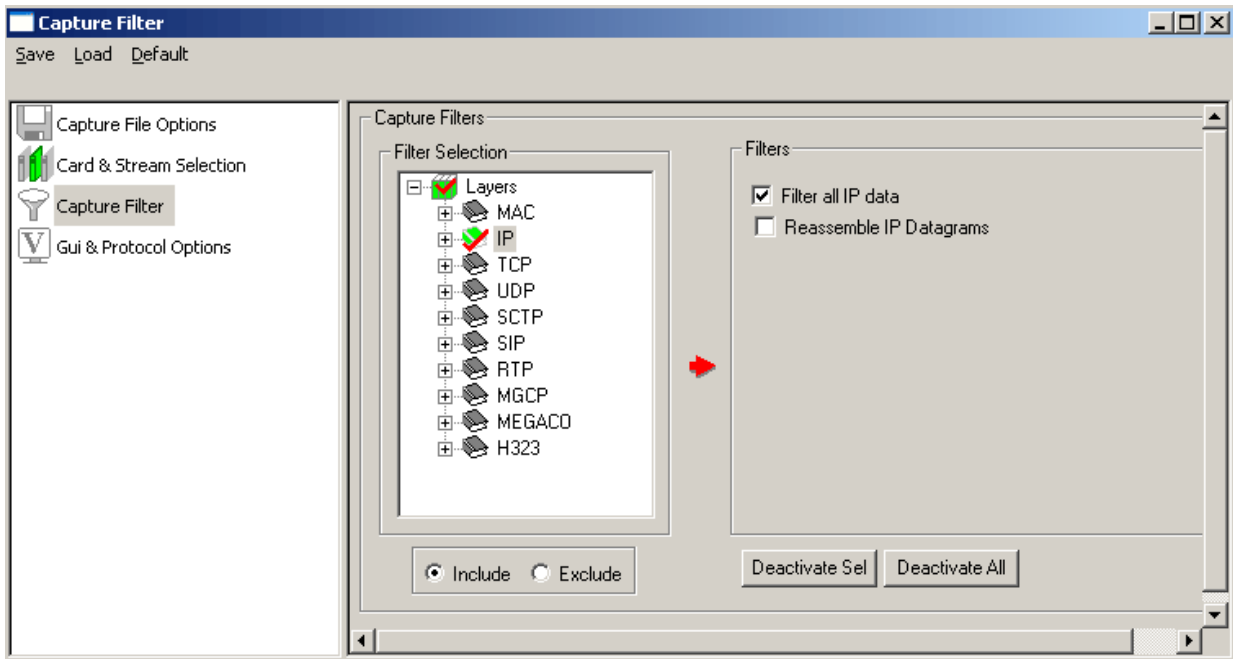


Figure 58: IP Layer

If the machine where **PacketScan™** is running is connected to the monitor port of the switch, all the IP data of all the machines connected to the LAN will be captured. In case, if specific part of IP data is to be captured, then the IP address (Source & Destination) and direction should be specified as shown in the figure below.

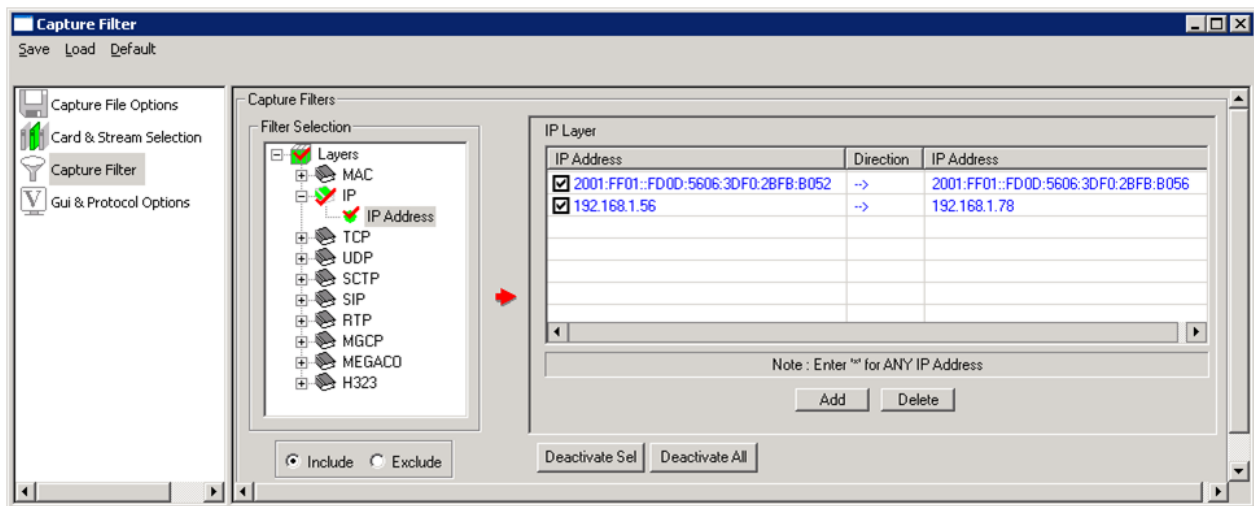


Figure 59: IP Address

ANY:

This ANY option is used when the user wants to capture IP data from particular machine to any machine connected to the LAN and various directions of capture is set as shown in figure below.

In case the source IP address is specified and the Destination IP address is ANY, which means that IP data from the source IP to ANY machine connected to the LAN is captured. The directions of capture can be set as desired.

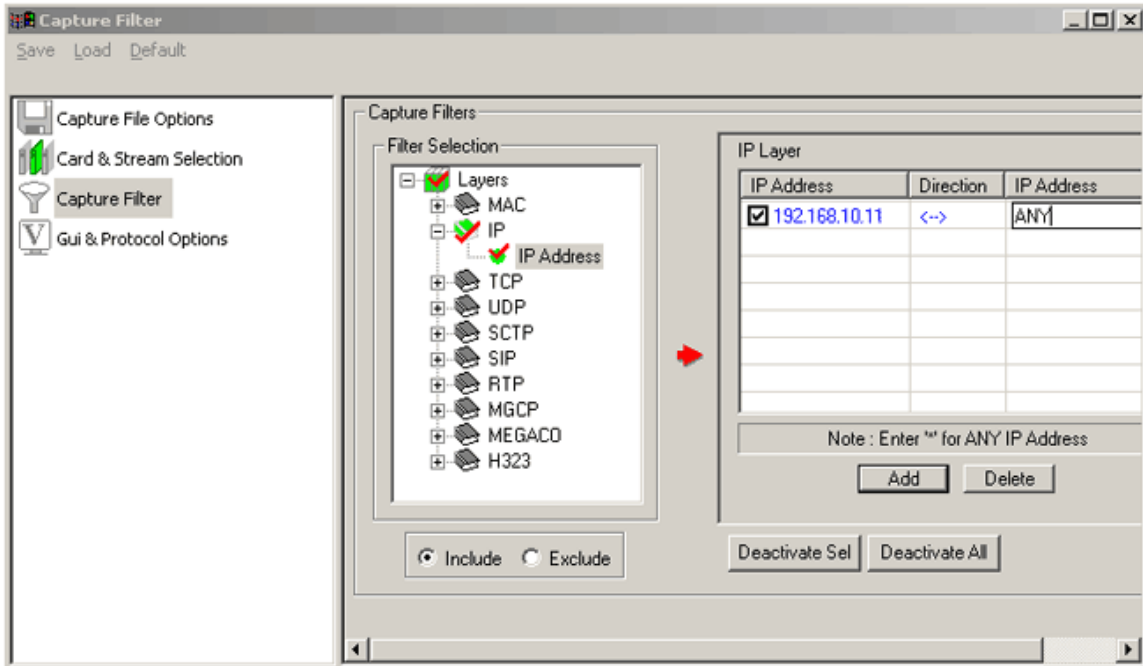


Figure 60: ANY IP Address

In case the source IP address is ANY and the Destination IP address is specified shown on (Figure 49), which means that IP data from the Destination IP to ANY machine connected to the LAN is captured.



Note:

- Enter '*' to indicate ANY as the source/destination address. In case the source address is specified and the destination address is set to ANY, it means that data from the specified source to any machine connected to the LAN is captured. The directions of capture can be set as desired. In case the source address is ANY and the destination address is specified, it means that data from the destination address to any machine connected to the LAN is captured.
- Both source and destination addresses should not be **ANY** at the same time.

7.4.3 TCP

Select **Filter All TCP data** option as shown in the figure to capture all TCP data.

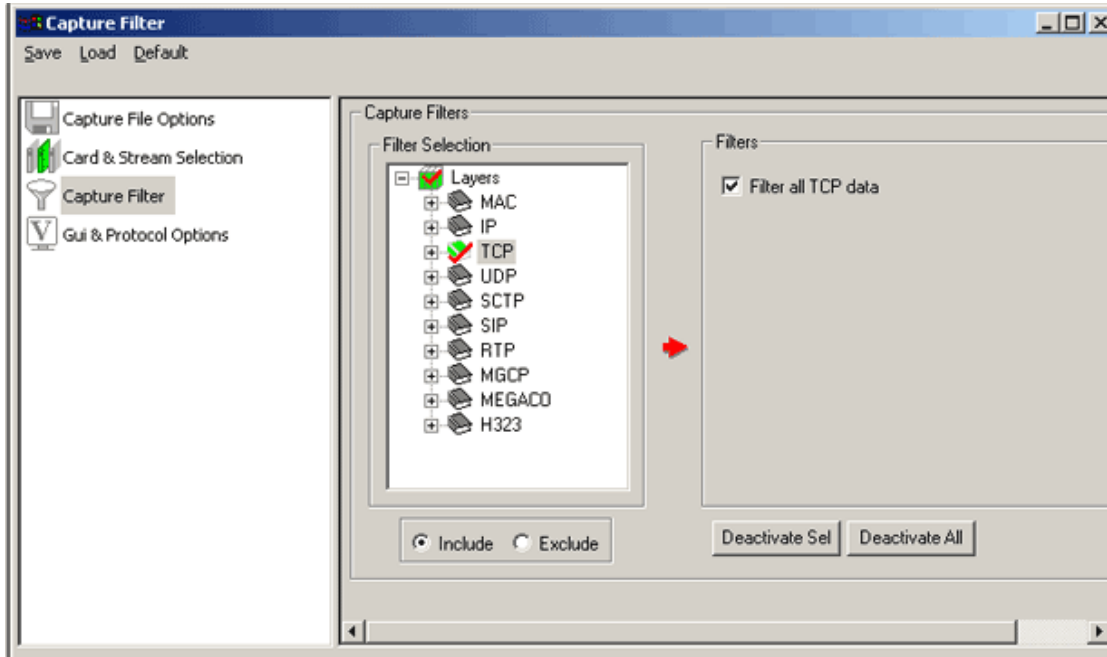


Figure 61: TCP Layer

If a part of TCP data is to be captured then, user can specify TCP source port and TCP destination port as shown in the figure below.

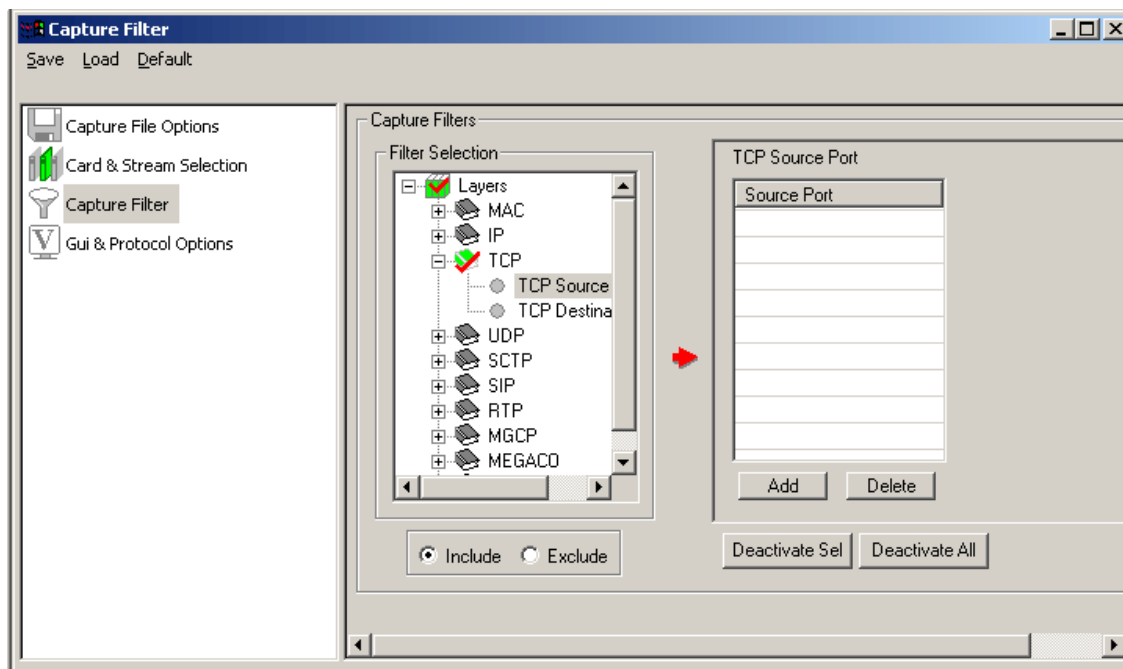


Figure 62: TCP Source and Destination Port

7.4.4 UDP

Select **Filter All UDP data** option to capture all UDP data as shown in the figure below.

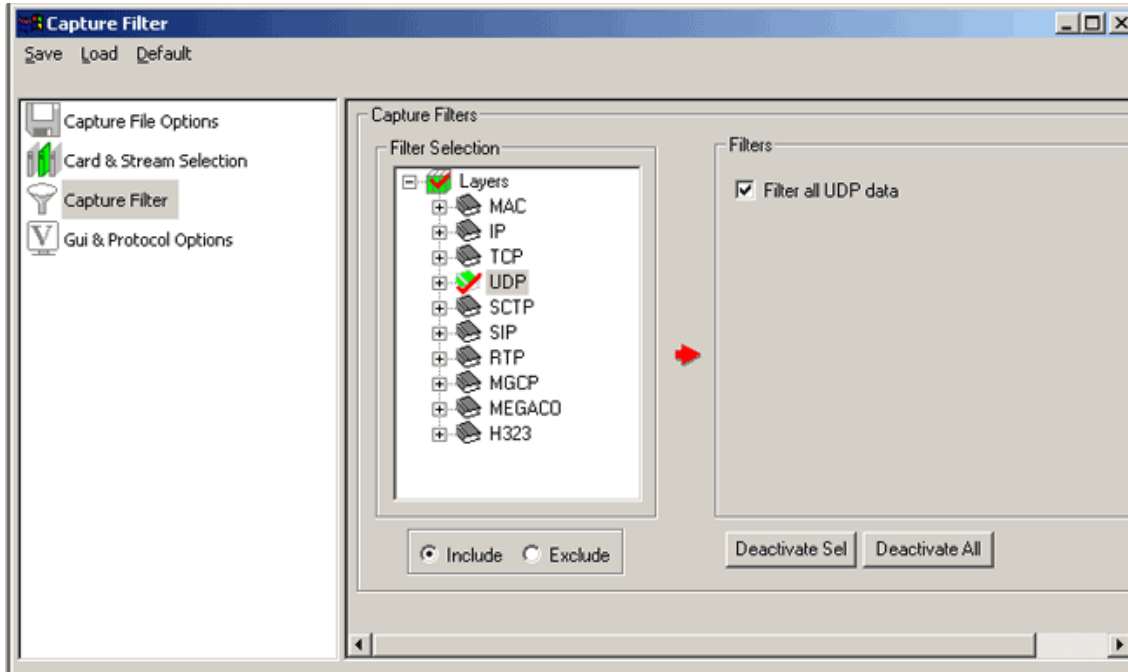


Figure 63: UDP Layer

User can specify UDP source port and UDP destination port to capture a part of UDP data as shown in the figure below.

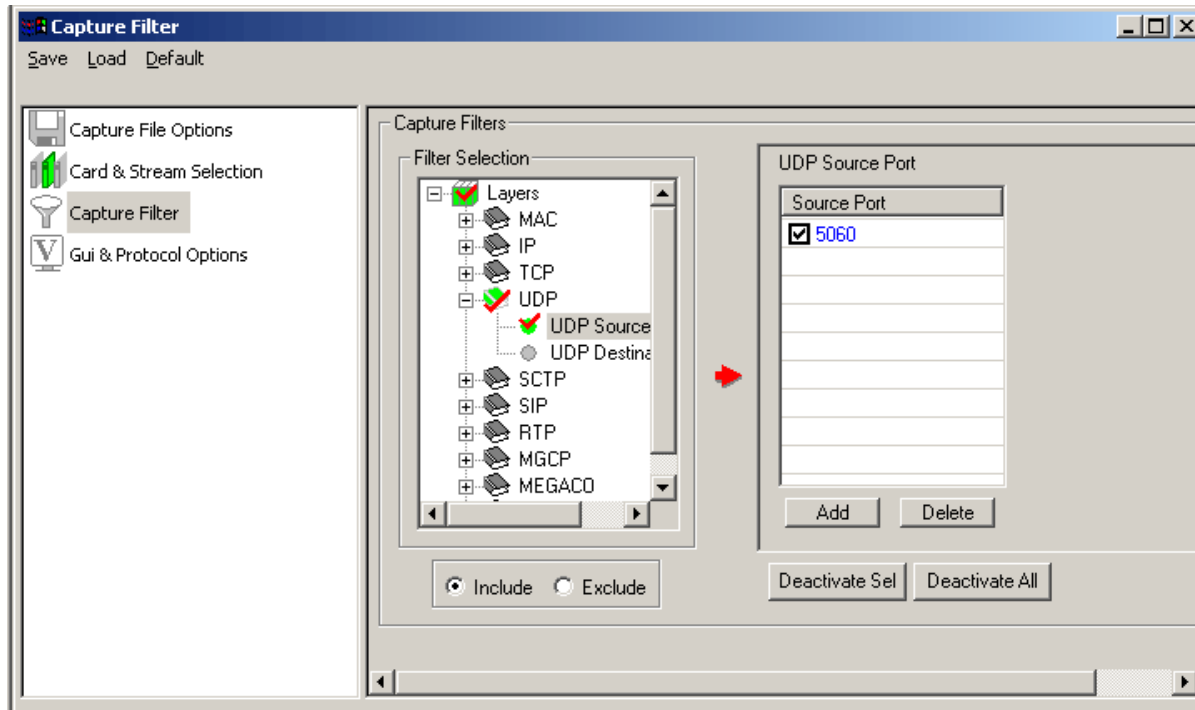


Figure 64: UDP Source and Destination Port

7.4.5 SCTP

Select **Filter All SCTP data** option as shown in the figure below to capture all SCTP data.

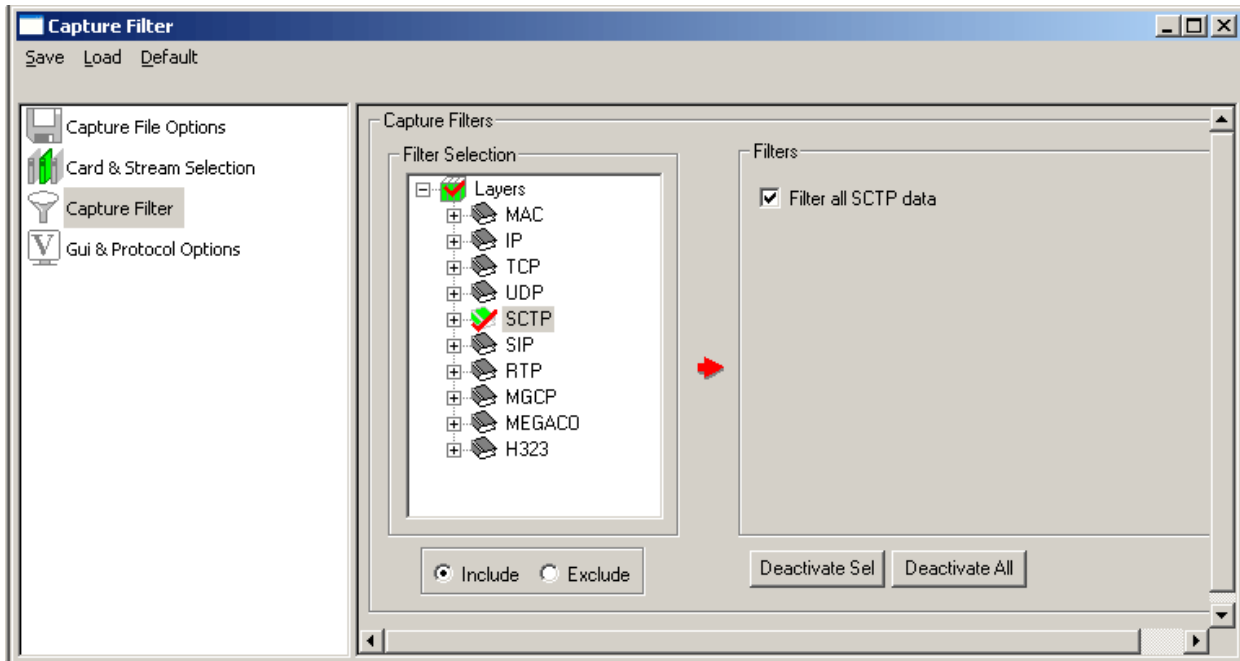


Figure 65: Sctp Layer

If a part of Sctp data is to be captured then, user can specify Sctp Ports as shown in the figure below.

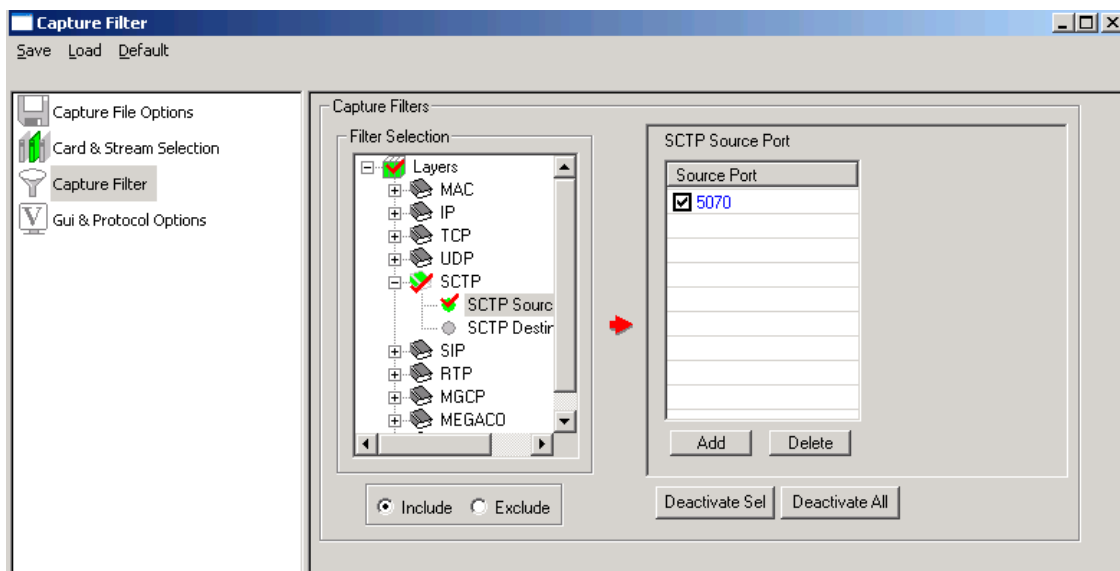


Figure 66: Sctp Source and Destination Port

7.4.6 SIP

Select **Filter All SIP data** option shown in the figure below to capture all SIP data.

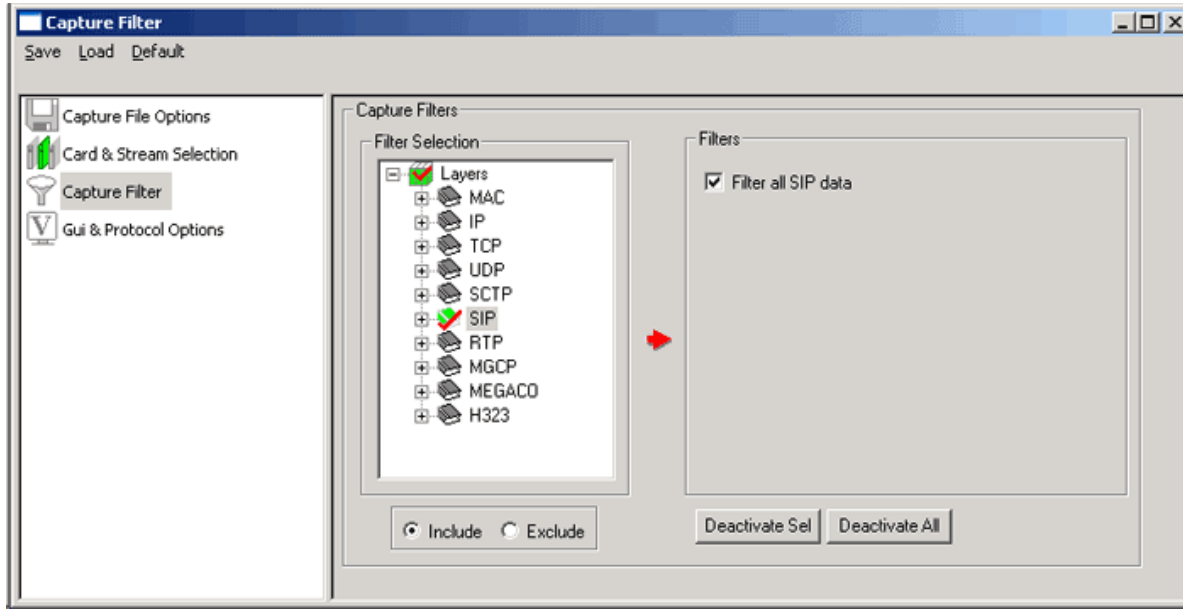


Figure 67: SIP Layer

If a part of SIP data is to be captured then, user can specify Additional SIP Ports as shown in the figure below.

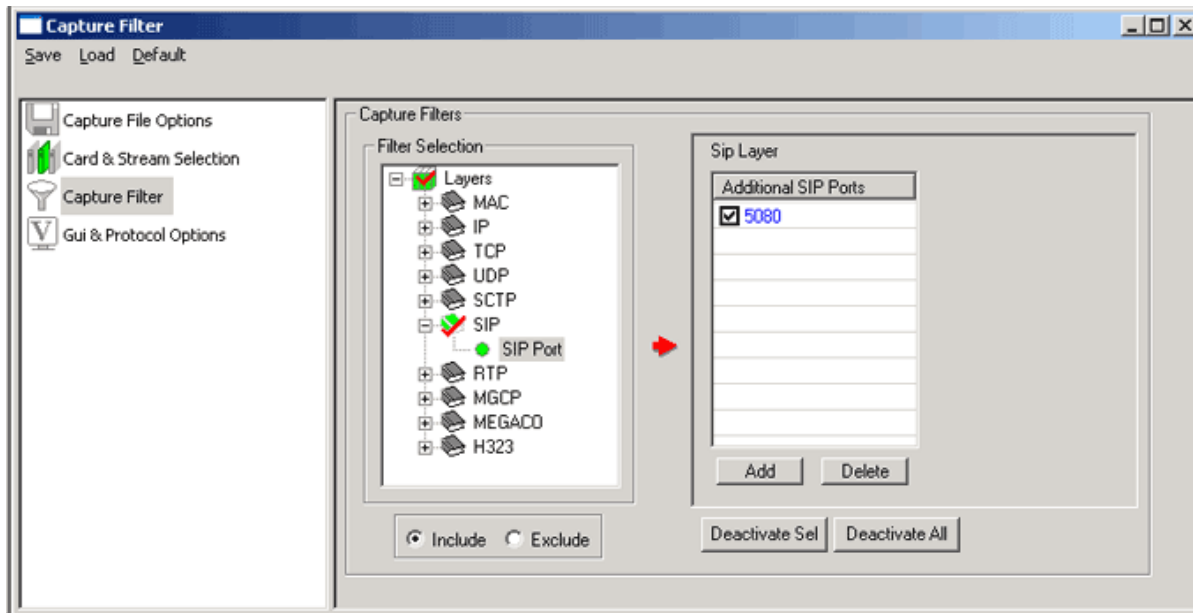


Figure 68: SIP Source and Destination Port



Note:

- If the transport method is TCP for SIP and RTP ports, then the corresponding ports are TCP source port and TCP Destination Port. Same holds for UDP.
- TCP or UDP based on the transport method is included automatically when SIP or RTP is selected.

7.4.7 RTP

Select **Filter All RTP data** option shown in the figure below to capture all RTP data.

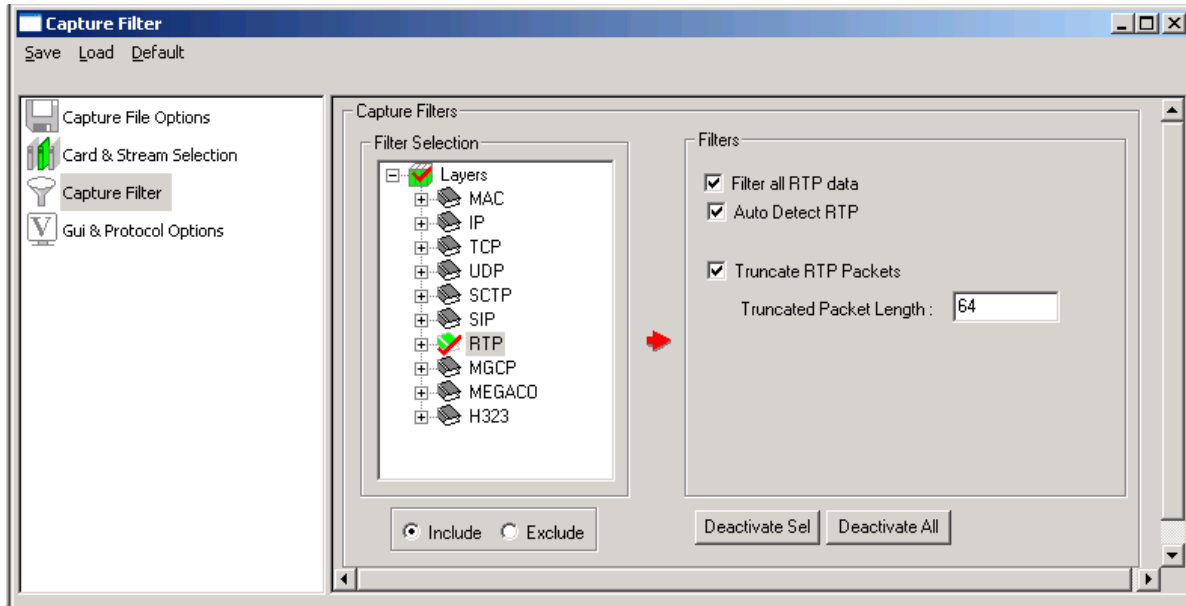


Figure 69: RTP Layer

Auto Detect RTP

Auto detect RTP is a feature by which the user can capture any RTP packets in between a particular session is in progress, if the user does not select this option then he may not be able to capture the packets which are getting transmitted especially in the case of manual call. This feature can be selected as shown in the above figure.

Example:

When we generate a manual call using [PacketGen™](#) (real-time VoIP simulator) with media, and after the call is established if you start the PacketScan™ without this feature enabled we cannot get the ongoing packets in real-time, but on the other hand if we select this option and start capturing we are able to capture the ongoing RTP packets also (though we miss out some of the SIP messages because of the delay in starting the capturing). This feature will be of more use in such cases. It is also useful in case of bulk calls as well.

If a part of RTP data is to be captured then, user can specify Additional RTP Ports as shown in the figure i.e., UDP Source/Destination Ports if the transport method is UDP or TCP Source/Destination Port if the transport method is TCP.

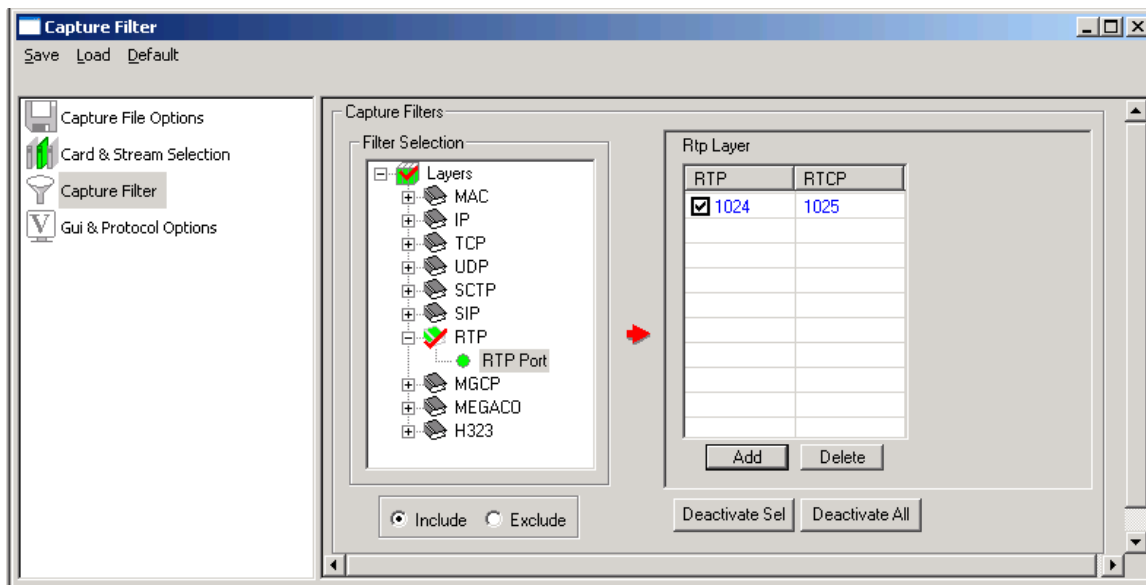


Figure 70: RTP Port

7.4.8 MGCP

Select **Filter All MGCP data** option shown in the figure below to capture all MGCP data.

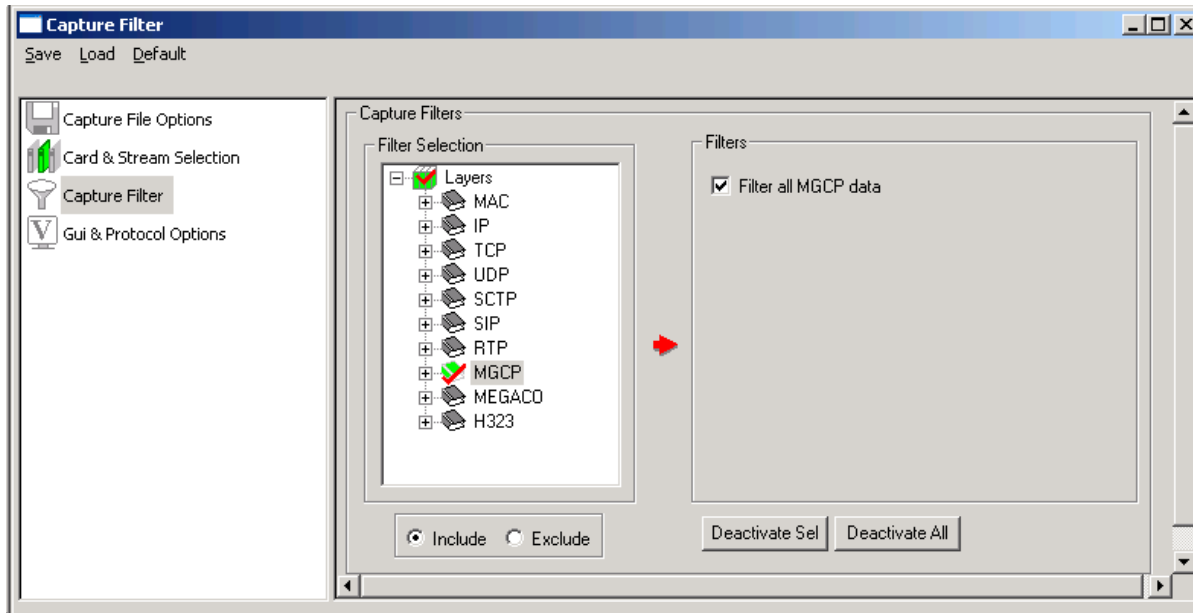


Figure 71: MGCP Layer

Further users can capture MGCP data on specified MGCP ports as shown in the figure below:

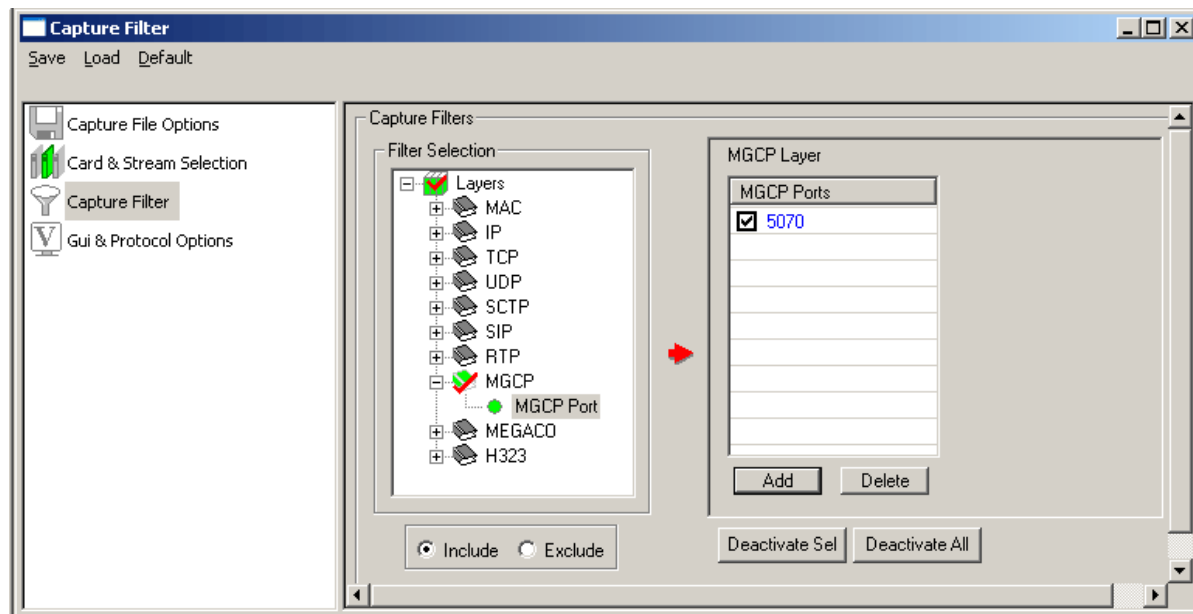


Figure 72: MGCP Port

7.4.9 MEGACO

Select **Filter All MEGACO data** option as shown in the figure below to capture all MEGACO data.

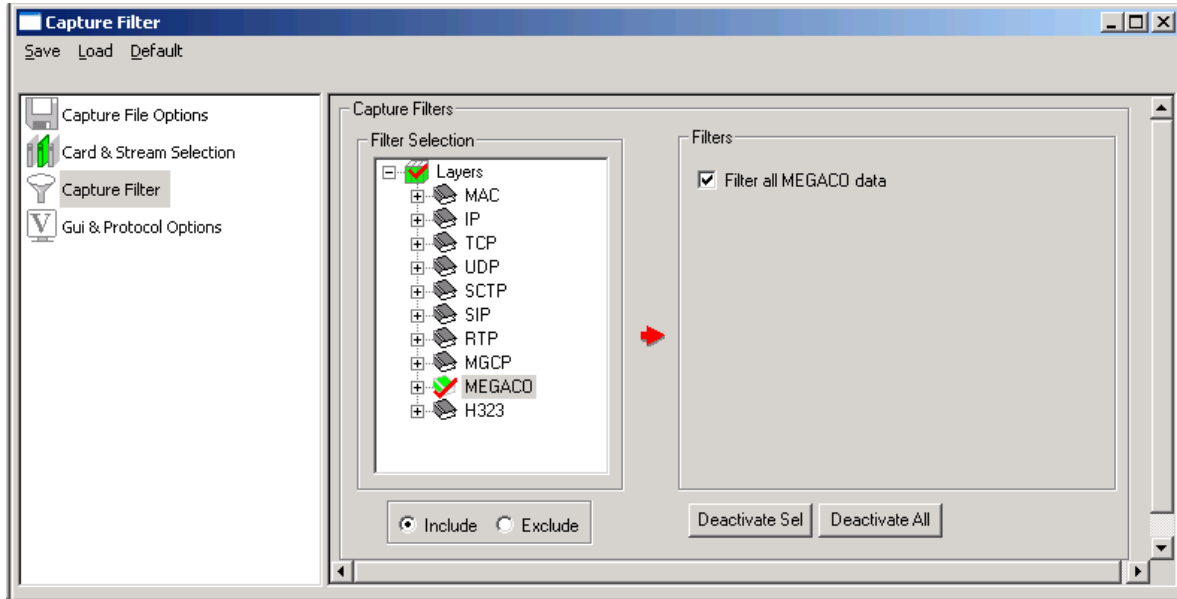


Figure 73: MEGACO Layer

Further users can capture MEGACO data as MEGACO Text or Binary as shown in the figure below:

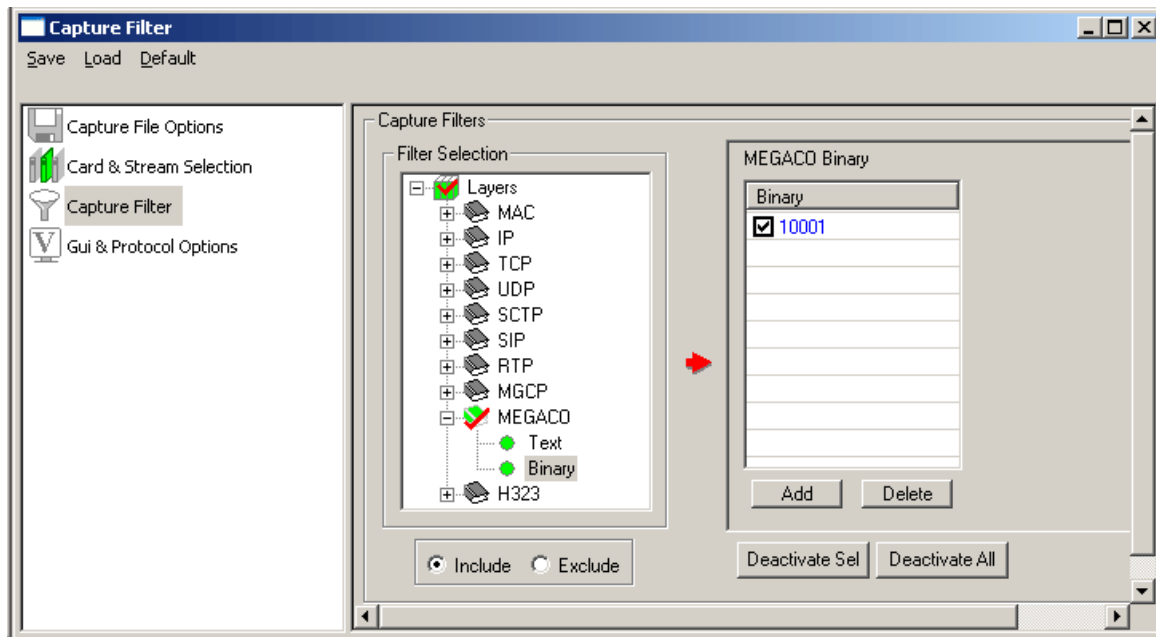


Figure 74: MEGACO Binary

7.4.10 H323

Select **Filter All H.323 data** option shown in the figure below to capture all H.323 data.

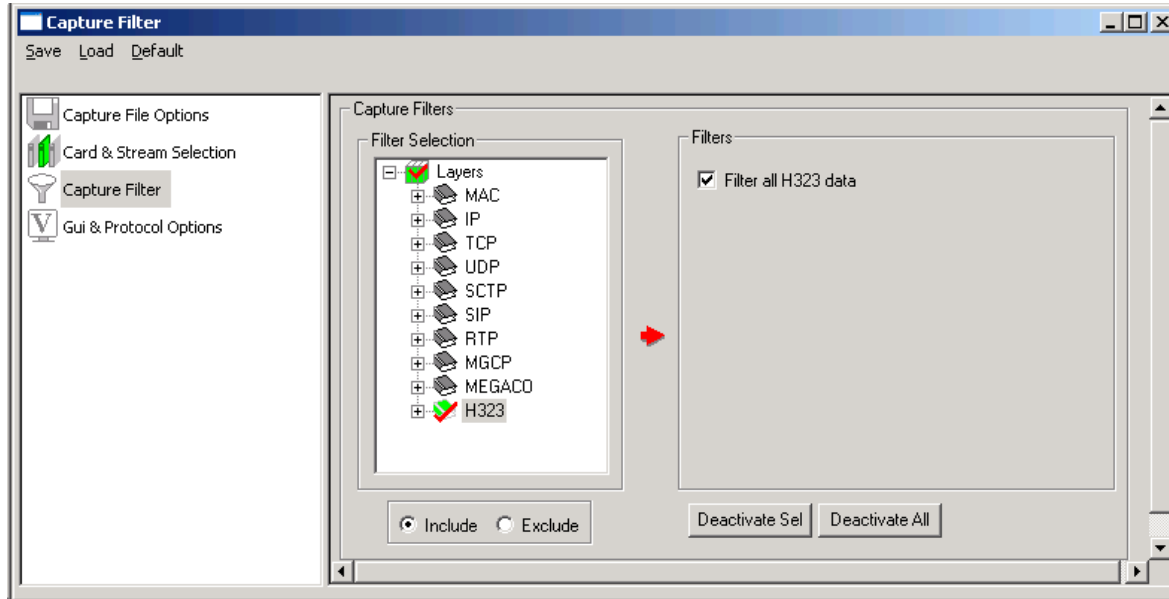


Figure 75: H.323 Layer

Further, users can capture H.323 data on specified ports H225, H245 and RAS as shown in the figure below:

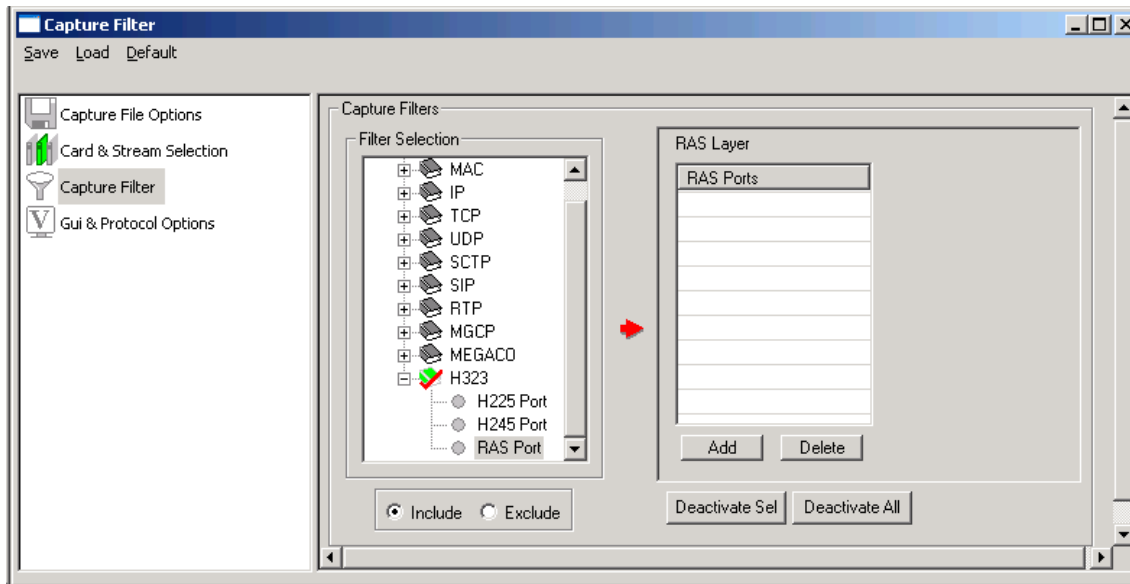


Figure 76: H.323 Ports

7.5 GUI and Protocol Options

Switches to GUI and protocol list: selecting columns, protocol standard, filtering criteria, search criteria, etc. For more information refer to [Protocol Analyzer Configuration](#).

Section 8.0 Statistics

Protocol statistics is one of the main features of protocol analyzers. The Statistics are calculated based on the protocol fields. The pane displaying statistics in PacketScan™ is as shown in the figure below:

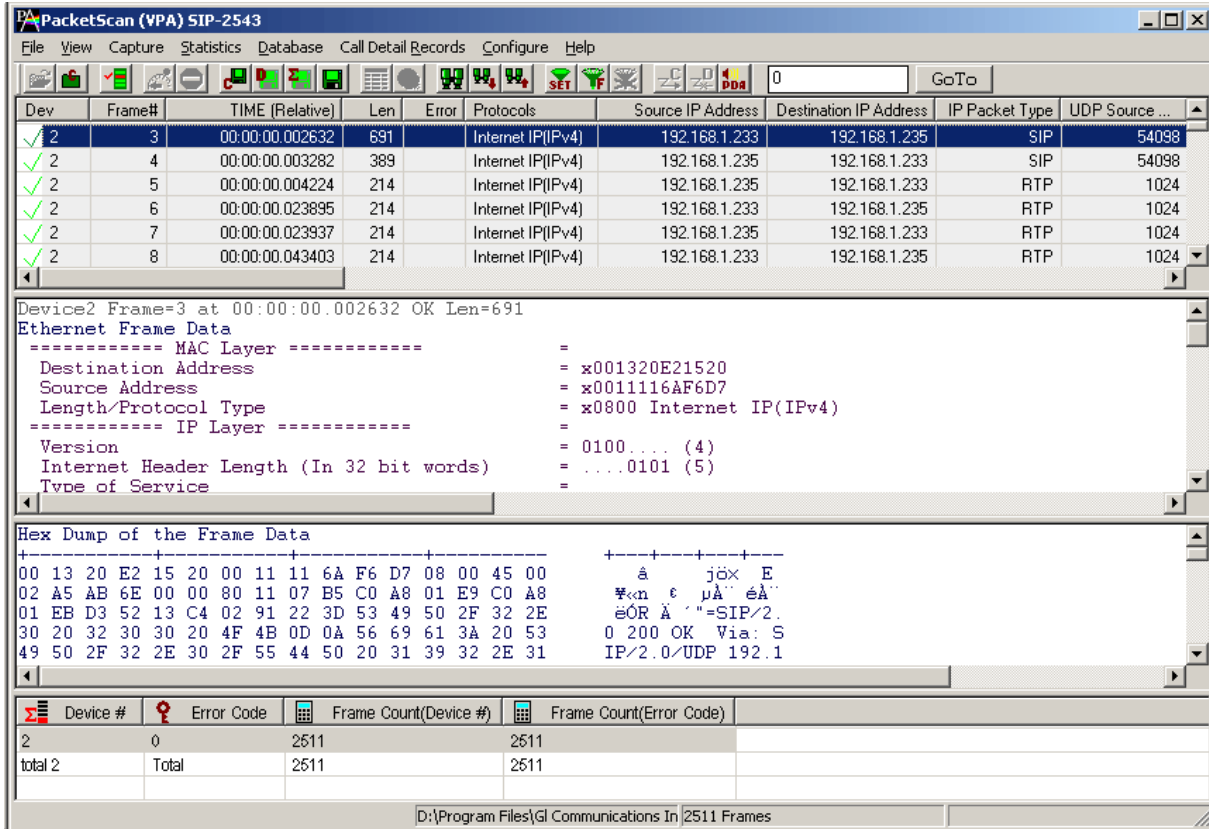


Figure 77: Protocol Analysis with Statistics View

8.1 Steps to Display Statistics

Statistics can be calculated and displayed in off-line and real-time modes.

In both cases statistics must be defined first using **'Define/Edit'** dialog as shown in the figure below, subsequently, Statistics View must be open using the **Statistics > Open Statistics View** or using **View > Define Views to Display**.

For real-time capturing, Statistics View must be open before tracing is started.

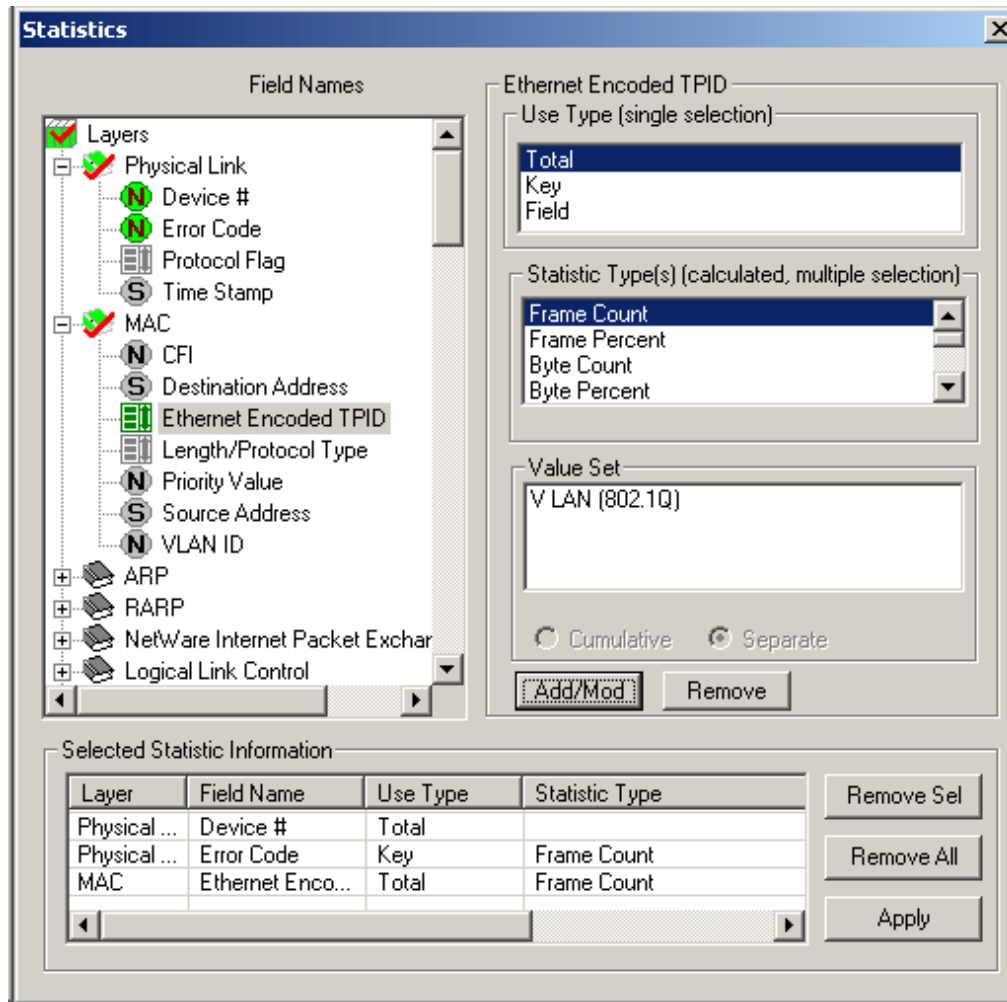


Figure 78: Statistics Definition Dialog

The statistics definition dialog has the following elements:

- **Field Names** displayed as the layer/field tree view in the upper left corner. This tree view is used to select a parameter for statistics calculation for an appropriate layer.
- **Use Type (UT)** selection list box in the upper right corner allows users to select Total, Key or Field type as statistics calculation type for each field name.
- **Statistics Type (ST)** list box allows users to select additional parameters (Frame count, Current Frames, Max, Min etc) for each of the field name selected. Selecting a parameter under this frame is a must, if the user has selected any Field Name as Use Type
- **Range List, Value Set** or **Wild Card** can be specified in the entry field below the statistics type list box to further narrow down the selection for the required statistics calculation
- **Add/Mod (Add/ Modify)** button is used to apply all the values selected for each field for calculation. On the contrary, the Remove button is used to remove the selections made for each field name

Once the **Add/Mod button** is clicked, the Selected Statistics Information pane at the bottom of the dialogue lists the conditions set for each field and provides buttons to remove the selected or all settings. All fields defined, as Total UT, Key UT or Field UT must appear in this pane to participate in statistics calculation as shown in the figure above.

8.1.1 Selecting Field Names (Step 1)

In the protocol tree view, navigate to the protocol layer to which the field item belongs and click to expand the tree and to select a field. The supported layers for the PacketScan™ and the field for respective layers will be displayed as shown in the figure below:

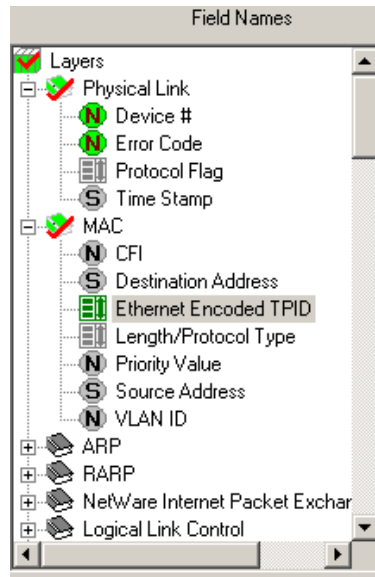


Figure 79: Selecting Filed Names

Classifying Fields under Field Names

All field names in the protocol displayed in the tree view belong to one of three types:

- Numeric
- String
- Enumerated (set)

Field names can be distinguished based on the icons representing them as shown in the figure below.

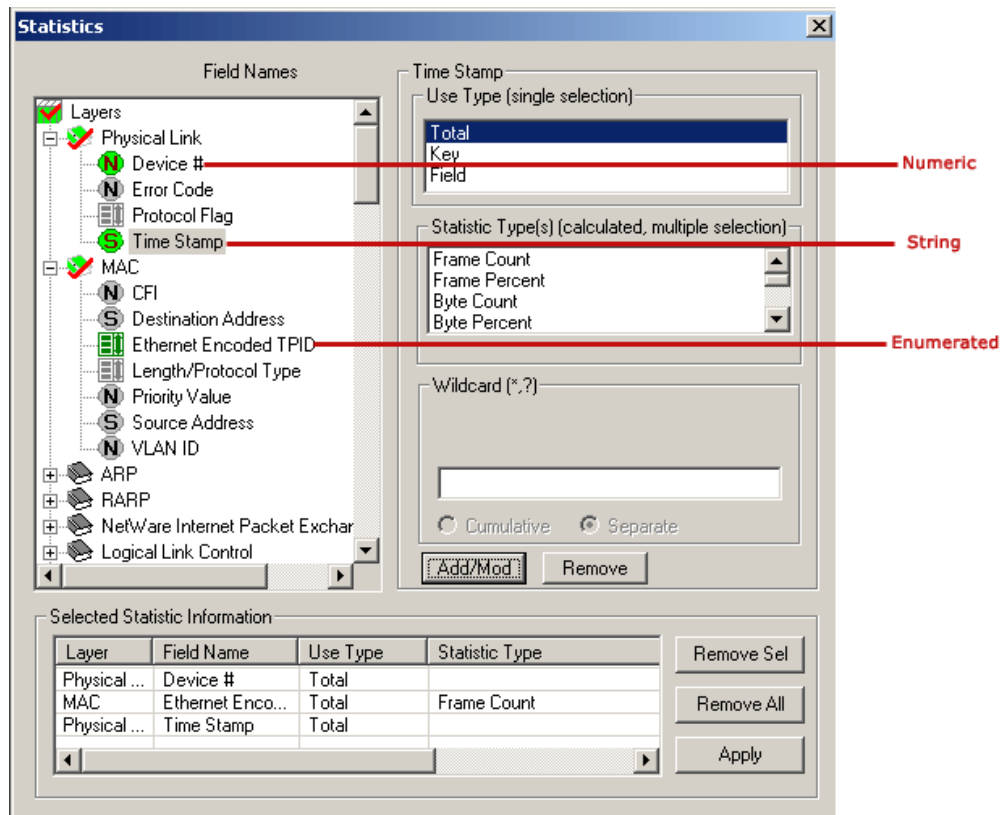


Figure 80: Field Types

8.1.2 Defining Use Type (UT) and Statistics Type (Step 2)

Use Type (UT)

The UT can be total, key or field types. Selecting proper type defines the table displayed in the Statistics View. At least one total or key UT must be defined. Total and Key UT directs creation of statistics view columns for the selected fields and also rows with unique aggregate value of Total and Key columns.

Total UT has dual role. Firstly it's used as a **Key UT**, defining rows with unique set of column values in the Statistics View. Secondly, it directs the statistics engine to display an additional row for totals (sum). The latter is similar to the sum function in the spreadsheets.

Unique set of column values means that different rows have a unique combination of values in the Key/Total columns.

Field UT defines only separate columns where the calculated Statistic Type is placed for the combination of key values.

The UT can be set as **Total, Key or Field**. A minimum of one UT must be defined for each field selected under **Field Names**.

Statistics Type (ST)

While the Use Type (UT) defines the rows in the Statistics View, the statistic type (ST) defines the columns. The following statistic types are available:

- Frame Count
- Frame Percent
- Byte Count
- Byte Percent
- Current Frames/Sec
- Current Bytes/Sec
- MAX Frames/Sec
- MAX Bytes/Sec
- MIN Frames/Sec
- MIN Bytes/Sec
- AVG Frames/Sec
- AVG Bytes/Sec
- MIN
- MAX
- SUM
- AVG

MIN, MAX, SUM and AVG should be specified only for numeric fields. As explained in [Classifying Fields under Field Names](#) all the fields belong to one of the following categories: numeric, string and enumerated (sets). When the same ST is specified for multiple fields, a new column is created in the statistics view for each field name.

Additional columns consume resources and slow down statistics calculation process. Only MIN, MAX, SUM and AVG columns will be different for different fields, other columns like Frame Count, Frame Percent, Byte Count, etc. will display the same information and will not be useful.

8.1.3 Update Selected Statistics Information List (Step 3)

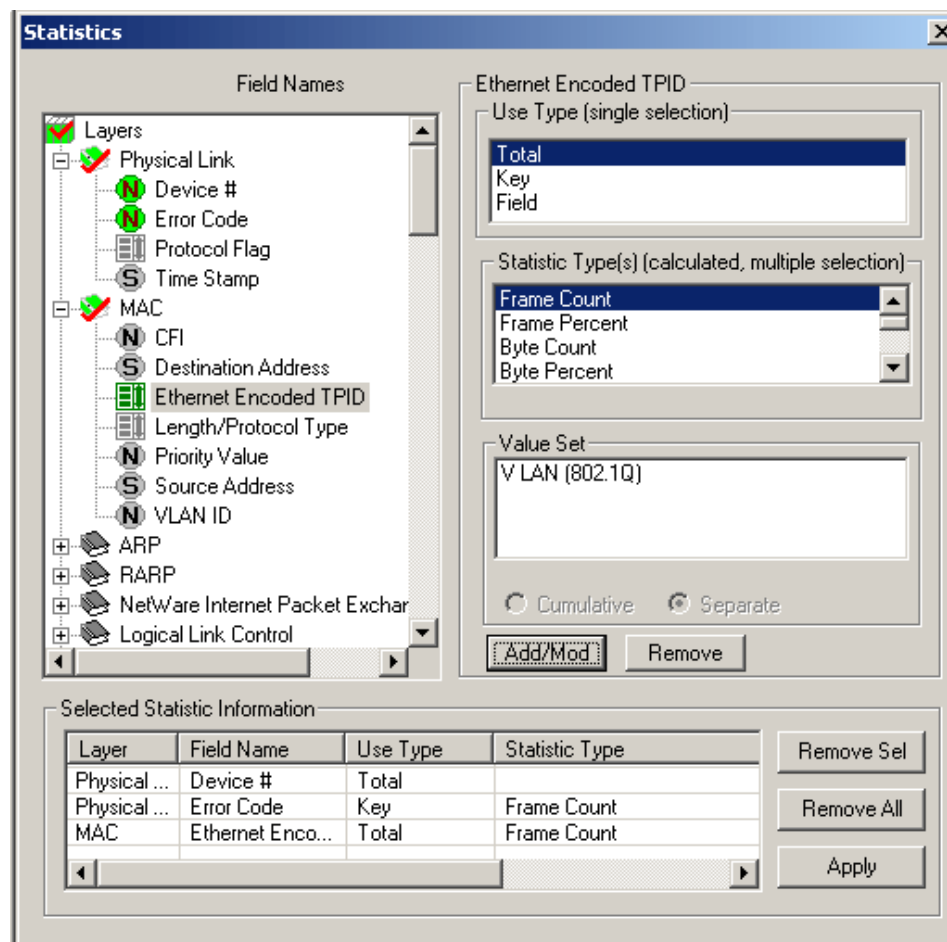


Figure 81: Selected Statistics Information List

After selecting the required Use Type and statistics Type, click **Add/Mod** button to add the selected statistics in the information list.

Click **Apply** shown in the figure above to activate the newly defined statistics information. If the **Statistics Definition** dialogue is closed without clicking on **Apply** button, it will discard all the newly defined statistics.

8.1.3.1 Example 1 – Statistics with a Key UT

Key UT: This option creates a unique column in the Statistics View, and a row for each unique value associated with this field. For example,

- 1) Open the sample trace file in offline analysis mode.
- 2) To define statistics, click **Statistics > Define/Edit**.
- 3) Select the field 'Protocol Flag' under physical layer, and choose **Key UT** as the use-type, and **Frame Count** as statistics type.
- 4) Select the available Value Set for the field Protocol Flag.
- 5) Click **Add/Mod button** and then click **Apply**. The selected statistics pane appears as shown in the figure below.

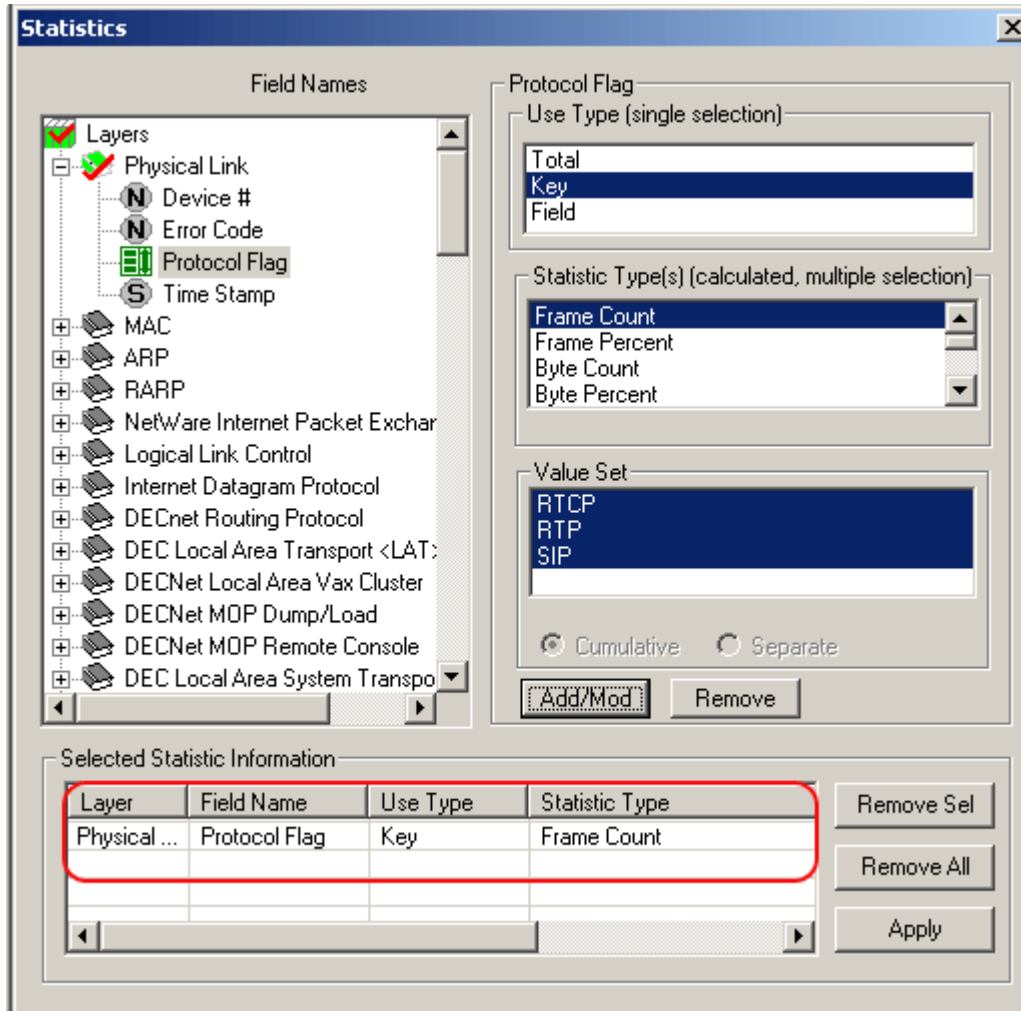


Figure 82: Define Statistics with a Key UT

6) Click **Statistics > Open Statistics View** to open the Statistics View as shown in the figure below:

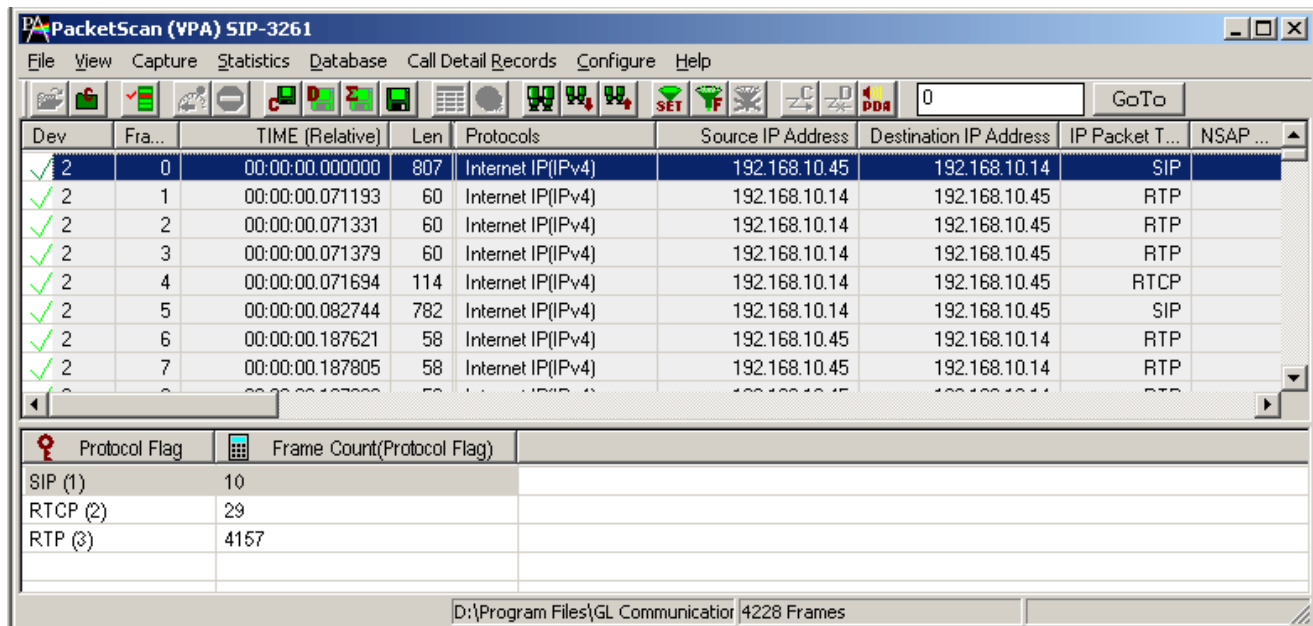


Figure 83: Statistics Field set as Key UT

In the above example, unique rows are defined based on field (Protocol Flag) selected as Key UT and for the selected value set, and columns are defined based on the statistics type (frame count for each protocol flag) selected for this key UT.

8.1.3.2 Example 2 – Statistics with a Total and a Key

Total UT: This option not only makes the column a key column but also creates an additional total row for each unique value of the column.

Total UT and Key UT values combined together uniquely define a row in the Statistics View.

Key UT defines a unique column value that can be used for calculating a Statistic Type like frame count, sum, avg, min, max, etc. This calculated statistics will be displayed only if all the key UT values are unique and are numeric else the Statistics View displays just the word 'Total' in the row dedicated for the same purpose. For example –

- 1) Open the sample trace file in offline analysis mode.
- 2) To define statistics, click **Statistics > Define/Edit**.
- 3) Select the field 'Device #' under physical layer, and choose **Total UT** as the use-type and then select **Frame Count** as statistics type.
- 4) Click **Add/Mod** button and then click Apply.
- 5) Select the field 'Payload Type' under RTP layer, and then select **Key UT** as the use-type. Also, select the available value set for the payload type.
- 6) Click **Add/Mod** button and then click **Apply**. The selected statistics pane appears as shown in the figure below.

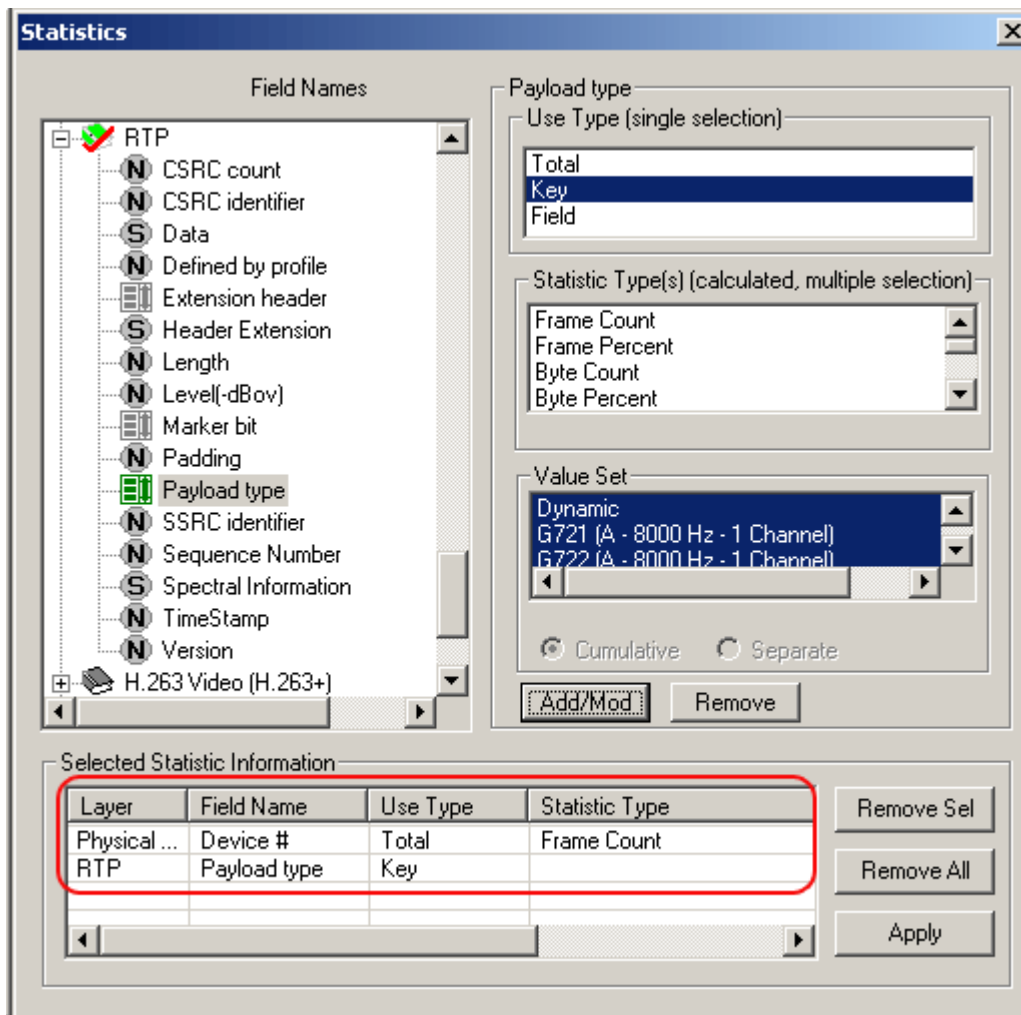


Figure 84: Define Statistics with a Total & Key UT

7) Click **Statistics > Open Statistics View** to open the Statistics View as shown in the figure below:

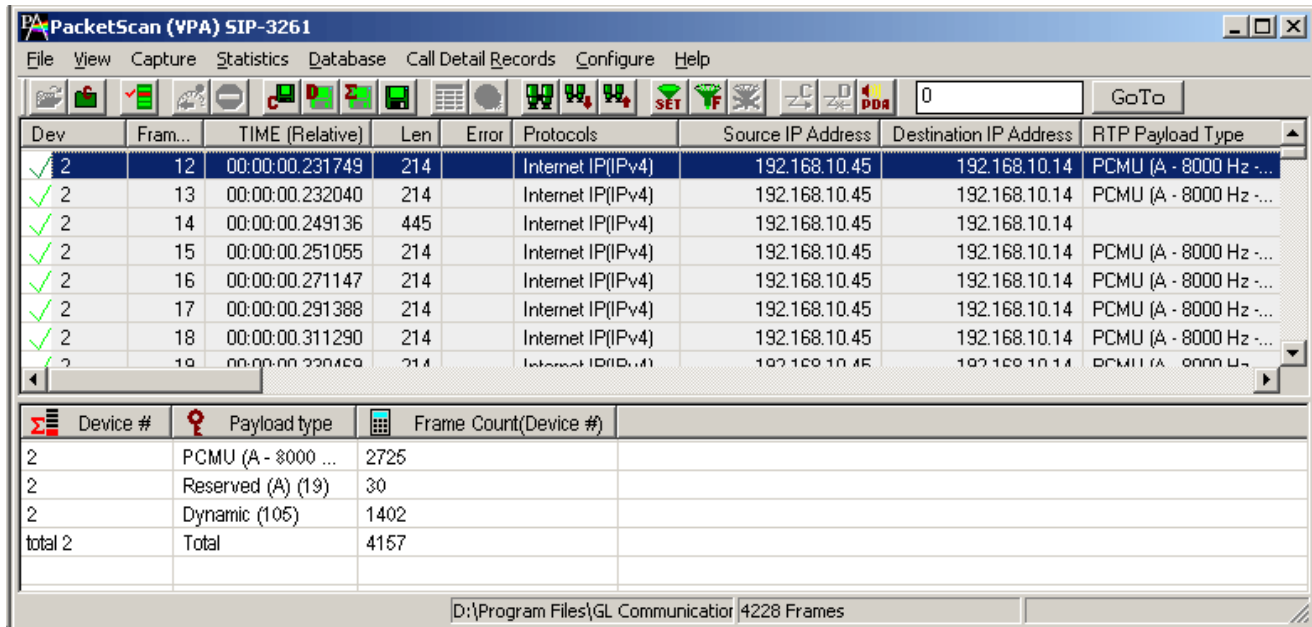


Figure 85: Statistics with Total and Key

In the above example, unique rows are defined based on field selected as the Key UT (payload type values), and columns are defined based on the statistics type (frame count for each device) selected for this Total UT. Since the device is selected as Total UT, additional row displaying the total frame count per device are displayed.

8.1.3.3 Example 3 – Statistics Total and Field UT

Field UT: This option defines additional columns for the parameters selected under **Statistics Type** frame. **Field UT** creates just an additional column for the selected field. However, differently from Key UT and Total UT, the Field UT does not create additional rows for each unique value associated with the field. For example,

- 1) Open the sample trace file in offline analysis mode.
- 2) To define statistics, click **Statistics > Define/Edit**.
- 3) Select the field **'Protocol Flag'** under physical layer, and choose **Total UT** as use-type.
- 4) Click **Add/Mod** button.
- 5) Select Source Port under **'UDP'**, and choose **Field UT** as use-type. To get the frame count for with source port ranging from 5000 to 800, select **Frame Count** as the **Statistics Type** and enter the '5000-8000' in the range list.
- 6) Click **Add/Mod** button and then click **Apply**. The selected statistics pane appears as shown in the figure below.

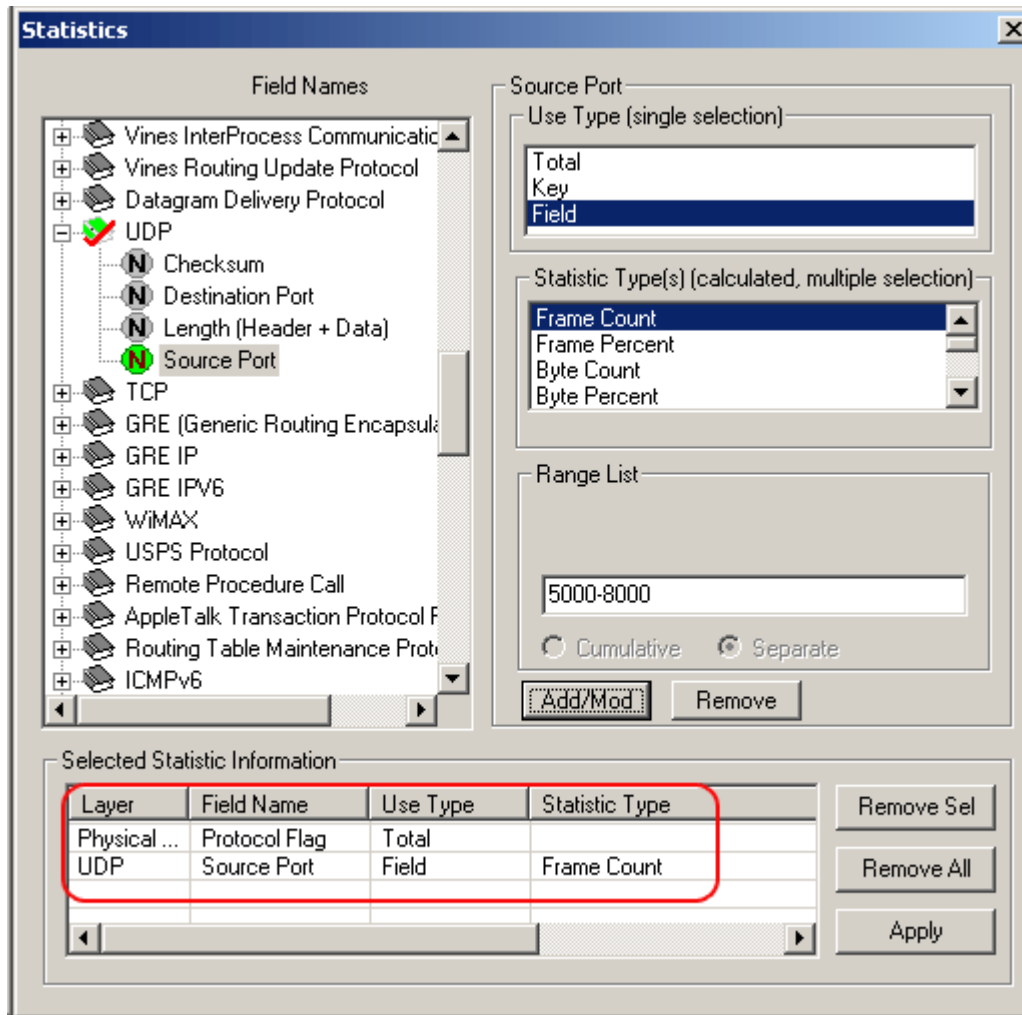


Figure 86: Define Statistics with a Total and Field UT

7) Click **Statistics > Open Statistics View** to open the Statistics View as shown in the figure below:

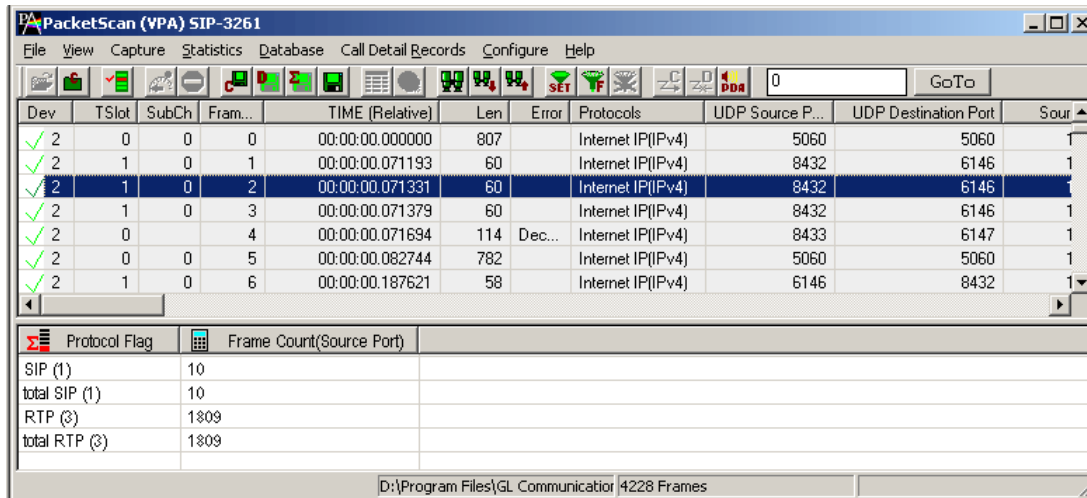


Figure 87: Statistics with a Total and a Field

In the above example, we have **Protocol Flag** set as Total UT, **UDP Source Port** set as Field UT along with **Frame Count** as Statistic Type. The statistics view shows the total number of frames associated with protocol type is displayed.

8.1.4 Ranges, Wildcards and Enumerated Value Sets

Depending on the field type additional criteria may be specified to include only frames with the matching:

- Ranges for numeric fields
- Wildcards for string fields
- Sets of values for enumerated fields

Ranges

Depending on the field type a range list can be specified for numeric fields as space separated numbers or ranges of numbers. For example, the range list 1 12-15 4-6 will include fields with the following integer values: 1, 4, 5, 6, 12, 13, 14, and 15. Frames with all other values will be excluded from statistics, see the below figure below.

Ranges can be specified only for numeric fields.

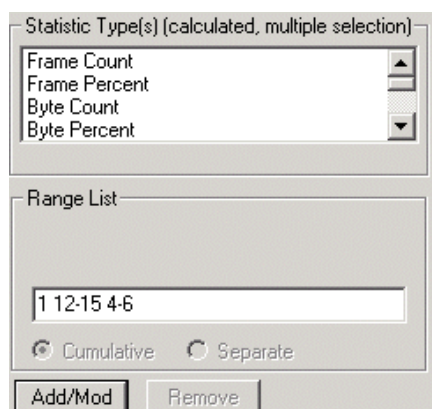


Figure 88: Range List for Numeric Fields

Wildcards

Valid string field values can be specified using wildcard characters '*' (asterisk) and '?' (Question mark).

'*' means zero or more characters of any value

'?' means any single character

'301*', for example, means any string starting with '301'

'301*5*' means any string starting with '301' and containing '5' at any position after '301'

'*3?4?5*' means a string containing '3' followed by any single character followed by '4' followed by any single character followed by '5' followed by zero or more characters.

Wildcards are valid only for string fields.

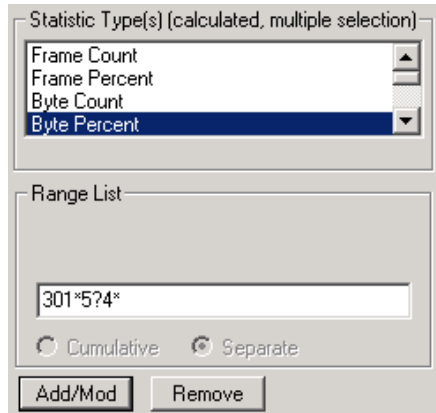


Figure 89: Wildcards for String fields

Value Sets

Enumerated fields can have a fixed set of values with associated name. Some of these names can be selected to narrow down the statistics as shown in the figure below.

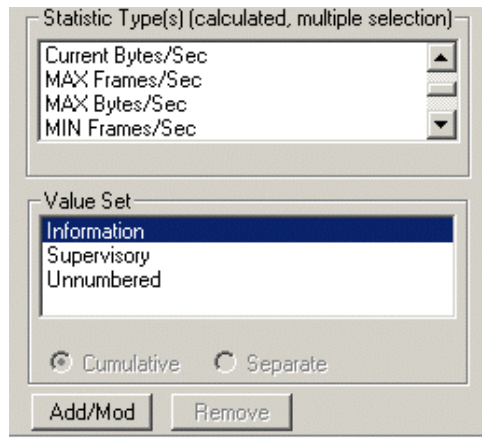


Figure 90: Specifying Value Sets

8.1.5 Modifying and/or removing configured statistics

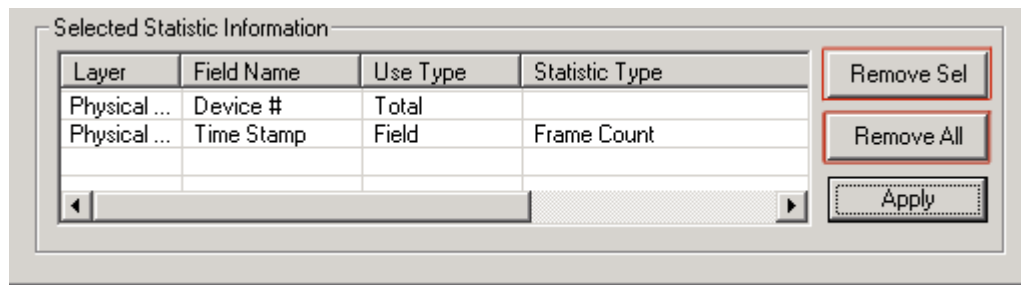


Figure 91: Modify/Remove some or all statistics

In the process of the statistics definition one can go to the **Selected Statistics Information** list control and select a line by clicking on it. This will cause automatic repositioning of the tree view and statistics information for the selected field to be displayed in the UT, ST and **Range/Wildcard/Value Set dialog controls**. User can then modify the information and click **Add/Mod** button to make the changes effective as shown in the figure of the **Selected Statistics Information list**.

Click **Remove Sel** button to remove selected lines from the criteria.

Click **Remove All** to disable statistics.

8.2 Opening and Closing Statistics View

Statistics View can be opened and closed at any time during the offline analysis. Opening a trace view can be a lengthy process for large traces when statistics are enabled.

The Statistics View for an on-line tracing must be opened before real time analysis is started.

To open the Statistics View select **Statistics > Open Statistics View** menu item as shown in the figure below.

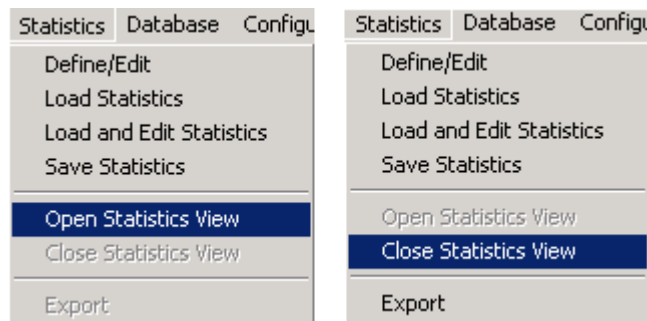


Figure 92: Opening and Closing Statistics View

To close the Statistics View, select **Statistics > Close Statistics View** menu item.

8.3 Loading Statistics

Select, **Statistics > Load Statistics** to load the saved statistics criteria as shown in figure below. One can load the statistics from a previously saved Statistics Definition File (*.ini).

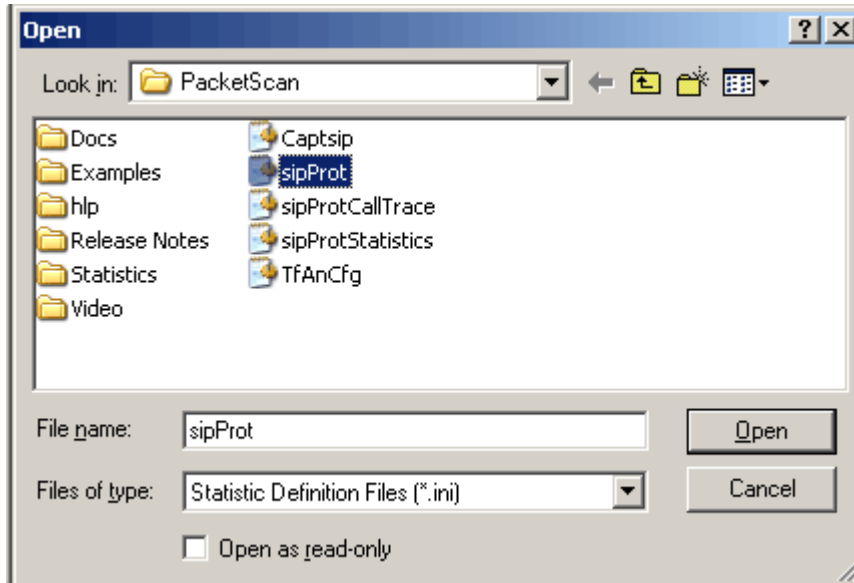


Figure 93: Loading Statistics

8.4 Load and Edit Statistics

Select **Statistics > Load and edit statistics** menu item to load the saved statistics and to modify the statistics information.

8.5 Save Statistics

Select **Statistics > Save Statistics** to save the statistics. **Save Statistics** saves the file with statistics criteria. Enter the desired file name and click **Save**, the statistics file is saved with the extension ".ini" (Statistics Definition Files).

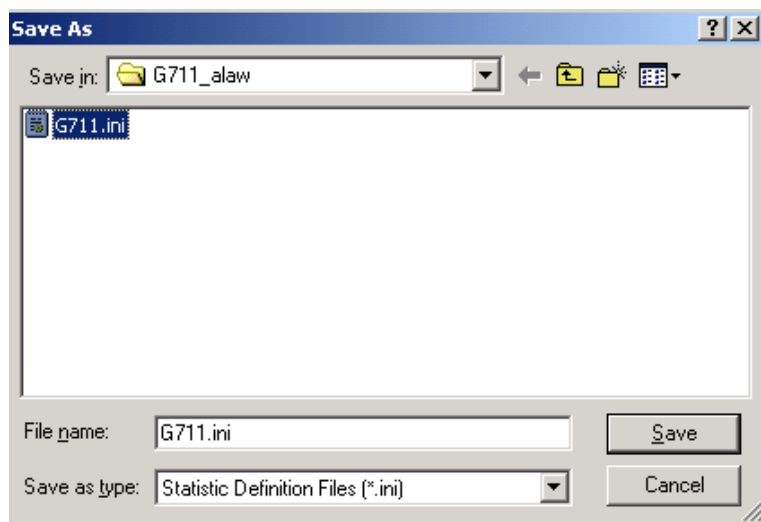


Figure 94: Save Statistics as Filename

8.6 Export Statistics

Select **Statistics > Export Statistics** to export the Statistics View into a file with extension 'sef' (Statistics Export Files) for subsequent import into a database or spreadsheet.

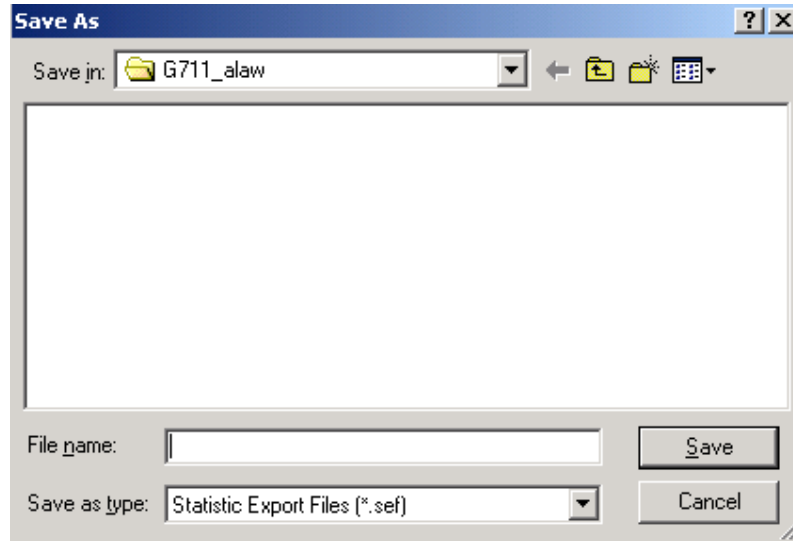


Figure 95: Export Statistics as Filename

(Intentional Blank Page)

Section 9.0 Configuring for Call Detail Records

The objective of call detail record is to isolate call specific information for each individual call from the captured data and display the information in an organized fashion. The call-detail records are displayed as shown in the figure below.

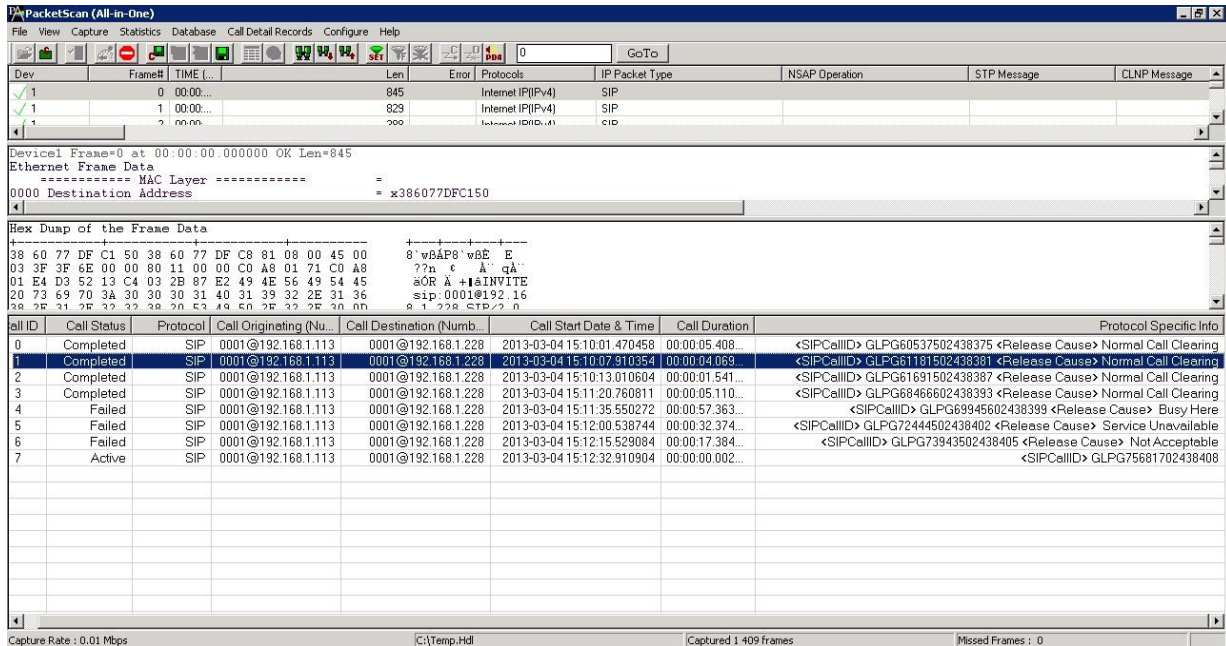


Figure 96: Call Detail Records View

9.1 Build Call Detail Record

Select **Call Detail Record > Build Call Detail Record** menu item as shown in the figure below. Build Call Detail Record is checked for the activation of call trace application. This should be done before starting the real-time capture or before opening an **hdl** file in offline mode.

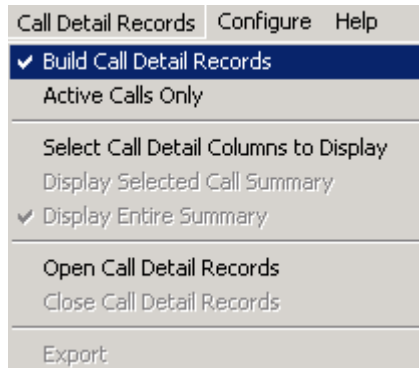


Figure 97: Build Call Detail Record

9.2 Active Calls Only

Select **Call Detail Records > Active Calls** Only menu item to view only active calls.

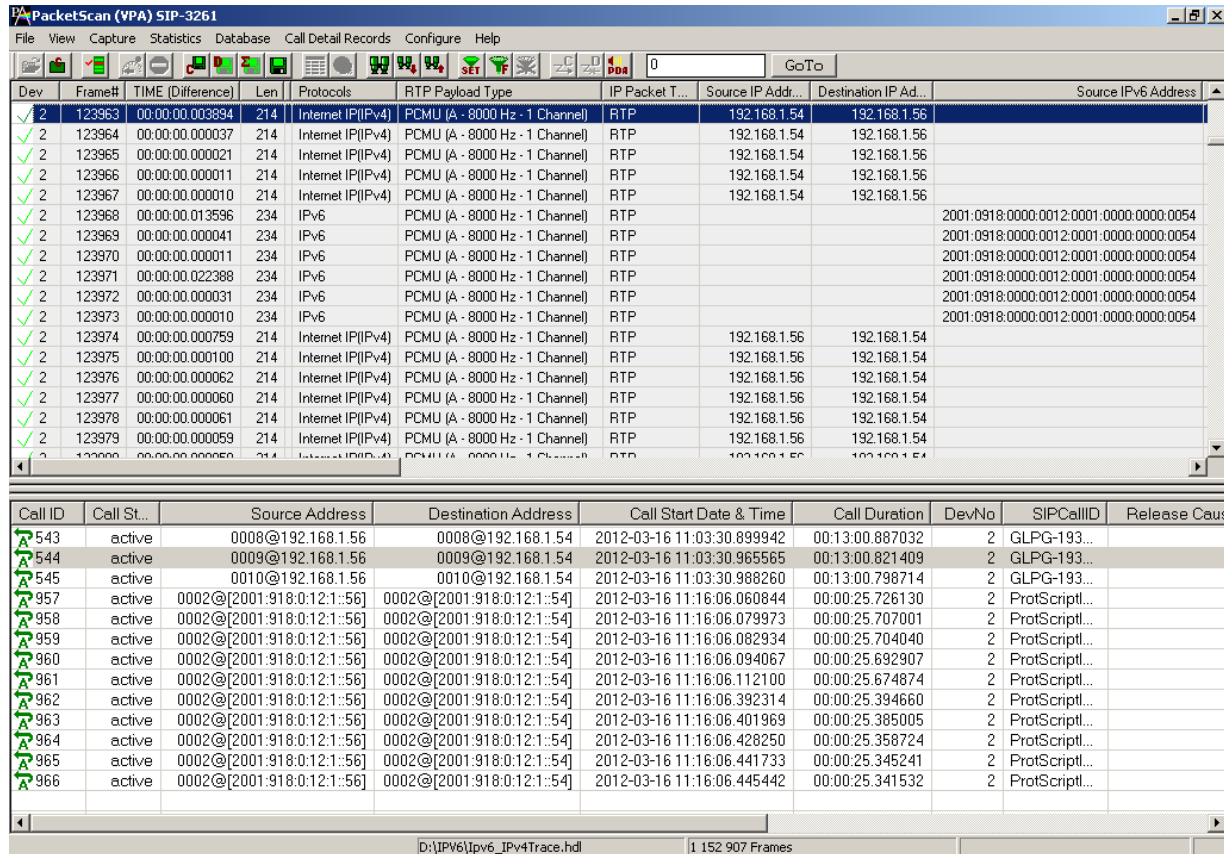


Figure 98: Display Active Calls Only

9.3 Open Call Detail Record

Select **Call Detail Record > Open Call Detail Record** menu item. Call Detail Record View can be opened and closed in off-line trace viewing any time.

To open Call Detail Record View

- Select **Call Detail Record > Open Call Detail Records** menu item or
- Click **View > Define Views** menu item.

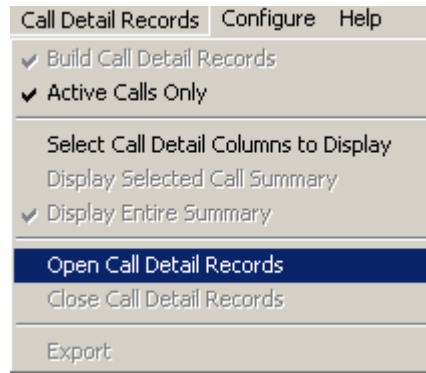


Figure 99: Open Call Detailed Record

Note:

- Build Call Detail Record menu item should be checked before opening Call Detail Records view.
- If the Call Trace view is selected from View>Define Views to Display menu item without checking Build Call Detail Record, a warning message is displayed as shown in the figure below.
- Call Detail Record View for on-line tracing must be opened before on-line tracing is started.

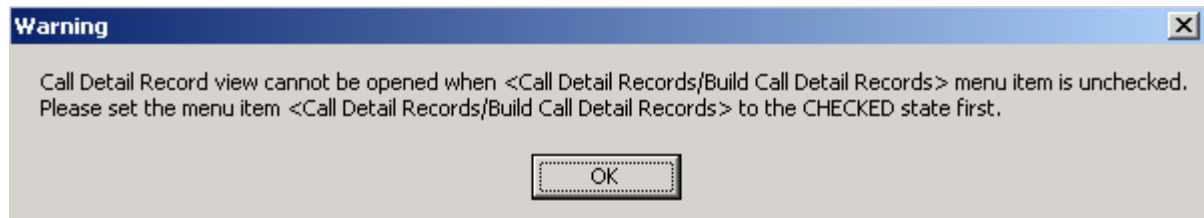



Figure 100: Warning Message


9.3.1 Active and Completed Calls

Call ID refers to the identification of each call. There are icons visible to the left of these Call ID numbers

Active Calls:





Active calls () are marked in green and the call status is specified as Active. An arrow is seen above the letter A, which indicates the direction of the call.

Completed Calls:

Completed calls () are marked in gray and the call status is specified as completed. An arrow is seen above the symbol (-), which indicates the direction of the call.

9.3.2 Call Duration

Call duration is calculated for completed calls. The total time for the call from start to end is calculated as shown in the figure below.

Call ID	Call Status	Source Address	Call Duration	DevNo
 0	completed	a001@192.168.10.32	00:00:00.100133	1
 1	completed	a001@192.168.10.32	00:00:00.011209	1
 2	completed	a001@192.168.10.32	00:01:00.113419	1
 3	active	a001@192.168.10.32	00:01:20.369678	1

Capture Rate : 0.00 Mbps C:\Temp.Hdl Captured 30 frames Missed Frames : 0

Figure 101: Call Duration

9.3.3 Find CDR

This feature allows you to search for a particular call from the captured traces. Right-click on the Call Detail View and select **Find CDR** option to open the screen as shown below:

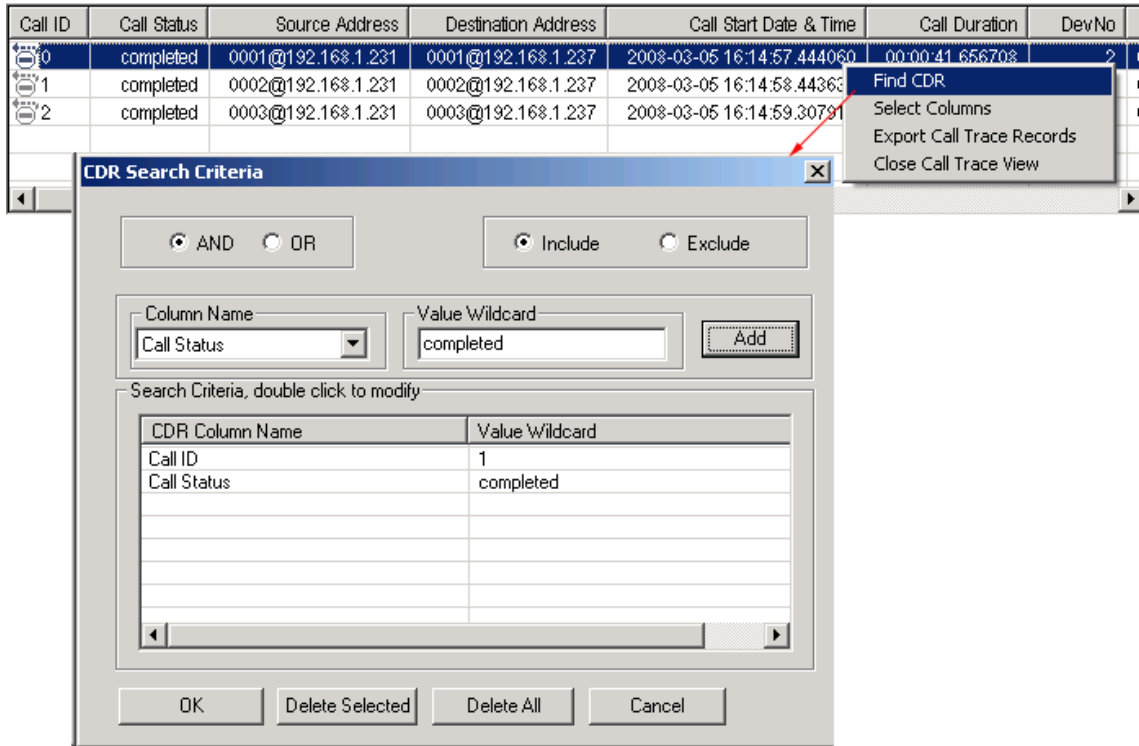


Figure 102: Find CDR

Select the parameters from the **Column Name** and enter the criteria in the **Value Wildcard** text box. The parameters satisfying the conditions may be included or excluded from the result using the **Include** or **Exclude** options. All the selected criteria logically use **OR** or **AND** operations. A frame is filtered if at least one criterion matches (OR logic), or each criteria matches (AND logic).

Wildcards

All values in Call Detail View are considered as string. To search for a specific call, valid string field values can be specified using wildcard characters '*' (asterisk) and '?' (question mark)

'*' means any zero or more characters

'?' means any single character

'301*', for example, means any string starting with '301'

'301*5*' means any string starting with '301' and containing '5'

'*3?4?5*' means string containing '3' followed by any single character followed by '4' followed by any single character followed by '5'.

Wildcards are valid only for string fields.

For example, to search for calls with call status 'completed' enter the value for Call Status parameter in the wildcard textbox as 'completed'.

Click **Add**, and then click **OK** to exit the window.

This presents the call detail view with **Next & Prev** navigation button to navigate through records and find the calls matching the criteria as shown below.

Call ID	Call Status	Source Address	Destination Address	Call Start Date & Time	Call Duration	DevNo
0	completed	0001@192.168.1.231	0001@192.168.1.237	2008-03-05 16:14:57.444060	00:00:41.656708	2
1	completed	0002@192.168.1.231	0002@192.168.1.237	2008-03-05 16:14:58.443636	00:00:41.865879	2
2	completed	0003@192.168.1.231	0003@192.168.1.237	2008-03-05 16:14:59.307919	00:00:42.015382	2

Off-line Viewing D:\Program Files\GL Communica 9581 Frames

Figure 103: Specify CDR criteria

9.4 Select Call Detail Columns to Display

Select **Call Detail Records > Select Call Detail Columns** to Display menu item as shown in the figure below. This contains a list of possible Columns. Here we can select the columns of interest using ctrl key and click **OK**.



Note:

The Columns can also be selected after opening the Call Data Record view by right-clicking on pane and choosing 'Select Columns' option.

Call ID	Call Status	Source Address	Destination Address	Call Start Date & Time	Call Duration
0	completed	test4@192.168.10.45	test3@192.168.10.14	2009-10-05 14:20:22.202295	00:00:28.004663

Find CDR
 Select Columns
 Export Call Trace Records
 Close Call Trace View

Call Detail Records Configure Help

- Build Call Detail Records
- Active Calls Only
- Select Call Detail Columns to Display
- Display Selected Call Summary
- Display Entire Summary
- Open Call Detail Records
- Close Call Detail Records
- Export

Select Call Trace Columns to Display

- Call ID
- Call Status
- Source Address
- Destination Address
- Call Start Date & Time
- Call Duration
- DevNo
- SIPCallID
- Release Cause
- CRV
- Conference ID
- CallType
- CallIdentifier(GUID)
- SrcIPAddr
- DestIPAddr

OK Select All Deselect All Cancel

Figure 104: Select Call Trace Columns to Display

Call ID details, the calling status whether the call is active or completed, calling number, called number, call duration, release cause, device number, SIP Call ID are shown in the Call Detail View.

Users have the option to select the Call Detail Records information (along with frame summary and frame octets) to be sent over TCP/IP to a central database. For more details refer to [Connecting to Remote Database](#)

9.4.1 Call Detail Records View

The following call record details are available in the Call Detail View.

- **Call ID** – Locally generated unique call number to identify a call. Represented as an integer.
- **Call status** – the status of a call as either active or completed.
- **Source Address** – Callers URL engaged in a SIP Call.
- **Destination Address** – caller’s URL engaged in SIP Call.
- **Call Start Date and Time** – the date (Y/M/D) and the time at which the call was made.
- **Call duration** – duration of the completed call.
- **Device number (Dev No)** – device number on which the call was captured.
- **SIP CallID** – Call Id of the SIP Call established
- **Release Cause** – call termination cause
- **CRV** – call reference value
- **Conference ID** – Conference id present in H225 Call Layer of a H.323 message.
- **CallType** – information about point-to-point Vs point-to-multipoint call
- **Call Identifier** – call identifier of a H.323 Call.
- **SrcIPAddr** – address of a source node that uniquely identifies the source computer while participating in LAN/WAN communication.
- **DestIPAddr** – address of a destination node that uniquely identifies the source computer while participating in LAN/WAN communication.

9.5 Display Selected Call Summary

Select the desired call in the Call Detail View and select **Call Detail Records > Display Selected Call Summary** menu item to view only records that belong to the selected call.

Also double click on the specific call in the Call Detail Record view pane to view the summary of the selected call.

9.6 Display Entire Summary

Select **Call Detail Records > Display Entire Summary** menu item to view the entire summary of the calls.

9.7 Closing Call Detail Record

Call Detail Record can be closed from the **Call Detail Record>Open & Close Call Detailed Record** menu item as shown in the figure below or by choosing **Close Call Trace View** option by right-clicking on call detail view.

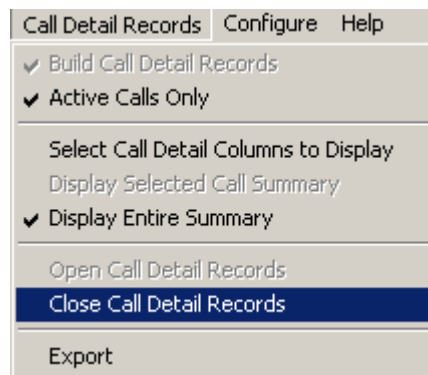


Figure 105: Close Call Detailed Record

9.8 Export Call Detail Records

Select **Call Detail Records > Export** menu item or right-click on the call detail view and choose **Export Call Trace Records** option to open the window as shown in the figure below to export the call details into a file. It exports the trace file details with extension name "cte" for subsequent import into a database or spreadsheet.

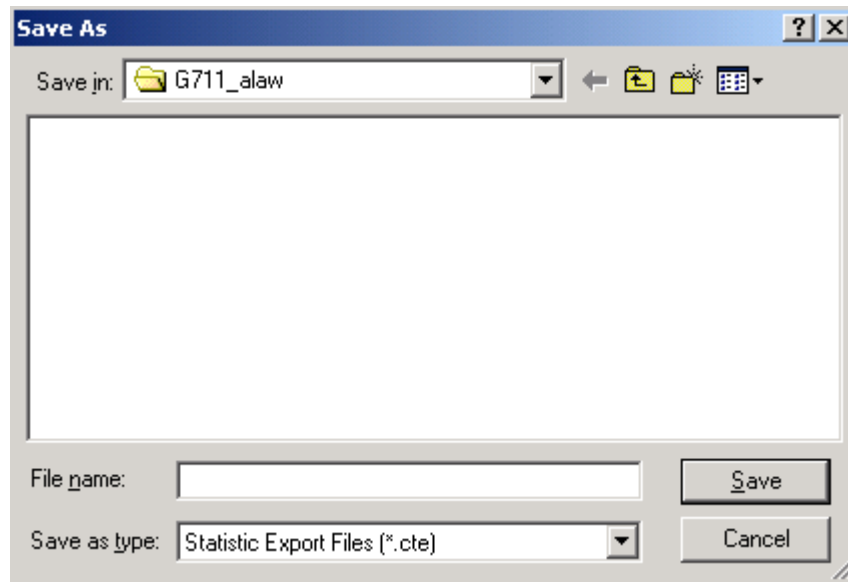


Figure 106: Export Trace File

(Intentional Blank Page)

Section 10.0 Protocol Analyzer Configuration

This window provides a consolidated interface for all the important GUI and Protocol settings required in the analyzer. This includes various options such as protocol selection, startup options, stream/interface selection, filter/search criteria and so on.

Select **Configure > Protocol and GUI** from the main menu, to open the screen as shown in the figure below.

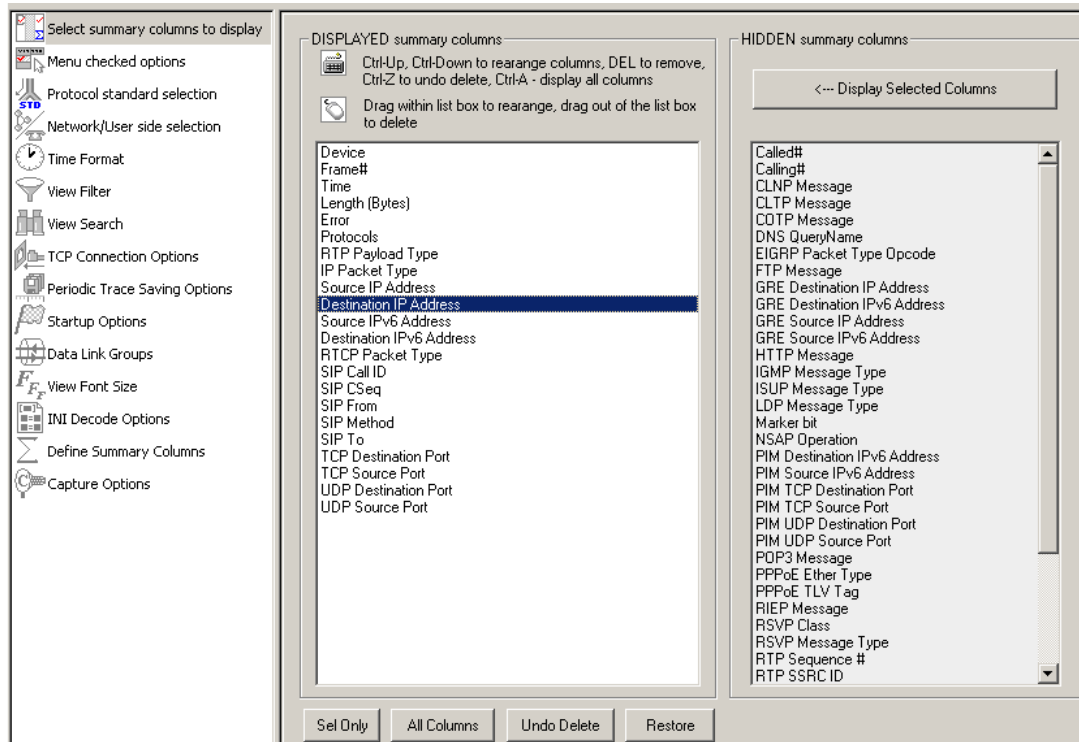


Figure 107: Protocol and GUI option

Additionally, user can save the configuration settings done in any of these options to a file or just revert to the default values by using the following menu options:

Menu Options

Save: Select **Save** from the menu to save the configuration settings for any of the options to an Analyzer Configuration File (*.ACF) as shown in the figure below.

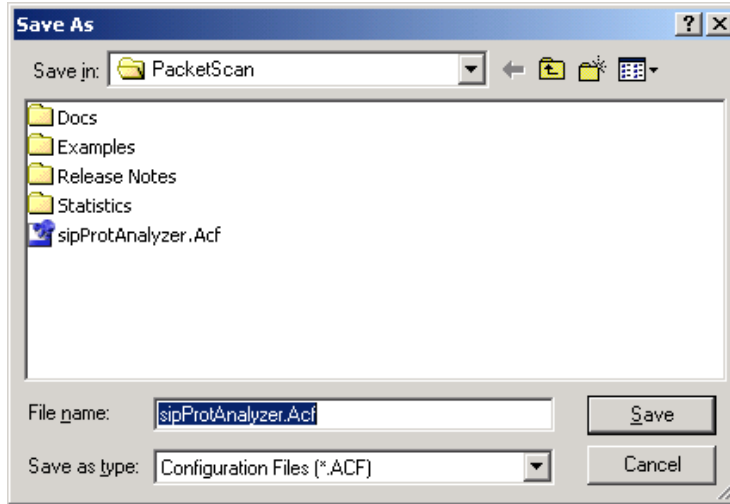


Figure 108: Save As

Load: Select Load to load the previously saved *. ACF file from the location where this file was saved as shown in the figure below.

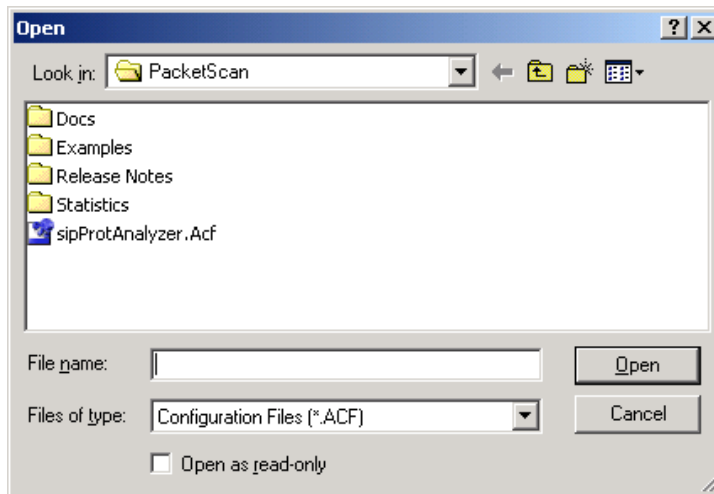


Figure 109: Load Option

Default: Select Default from the menu to revert back to the default settings.

10.1 Select summary columns to display

For more information on this, refer to section [Summary Column Selection](#).

10.2 Menu Checked Options

This list the following two options

- Select **View > Latest Frame/Packet** check box to display the latest frame in the Summary View
- Select **Enable Periodic Trace Saving** check box to save the settings of **Periodic File Saving Specification**

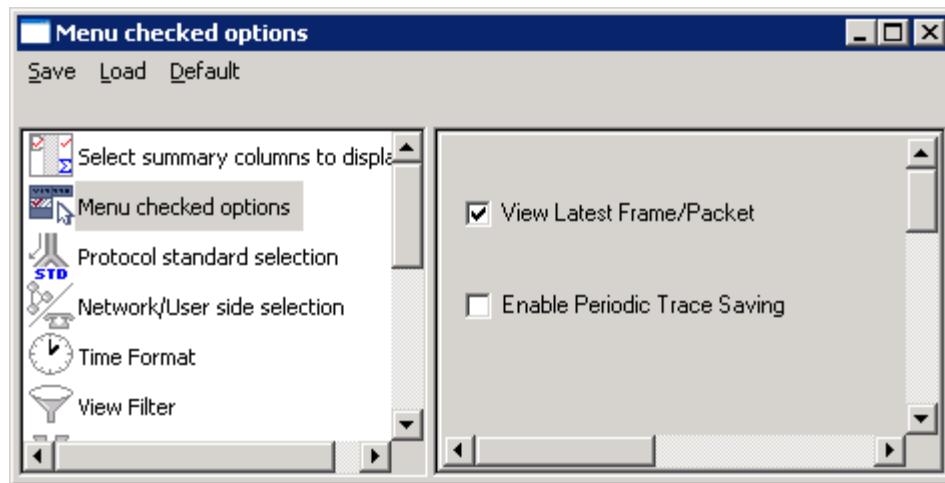


Figure 110: Menu Checked Options

10.3 Protocol Standard Selection

Select **View > Protocol** to select the decoding standard used to parse and display information. The decoding standard does not affect information saved to a disk file and therefore can be changed at any time.

PacketScan™ supports decoding of almost all industry standard signaling protocols – See [Protocol List](#) for complete details.

- SIP, SIP-I, SIP-T, H.323, MEGACO, MGCP, Diameter, Skinny
- LTE (Requires Additional License)
- SIGTRAN – SS7, ISDN (Requires Additional License)
- GSM A over IP (Requires Additional License)
- GPRS Gb over IP (Requires Additional License)
- UMTS over IP (Requires Additional License)
- T.38 and Video calls

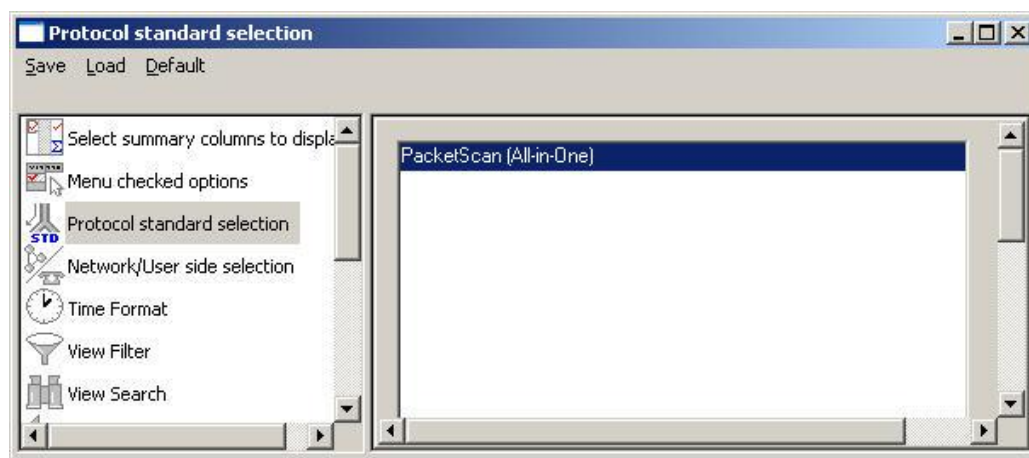


Figure 111: Protocol Standard Selection

10.4 Network / User Side Selection

Select **As Captured** option button to retain the selected user/network options.

Select **Inverse Captured** option to inverse the selected user/network options.

Select **User Defined** option button to specify the network side cards. This option can be specified when multiple cards are used. Enter the card number, which should be on the network side.

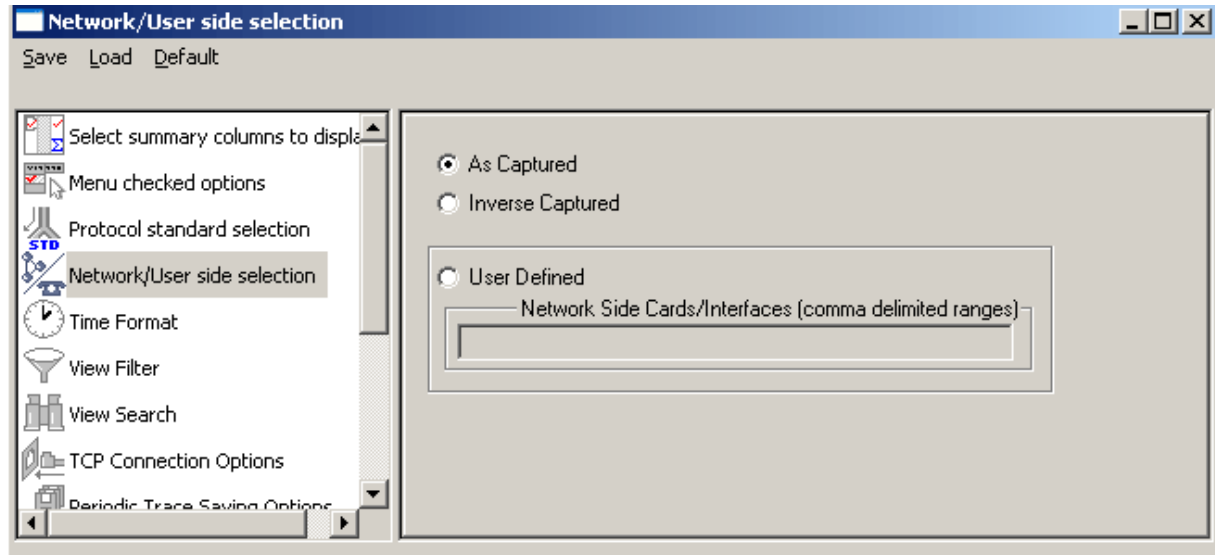


Figure 112: Network/User side Selection

10.5 Time Format

Four time display formats are supported for both **Real-time** and **Offline** analysis. These time formats can be changed during both off-line and real-time analysis by selecting the required time format as shown in the figure below. For more details, refer to [Time Display Formats](#).

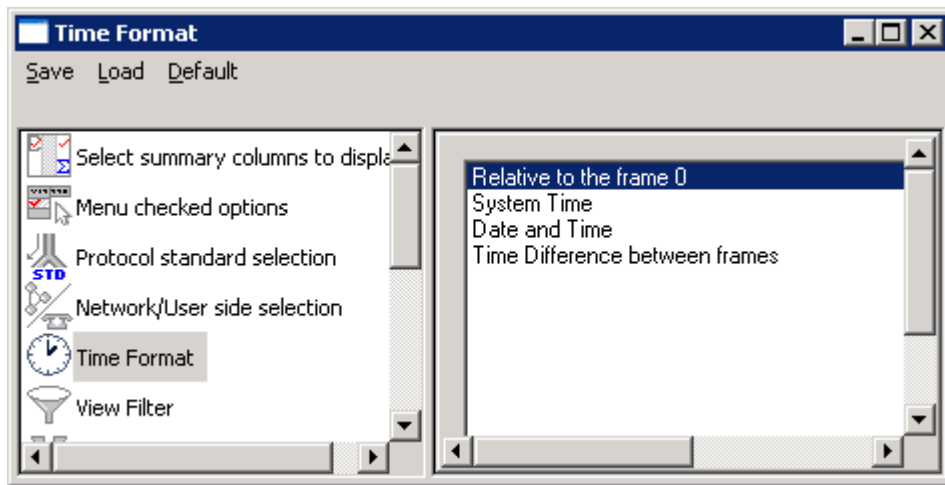


Figure 113: Time Format

10.6 Filtering Criteria

This option is used to filter frames displayed in the Summary View. For more information on View Filter, refer to section [View Filtering Criteria](#).


10.7 View Search

This option is used to search the Summary View by decoded Summary column values. For more information on **View Search** refer to section [Searching for Specific Frames](#).

10.8 Connecting to Remote Database

Protocol Analysis Probes run on multiple computers. The probes can send protocol summary information and binary frame data via TCP/IP connection to a Database Loader to load data into a database.

Users have the option to select the captured information to be sent over TCP/IP to a Central Database. PacketScan™ can send Frame Summary, Frame Octets, and Call detail records to database for the captured SIP and H.323 calls. The Database Loader application must be connected to a database in order to load probe protocol information into database.

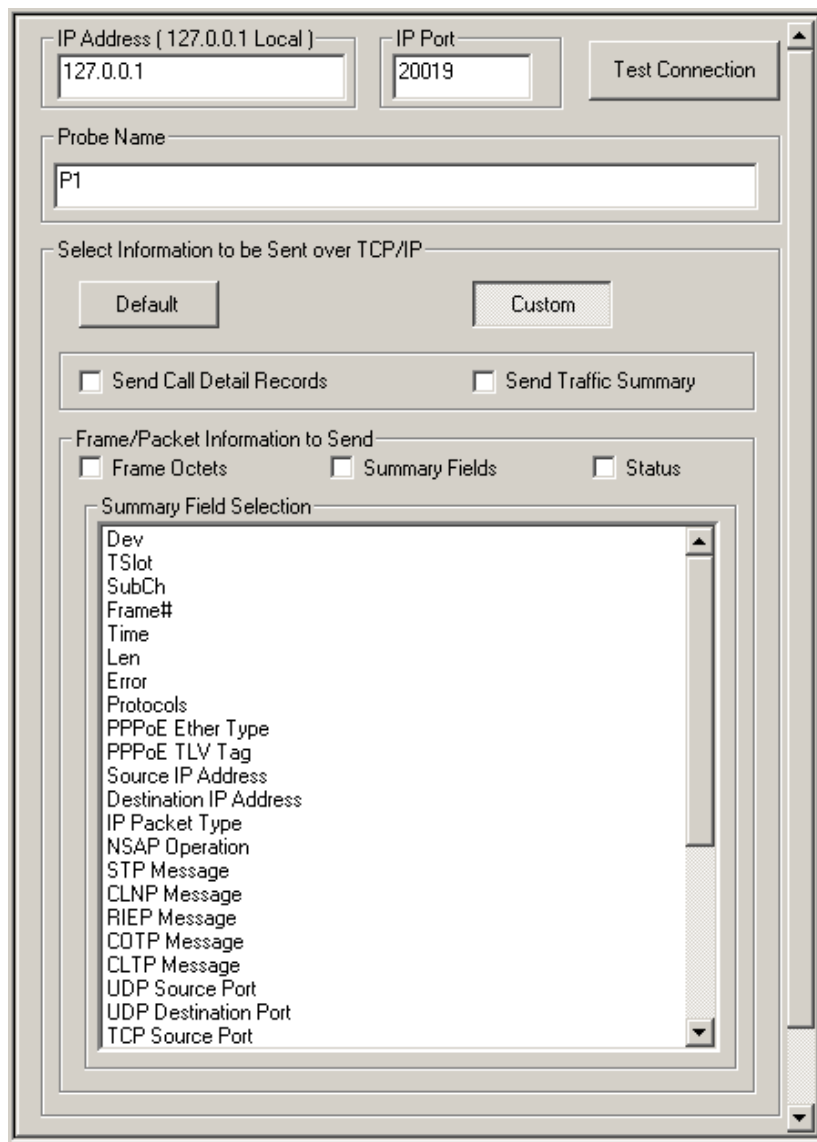
To set the TCP-IP parameter, select **TCP Connection Options** from the **Database** menu or click on  TCP Connection Options button from **Configure > Protocol and GUI Options** to open the window as shown in the figure below.

In order to test the TCP/IP connection, the probe IP address and the IP Port number must be entered.



Note:

Users require CallTraceRecvViaTcp.exe and SumRecvViaTcp.exe to be running on the destination system.



The screenshot shows the 'TCP Connection Options' dialog box. At the top, there are two input fields: 'IP Address [127.0.0.1 Local]' containing '127.0.0.1' and 'IP Port' containing '20019'. To the right of these is a 'Test Connection' button. Below this is a 'Probe Name' field containing 'P1'. The next section is 'Select Information to be Sent over TCP/IP', which includes 'Default' and 'Custom' buttons, and two checkboxes: 'Send Call Detail Records' and 'Send Traffic Summary', both of which are unchecked. The final section is 'Frame/Packet Information to Send', which includes three checkboxes: 'Frame Octets', 'Summary Fields', and 'Status', all of which are unchecked. Below this is a 'Summary Field Selection' list box containing the following items: Dev, TSlot, SubCh, Frame#, Time, Len, Error, Protocols, PPPoE Ether Type, PPPoE TLV Tag, Source IP Address, Destination IP Address, IP Packet Type, NSAP Operation, STP Message, CLNP Message, RIEP Message, COTP Message, CLTP Message, UDP Source Port, UDP Destination Port, and TCP Source Port.

Figure 114: TCP Connection Options

PacketScan™ can detect connection drops to database, reconnect if connection is broken. It also sends keep-alive messages to the database loader periodically to maintain the connection status.

The **Custom** option allows setting the call detail records, traffic summary, frame/packet information (Frame Octets, Summary Fields, Status) to be sent, and the Summary field selection options. The **Default** options do not provide options to select the required information to be sent; instead default summary information is sent to database.

Send Call Detail Records: If this option is checked, all the call detail records in call detail record view will be sent to the remote database.

Send Traffic Summary: If this option is checked, all the Summary View details in Packet Data Analysis – Traffic Analyzer Summary View will be sent to the remote database. Traffic Summary sent to central database includes following fields:

Signaling Parameters

- **CallId:** Locally generated unique call number to this call. Represented as an integer
- **Calling Party:** Participant address which uniquely identifies calling Party. It can be PhoneID, URI or IP Address
- **Called Party:** Participant address which uniquely identifies called Party. It can be PhoneID, URI or IP Address
- **CallId:** Global unique identifier of the call. For sip its combination of random number and/or host address.
- **StartTime :** Start time of the call, i.e. time when call initiating message is received.
- **CallDuration:** Duration of the call. Represented in hh::mm::secs format
- **CallAnswered:** Indicates whether the call is answered successfully or not. If answered value will be 1 else 0.
- **Call Failure reason:** Indicates call failure reason. It is an integer with values 0-5. We group the failed calls based on the failure reason.
 - 0 - Successfull calls.
 - 1 - User is Busy. ex: SIP 486
 - 2 - No Answer from other end
 - 3 - Unknown Destination ex: SIP 404
 - 4 - Network Failures ex: SIP 5xx,6xx
 - 5 - other failures ex: SIP 4xx
- **SessionRequestDelay:** Time interval between the moment the Session Initiating message is sent by the originating agent and the first provisional response received by the called party. It is utilized to detect failures or impairments causing delays in responding to a session request. Represented in msec.
- **Session Disconnect Delay:** Time interval between the moment the Session Ending message is sent and response received for it. This metric is utilized to detect failures or impairments delaying the time necessary to end a session. Represented in msec.
- **SIP Originating Ip:** IP address of the calling agent.
- **SIP Destination IP:** IP address of the called agent.
- **RTP Source Ip:** IP address of RTP traffic generator at Caller.
- **RTP Destination IP:** IP address of RTP traffic generator at Callee.
- **SIP Error Code:** It gives the SIP error code such as 4xx, 5xx, 6xx if any received for failed calls. It is an integer value.
- **Protocol Type:** Signaling protocol used for the call. Ex: SIP, H323

Traffic parameters for each side of call (for Left and Right channel)

- **SSRC Id:** Synchronization Source, unique identifier for the RTP traffic stream.
- **Codec String:** Codec used for this call Ex: G729, PCMU.
- **Total Packet count:** Total Traffic packets received on this stream. Includes both RTP and RTCP.
- **Missing Packet count:** Total RTP packets count that have not been received by PacketScan for this session.
- **Missing Packet ratio:** Missing packets over total packets expressed in percentage
- **Duplicate Packet count:** Total Duplicate RTP packets received for this session.
- **Duplicate Packet ratio:** Duplicate Packets over total Packets expressed in percentage

- **Reorder Packet count:** Total Out of order RTP packets that are received in out of order.
- **Reorder Packet ratio:** Out of order Packets over total Packets expressed in percentage
- **Conversational MOS:** Mean Opinion Scores (MOS) is a way of estimating how good or bad a call will sound to a user based on packet metrics, primarily loss and jitter. For uncompressed voice a score of 5 is perfect and a score of 1 is completely unintelligible. Each codec has its own theoretical maximum though, (4.2 for G.711, 3.92 for G.729 etc). These values are calculated as per ITU-T G.107 E-Model. CMOS (Conversational MOS) is a bidirectional metric which does account for delay/echo.
- **Conversational Rfactor:** The voice quality metric that measures quality based on transmission delay, burst packet loss, and burst loss recency. Same as CMOS but measured on a scale of 0 to 100.
- **Listening MOS:** LMOS is a unidirectional metric that does not account for things like delay and echo.
- **Listening Rfactor:** The voice quality metric based on burst packet loss and codec selection. Same as LMOS but measured on a scale of 0 to 100.
- **Packet Discarded:** Packets that are received but arrived very late or early. As a result they are discarded by jitter buffer while calculating MOS/R-Factor.
- **Packet Discarded ratio:** Discarded packets over total RTP packets expressed in percentage.
- **Average Gap:** Gap is the time interval between two consecutive RTP packets. This interval is calculated based on the time when PacketScan™ received the packet. It is in milliseconds. Average gap is calculated as the mean of the gaps for all the packets received.
- **Average Delay:** It is the difference in packet spacing at the receiver compared to the sender for a pair of packets. Average Delay is the mean of the delays observed for all the packets.
- **Average Jitter:** Variation in packet arrival times. Discrepancy in milliseconds between when a packet is expected to arrive and when it actually arrives. Average Jitter gives the mean of the jitters observed for all the packets received.
- **Average InterArrival Jitter:** The average Inter-Arrival Jitter is calculated as a mean of the Inter-Arrival Jitter field appearing in the Sender Report and Receiver Report of RTCP packets.
- **Cummulative Packet Lost:** The total number of RTP data packets from source SSRC_n that have been lost since the beginning of reception. This will be reported by RTCP SR/RR packets.
- **Minimum Gap:** Minimum gap observed for the session.
- **Maximum Gap:** Maximum gap observed for the session.
- **Minimum Jitter:** Minimum Jitter observed for the session.
- **Maximum Jitter:** Maximum Jitter observed for the session.
- **Minimum Delay:** Minimum Delay observed for the session.
- **Maximum Delay:** Maximum Delay observed for the session.
- **Average RTD:** Round-trip delay on one session is the time taken (in milliseconds) for the packet to travel from PacketScan™ to the other end destination (either caller or callee) and back to PacketScan. Refer Round Trip Delay calculation for details.
- **Minimum RTD:** Minimum RTD observed for the session
- **Maximum RTD:** Maximum RTD observed for the session

To send specific frame summary fields, users are required to select the summary fields in a particular order.

Prerequisites for remote protocol analysis probes are following:

- Database installation and configuration
- Creating and configuring protocol table
- Database Loader installation and configuration

Probes can be configured to filter only subset of frames according to some criteria. For example, to load the database with complete information, all the three data types for exporting (loading into database), i.e., **frame octets**, **summary fields** and **status** information must be checked or the **send call details** records option must be checked. For detail information on this, refer to [PacketScanWeb™](#).

Initialization Procedure for Database Connection


PacketScan™ includes preset configuration file 'SipProtAnalyzer.Acf' and 'H323ProtAnalyser.Acf' in the installation directory that is configured to send specific Frame Summary fields to the database. Users can load this pre-configured file while sending Frame Summary to the database as explained below.

- 1) Load the pre-saved configuration file **SipProtAnalyzer.Acf** for SIP records or **H323ProtAnalyzer.Acf** for H.323 records from **Configure > Load All Options** or **Configure > Protocol and GUI Options > Load** menu.
- 2) Select **TCP Connection Options** from **Analyzer GUI and Protocol Configuration** dialog.
- 3) Database **IP Address**, **IP Port**, and **Probe Name** are set to default values in the configuration file. Users can edit these values according to his settings.
- 4) The configuration file has been set to send **Traffic Summary**, **Frame Octets**, and **Summary Fields** by default. User can select these options according to the requirements.



Note:



It is advised not to select any other fields under Summary Fields in this configured file. Changing Summary Fields order will populate database improperly.

- 5) Now, in order to send signaling Frame Summary (SIP or H.323) to database, perform the following and save the configuration file.
 - Select **View > Filtering Criteria** or click on the  **Set Filtering Criteria** icon from the analyzer main window to set the filter.
 - Select and expand **MAC** layer under **SIP 3261 for SIP messages** or **H.323 for H.323 messages**, and select **Packet Type** field.
 - Select **SIP** as the **Packet Type Value** and click **Activate** button to apply the settings. This configures to display only **SIP** messages in the analyzer, and sends **Frame Summary** for only SIP messages.
 - For H323, select **H225, H245 and RAS** as the **Packet Type Value** and click **Activate** to apply the settings. This displays only **H.323** messages in the analyzer and sends **Frame Summary** for H.323 messages.



Note:

- Sending frame summary for all the captured frames (like RTP/RTCP) for a call may not serve more information and it will overload database with traffic frames.
- With the above settings, though PacketScan™ captures all the frames as per the "Capture Filter" settings, only SIP messages will be displayed in the analyzer when filtering criteria is applied.
- The traffic frame details can be viewed in the Packet Data Analyzer – Summary and Detail View.

- 6) Click on '**Save**' menu to save the settings to a configuration file, which can be used for future analysis, and close the dialog.
- 7) Select **View > Activate Filter** or click on the  icon from the main analyzer window to activate filtering. This will allow to display SIP or H.323 messages as configured and frame summary will be sent for only displayed messages (i.e. SIP or H323).
- 8) To deactivate filter, click **Deactivate Filter**  from the toolbar or select **View > No Filtering** from the main menu.
- 9) Ensure to disconnect from database before deactivating filter, else frame summary will be sent to all captured frames and corrupts database.
- 10) Now invoke Packet Data Analyzer – Summary View, connect to database and start real-time capture.

10.9 Periodic Trace Saving Options

For detail information on periodic trace saving options refer to section [Periodic Trace Saving Options](#).

10.10 Startup Options

Startup option are used to enable the startup tasks such as enabling periodic trace saving, activating filter, connect to a remote database via TCP/IP and start real-time tracing.



Note: This feature is applicable to real-time analyzer only.

Click on  from **Configure > Protocol and GUI Options** to open the screen as shown below.

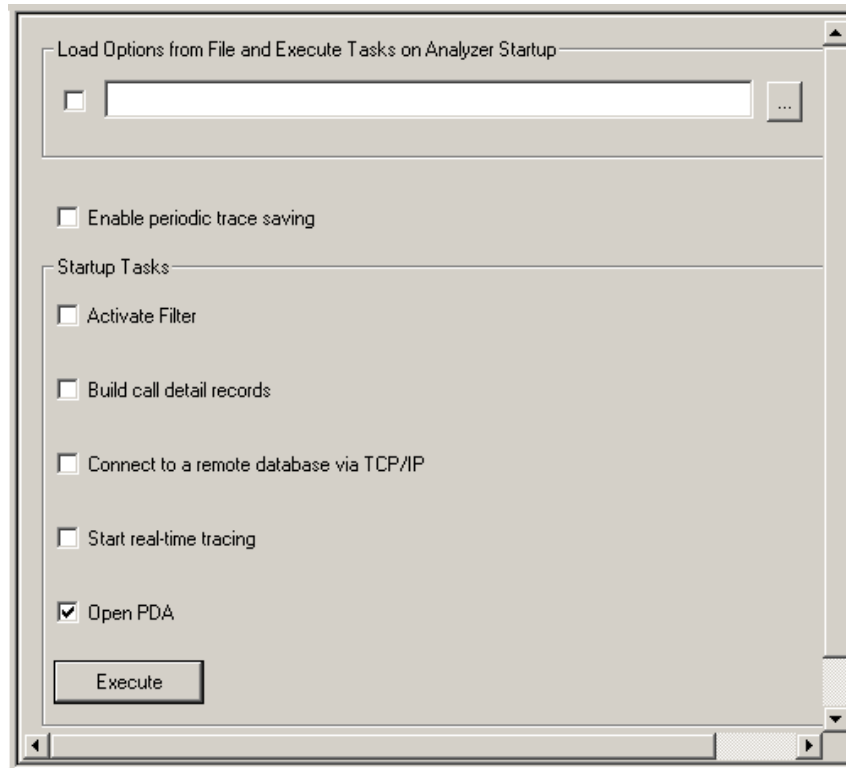


Figure 115: Startup Options

Enable periodic trace saving

Enables periodic trace saving immediately when analyzer is opened. For more information on this, refer to [Periodic Trace Saving Options](#).

Activate Filter

Activates filter when analyzer is opened. For more information on this, refer to the section [Activate Filter](#).

Build Call-detail Records

Activates Call Detail View when analyzer is opened. For detail information on this, refer to [Build Call Detail Record](#) in [Call Detail Records](#).

Connect to a remote database via TCP/IP

Connects to remote database loader when analyzer is opened. For more information on this, refer to [Connecting to Remote Database](#).

Start real-time tracing

Select the **Start real-time tracing** check box and click **Execute** to start the real-time capturing. A warning message for overwriting the temporary trace file gets displayed. If you want to overwrite click **Yes**, else, click **No** and save it in a new file in the desired location. This new file replaces the default specified in the capturing options dialog. For more information on this, refer to [Start Real-time](#) in [File Menu Options](#).

10.11 View Font Size

This option allows the user to choose the required font size to view the Summary, Detail, Hex, Statistics, and Call Detail Records Views. Select the option buttons with various font sizes such as Extra Large, Large, Normal, Small and Very small.

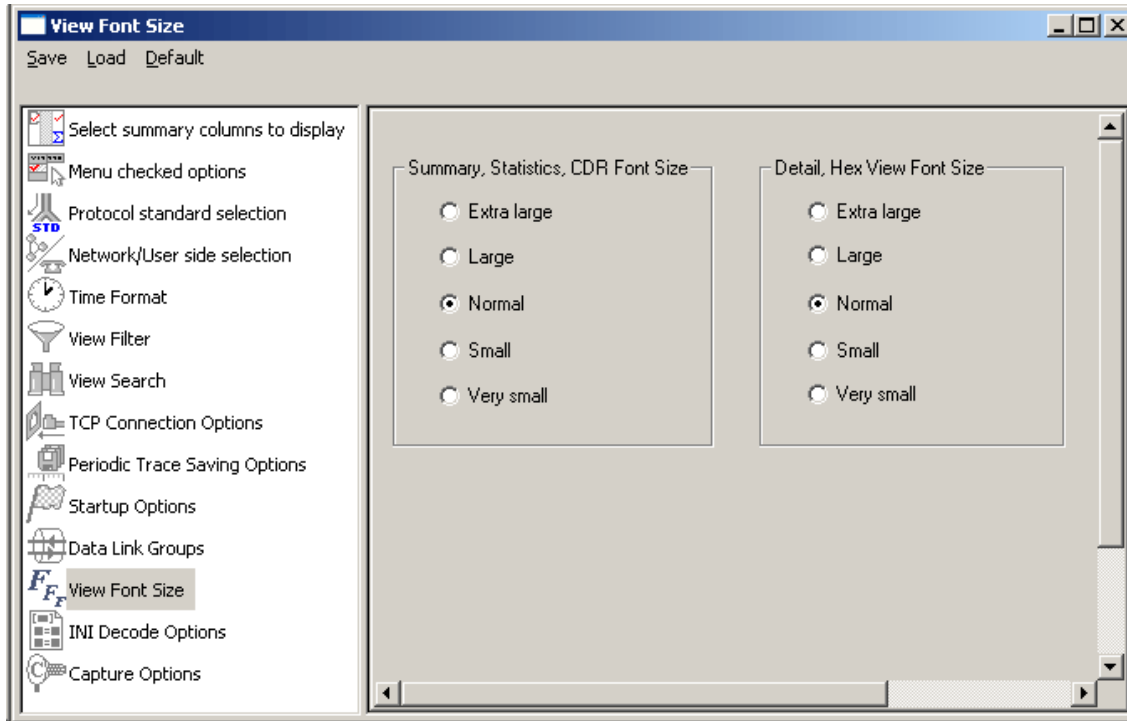


Figure 116: View Font size

10.12 Decode Customization Options in PacketScanProt.INI

The .INI file configuration enables the user to enter the required custom value in the PacketScanProt.ini file (located in Program Files\GL Communication Inc) to get proper decodes. PacketScanProt.ini, and IPCapt.ini are like any other ASCII file such as .txt file and hence can be edited easily.

The same can be edited in the GUI as explained below:

Click  INI Decode Options from **Configure > Protocol and GUI Options > INI Decode Options** screen.

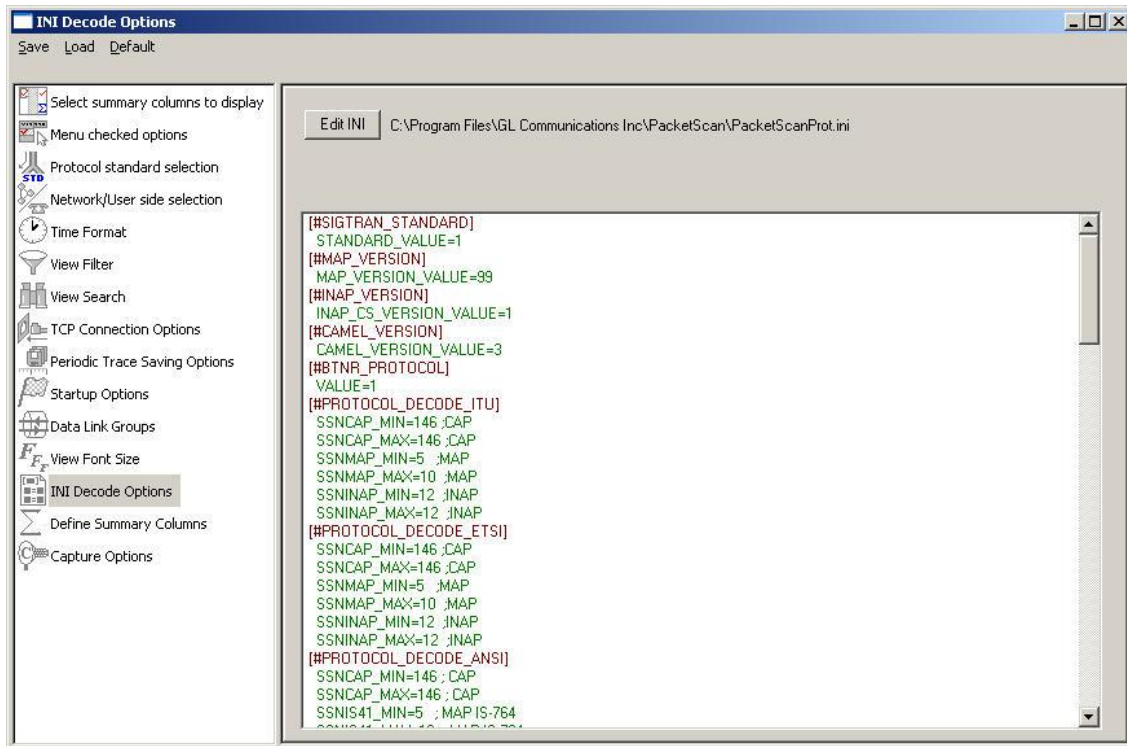


Figure 117: INI Decode Options

Click **Edit INI** to open the editor as shown in the figure below:

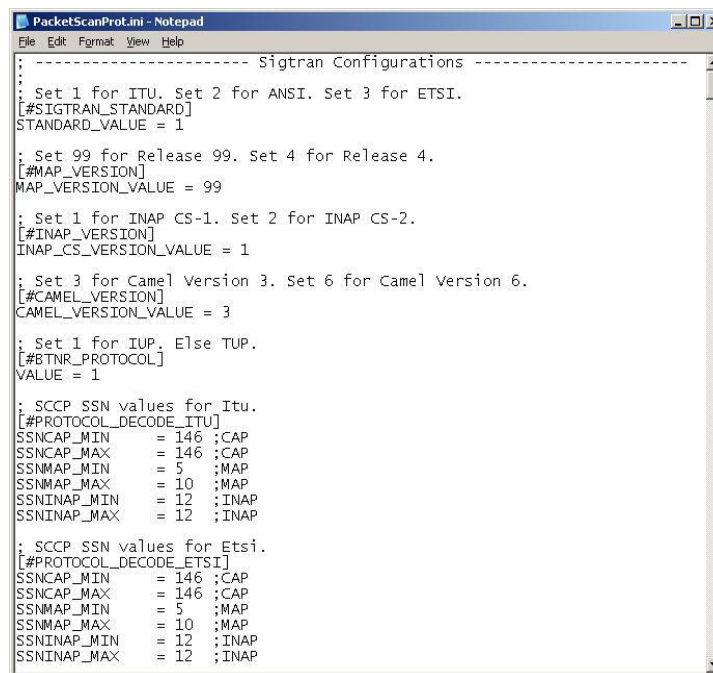


Figure 118: PacketScanProt.ini File

User can edit the following details in the INI file.

10.12.1 SIGTRAN

[!SIGTRAN_STANDARD]: This header indicates selection of Sigtran Standards. Select 1 for ITU standard. Set 2 for ANSI standards. Set 3 for ETSI standards. The default is set to 1 - ITU standard.

[!MAP_VERSION]- This parameter is used to select MAP release versions, i.e., R99 or MAP R4 CS1 layer, for decoding. If it is set to 99, then MAP R99 layer will be decoded, and if the value is set to 4, the MAP R4 layer will be decoded.

[#INAP_VERSION]- This parameter is used to select the INAP CS1 or INAP CS2 layer for decoding. If it is set to 1, then INAP CS1 layer will be decoded, and if the value is set to 2, the INAP CS2 layer will be decoded.

[#CAMEL_VERSION] - This parameter is used to select CAMEL Rel6 or CAMEL Rel3 layer for decoding. If it is set to 6, then CAMEL Rel6 layer will be decoded and if the value is set to 4, the CAMEL Rel3 layer will be decoded.

[#BTNR_PROTOCOL] -This identifier allows users to select TUP or IUP protocols for decoding. If it is set to 1, then IUP (BTNR) will be decoded, else TUP will be decoded.

SCCP SSN values for ITU - [#PROTOCOL_DECODE_ITU] - This parameter allows users to set INAP, CAP and MAP values for ITU decoding standards.

SSNCAP_MAX, SSNCAP_MIN - Maximum and minimum SSN value for CAP

SSNMAP_MAX, SSNMAP_MIN - Maximum and minimum SSN value for GSM MAP

SSNINAP_MAX , SSNINAP_MIN - Maximum and minimum SSN value for INAP

SCCP SSN values for ETSI - [#PROTOCOL_DECODE_ETSI] - This gives SSN value to set INAP , CAP and MAP value for ETSI decoding standard.

SSNCAP_MAX, SSNCAP_MIN Maximum and minimum SSN value for CAMEL

SSNMAP_MAX, SSNMAP_MIN Maximum and minimum SSN value for GSM MAP

SSNINAP_MAX , SSNINAP_MIN - Maximum and minimum SSN value for INAP

SCCP SSN values for ANSI - [#PROTOCOL_DECODE_ANSI] This header allows users to set the maximum and minimum values for TCAP and IS41.

SSNCAP_MAX, SSNCAP_MIN – Maximum and minimum value of SSN for CAP.

SSNIS41_MAX, SSN IS41_MIN - Maximum and minimum value of SSN for ANSI MAP IS-764.

SSNTCAP_MAX, SSNTCAP_MIN – Maximum and minimum value of SSN for TCAP.

SSNCNAM_MAX, SSNCNAM_MIN - Maximum and minimum value of SSN for CNAM.

SSNINAP_MAX , SSNINAP_MIN - Maximum and minimum SSN value for INAP

SIGTRAN_CALLTRACE_TYPE - [#SIGTRAN_CALLTRACE_SELECTION] – If set to '0' the ISUP call trace is enabled, or if set to '1', the TCAP (MAP) call trace is enabled, else the TCAP (CNAME) call trace is enabled.

SIGTRAN DUA Protocol Selection - [#DUA_HL] - The user adaptation layer 'DUA' in Sigtran stack carries either DPNSS protocol or DASS2 protocol. With **[#DUA_HL]** option, user can select between these two layers for decoding purposes. Set 0 for DPNSS. Else DASS2.

10.12.2 GSM A, UMTS IuCs

[#UMTS_DDMODE] – This header indicates Division Duplex Mode. UMTS provides Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes for selection. By default "DDMODE_VAL" is selected as FDD.

DDMODE_VAL = FDD

SCTP Protocol Payload - [#NBAP_SCTP_PPID] – This header identifies the SCTP protocol payload for NBAP. By default SCTP protocol payload identifier value is set to 10.

SCTP_PPID_VAL = 10

SCTP Port values - [#SCTP_PORT_FLAG_INDEX] - This header identifies SCTP port values to set for GSM A IP, RANAP and RNSAP.

For example, all SCTP packets receiving on port values in the range of **3000 to 3200** is branched to **RNSAP** and **6400 to 6600** is branched to **RANAP** interfaces. User can set the Port range **Minimum** and **Maximum** values as required.

Setting IuCS Codec Type [IUCS_CODECTYPE] – Set the codec type for IuCS calls - 2 for ALAW, 3 for MuLAW, 12 for GSM, 13 for EFR, 15 for HR, 14 for AMR, 29 for AMR_WB.

Enable IuCS and GSMA Call Processing [#PROCESS_IUCS_GSMA_CALLS] – If the value specified as '1' the PDA will process the IuCS and GSMA calls.

10.12.3 GPRS Gb

UDP Port values for GPRS-GB - [#UDP_PORT_FLAG_INDEX] – All the UDP packets having port values in the range of 2100 to 2200 is branched to GPRS-GB interface. Set the **Minimum** and **Maximum** values as required. This header identifies UDP Port values to select GPRS-GB

10.12.4 SIP, RTP, T.38 PDA Configurations

SIP Layer2 Protocol - [#LAYER_2_PROTOCOL] - This configures layer 2 protocol, which can be either MAC or any other unknown layer.

L2_PROTOCOL=4: If this value is set to 4, then ATM layer will be set as Layer 2 Protocol

L2_PROTOCOL=1: If this is set to 1, MAC layer will be set as layer 2 protocol.

L2_PROTOCOL=0 ; If this value is set to 0, then L2 layer is Unknown layer.

Layer2 Length - [#UNKNOWN_L2_LENGTH] – Allows specifying the value of length of layer 2 protocol (in bytes) for unknown layers.

Specifying HEC in ATM Header [#ATM_HEADER] – If the value specified as '1' it indicates Header Error Checksum is present in ATM header. If it is '0' then the HEC is not present in ATM Header.

RTP Payload - [#RTP_PAYLOAD_RFC4733]: This header indicates the RFC to be followed for out band events. RFC4733 = 1 indicates that RFC 4733 is used for decoding and RFC4733 = 0 indicates that RFC 2833 is used. In the above figure, RFC 4733 is set to 1.

Out-of-band Payload Type - [#RFC2833] - By default, out band payload type is set to 101. User can set it to different value, but both MIN_PAYLOAD and MAX_PAYLOAD values should be same.

Payload type for H.263 - [#RFC2190] - This field indicates payload type for H.263. The default value is 34.

Static Payload - [#WITHOUT_PAYLOAD] - This field indicates the static payload range.

RTP Session Expiry Timer - [#RTP_SESSION_EXPIRY_TIMER] - This field defines RTP session expiry timer if no RTCP and RTP packets are received for this specified amount of time in seconds. This helps in cleaning up inactive RTP sessions. By default this is set to 180 seconds.

Enable SIP Registration Messages - [#REGISTRATION_PROCESS] - If the value specified as '1' the PacketScan™ will process the SIP registration messages. If the value specified as '0', the PacketScan™ will not process the SIP Registration frames.

Enable T.38 Fax Processing - [#T38] -If the value specified as '1', the PacketScan™ will process the T.38 Fax calls. If the value specified as '0', the PacketScan™ will not process the T.38 Fax calls.

[AMR_WITH_IUUP_HEADER]

ENABLE_IUUP_HEADER = 0 – If this is set to 1, it will indicate IUUP header present in RTP Payload.

10.12.5 Skinny

Port Number for Skinny Protocol - [#SKINNY_PORT_NUMBER] - By default, port number of skinny protocol is set to 2000. User can set it to different value, but both MIN_PAYLOAD and MAX_PAYLOAD values should be same.

10.12.6 Megaco

Setting RFC Port Value [#BIN_MEGACO_VERSION] – If the value specified as '3015', the PacketScan™ will select Media Gateway Call Agent and If the value specified as '3525', the PacketScan™ will select Media Gateway Controller Call Agent.

10.12.7 LTE Diameter Configurations

LTE eGTP version - [#eGTP_VERSION] - Set the value as '8' for eGTP Release 8. Set the value as '9' for eGTP Release 9.

LTE S1 AP Payload Identifier - [#SCTP_PPI_S1AP] - This header indicates LTE S1 AP payload type. By default, out of band payload type is set to 100. User can set it to different value, but both S1APMIN and S1APMAX values should be same.

LTE X2 AP Payload Identifier - [#SCTP_PPI_X2AP] - This header indicates LTE X2 AP payload type. By default, out of band payload type is set to 200. User can set it to different value, but both X2APMIN and X2APMAX values should be same.

Diameter Application ID Identifier - [#DIAMETER_INTERFACE] - This identifier allows to set the Application ID value for various Diameter interfaces such as Cx, Dx, Rx, Zn, Zh, Wx, Gq, Gy, Sh, Dh, Gx, Rf, Ro, Wg, Wm, Pr, Wa, Wd, S6,...

10.12.8 General

Clean up Routine Timer - [#CLEAN_UP_TIMER] - Specifies clean up routine timer to delete purged terminated calls and free up memory for new. For every specified amount of time (in seconds) the cleanup thread will delete purged terminated call objects from the call list, freeing up space for new calls during high capture rate. By default this is set to 300 seconds.

10.12.9 IPCapt.ini File

Open the IPCapt.ini file from the installation directory in text format as shown in the figure below:

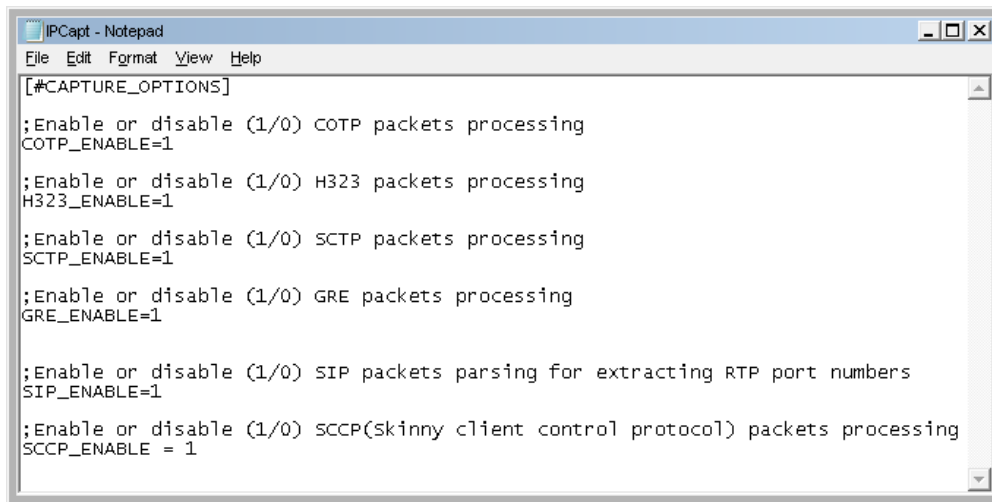


Figure 119: IPCapt.ini File

Now, user can enable/disable processing of selected protocols at capture level only using options provided in 'IPCapt.ini'. By default, all these options are enabled. Following options are currently included –

- COTP_ENABLE=1
- H323_ENABLE=1
- SCTP_ENABLE=1 (applicable only for SIGTRAN Analyzer)
- SIP_ENABLE=1
- SCCP_ENABLE = 1

To enable/disable options change the value to 1/0, and check for proper working –

COTP_ENABLE=1

If COTP_ENABLE option is disabled then COTP packets will not be processed and no decoding detail will be available.

H323_ENABLE=1

If H323_ENABLE option is disabled then no H.323 packets will be processed and no decoding detail will be available.

SCTP_ENABLE=1

If SCTP_ENABLE is disabled then no summary and no decoding detail will be available.

;Enable or disable (1/0) SIP packets parsing for extracting RTP port numbers

SIP_ENABLE=1

If SIP_ENABLE is set '0' (disabled) SIP packets will not be parsed at capture level to get associated RTP ports for the call. But SIP packets can be later processed in PDA

SCCP_ENABLE = 1

This option enables or disables (1/0) SCCP packets processing and reassembly.

If SCCP_ENABLE = 1 is set to 1, then it will process the SCCP (Skinny client control protocol) packets with reassembly.

Once the customizable decoding options are edited from GUI, a warning message appears as shown in the figure below. Restart the protocol analyzer, to apply the INI decodes changes.

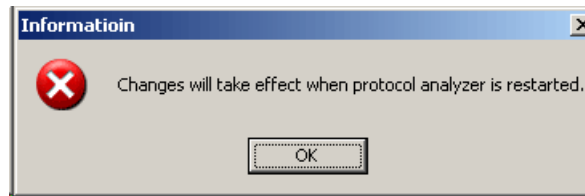



Figure 120: Warning Message



Note: The changes will take effect when an application is restarted.

10.13 Define Summary Columns

User can define the required summary columns through  **Define Summary Columns** option.

- 1) Select **Configure Menu → Protocol and GUI Options → Define Summary Columns**.
- 2) Expand the protocol layer and select the required field to display as shown in the figure below.

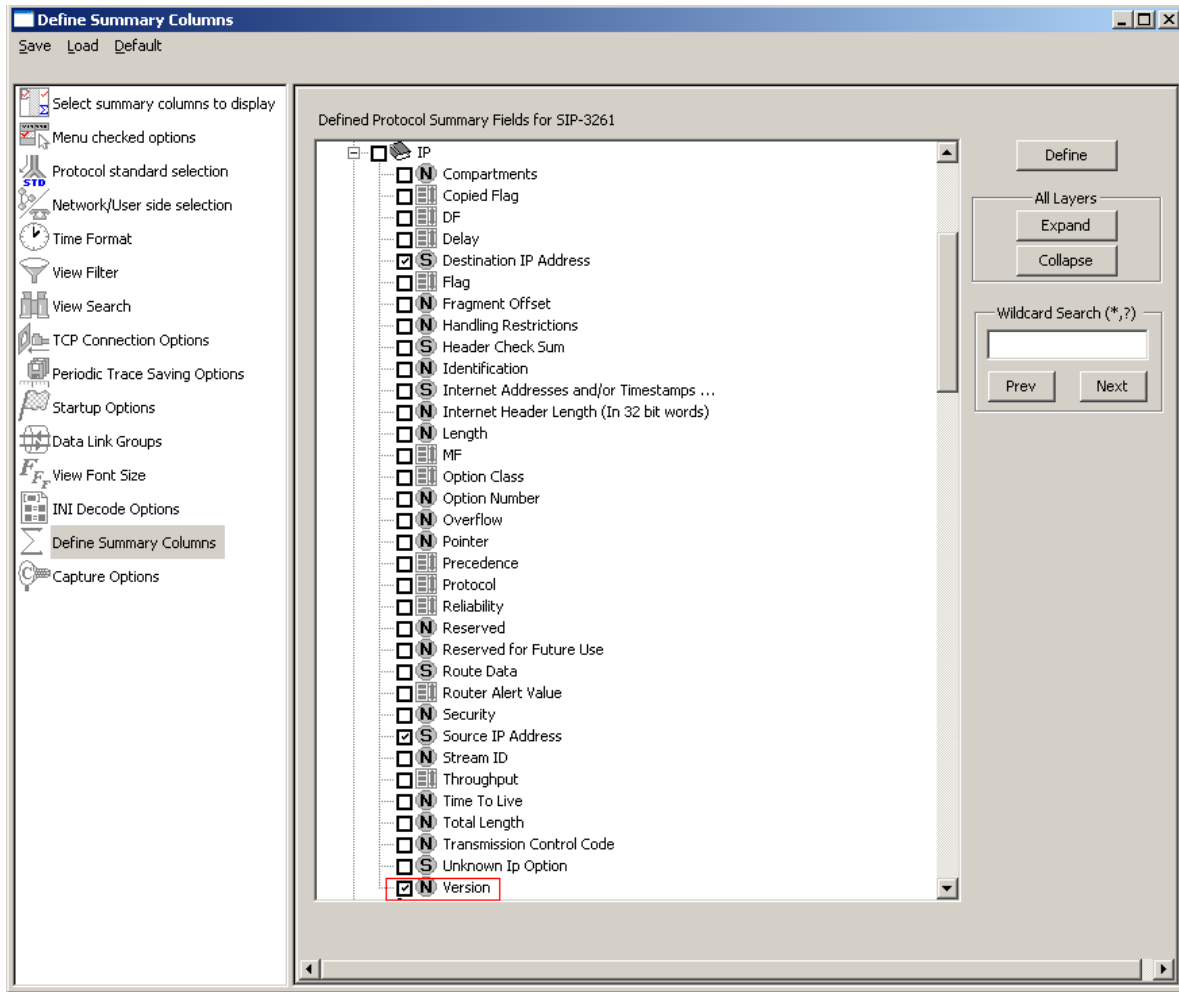


Figure 121: Define Summary Column

3) Click on "Define" and a popup message will appear, refer to the figure below. Click on "OK".

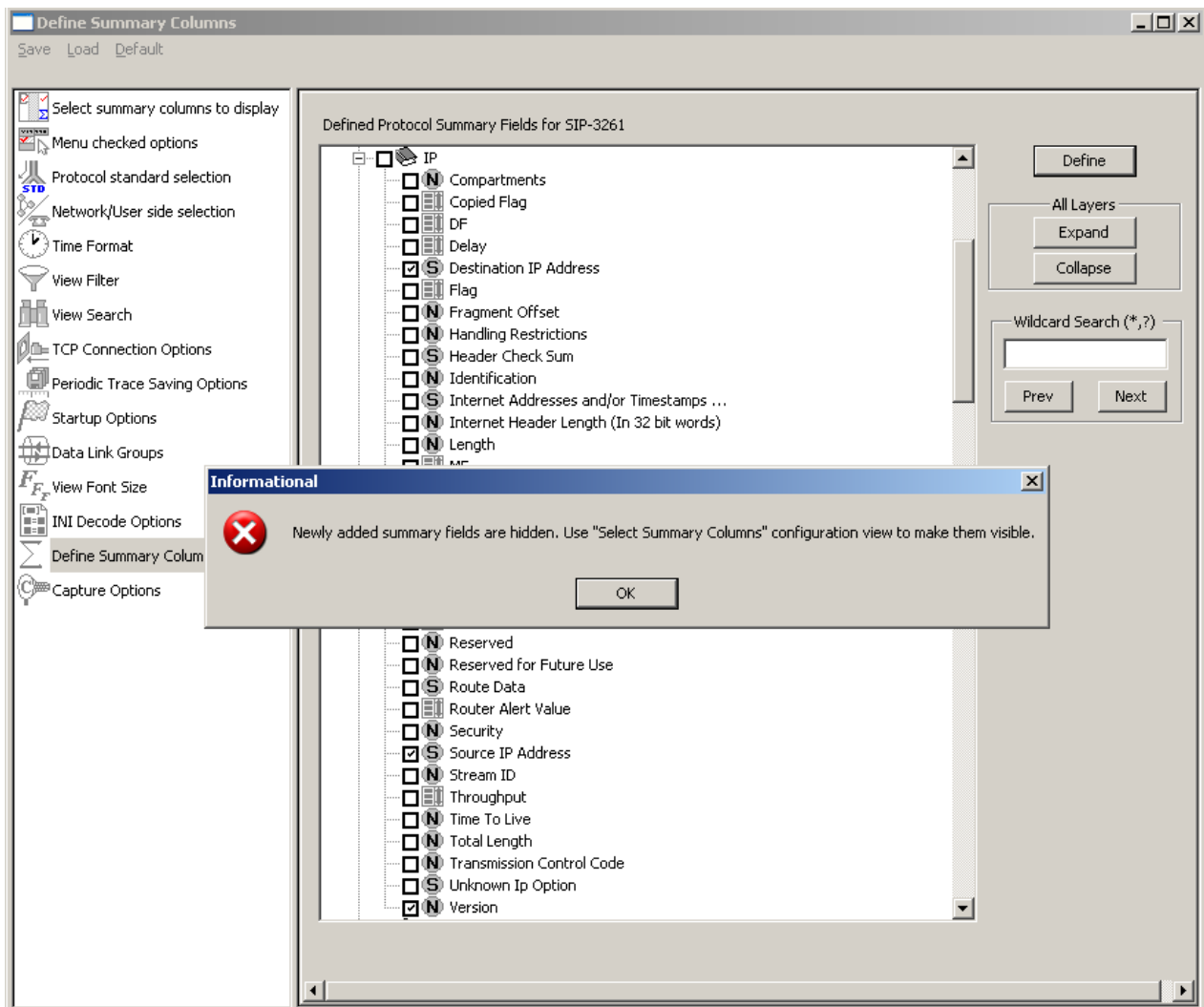


Figure 122: Popup Message

Other options available are:

Expand

Click on **Expand** to make all layers of the selected protocol standard visible.

Collapse

Click on **Collapse** to close the all the layers of the selected protocol standard.

Wildcard Search

User can search the required filter parameters through wildcard search. For example **A*t** can search the filters which starts from 'A' and ends with 't' such as **A-bit** or **Alphabet**.

- 4) Selected field is now visible in the **Select Summary Columns to Display**.
- 5) Select the field from the Hidden Summary Column and click on **Display Selected Column**.

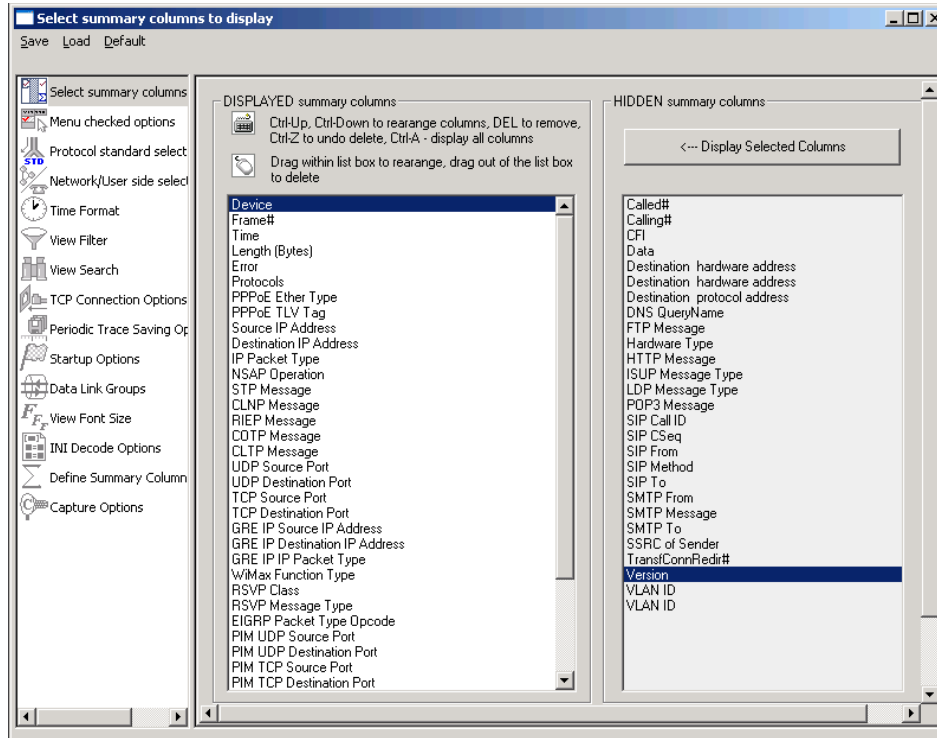


Figure 123: Adding the Summary Field to Display Summary Column

- 6) Selected field is now visible in the **Summary View**. Refer to the figure below:

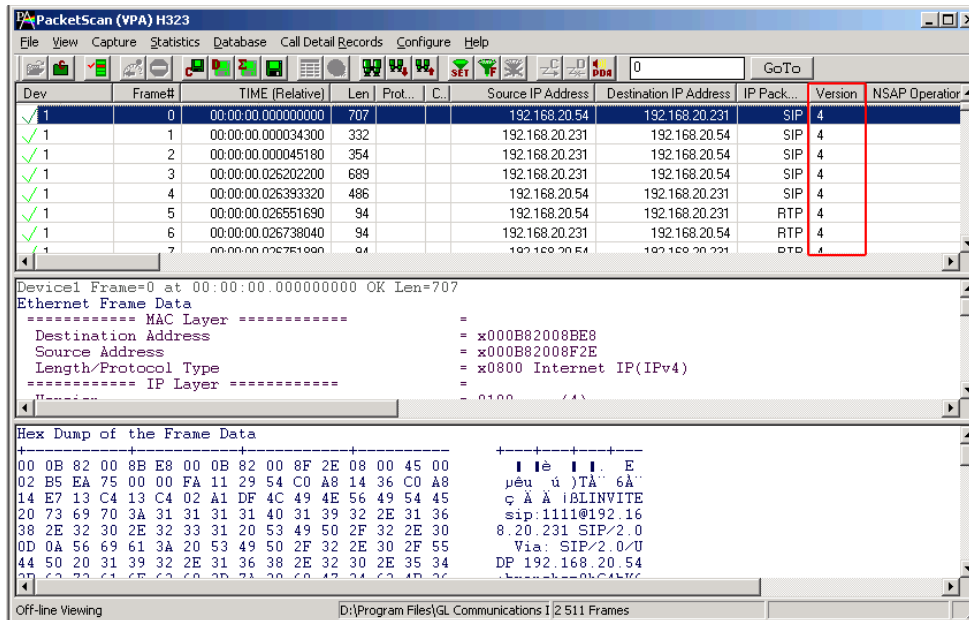


Figure 124: Added summary field



Note:

To remove the selected summary field, do the following:

1. **Select Configure Menu → Protocol and GUI Options → Define Summary Columns.**
2. Select the added summary field to be removed.
3. Click on 'Define'.

10.14 Capture Options

**Note:**

This feature is applicable to real-time analyzer only.

Switches to the list of capture options: selection of trace file, stream / interface selection, real-time filter, and others. For more information on this, refer to the section [Capture Menu Features](#).

(Intentional Blank Page)

Section 11.0 Status Indicators

PacketScan™ has the status indicators at the bottom of the window as shown in the figure below:

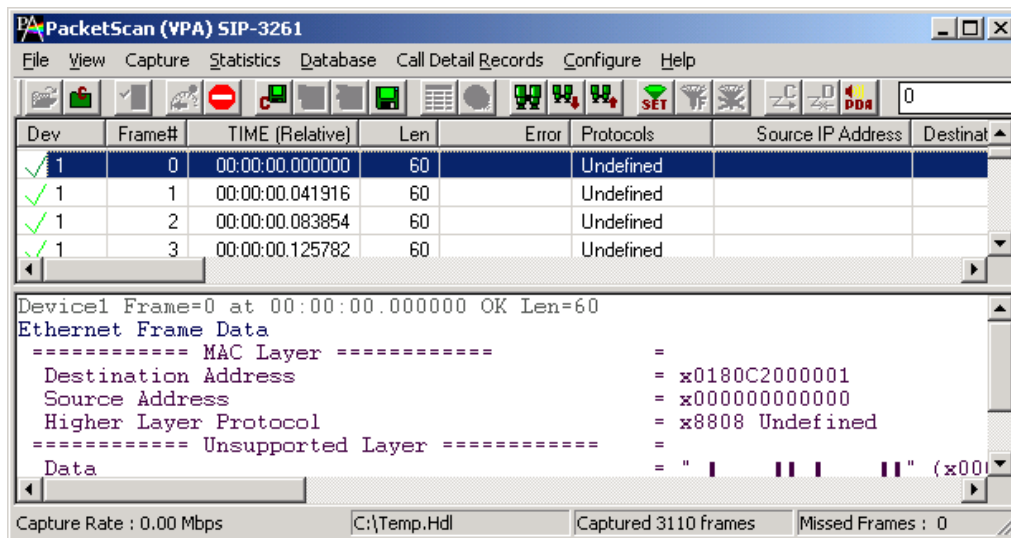


Figure 125: PacketScan™ Status Indicators

11.1 Capture Rate

The left status pane shows the rate (Mbps – Mega Bits Per Second) at which PacketScan™ is capturing data.

11.2 Trace File Name

The second status pane displays the trace file name.

11.3 Filtered and Total Frame Count

The third pane displays filtered and total Frame count when the filtering is active and just the total Frame count when filter is deactivated. During Online number of frames captured so far will be displayed in this status pane.

11.4 Missed Frames

During real time the fourth status pane displays number of frames missed.

(Intentional Blank Page)

Section 12.0 Packet Data Analysis – Traffic Analyzer Summary View

12.1 Overview

PDA- Traffic Analyzer Summary View displays summary of data transmission in each direction including calling number, called number, call id, start time, duration, missing packets, and so on. It includes –

- Separate statistical counts on total packets, calls, failed calls, captured frames, etc., for SIP, H323, RTP, MEGACO, GSM, and IuCS based calls.
- Graphs to view active calls, active jitter distribution, E-model based measurements for R-factor / MOS/ Packet Discarded, RTP packets over the duration of the call, T.38 Fax analysis, and Call flow graph.
- Call summary of each call that includes information of signaling parameters and audio parameters for each call. Also calculates and displays the video stats for all video calls. Users have the option to select the Traffic Summary information (along with Call Detail Records, and Frame/Package information) to be sent over TCP/IP to a central database. For more details refer to [Connecting to Remote Database](#).

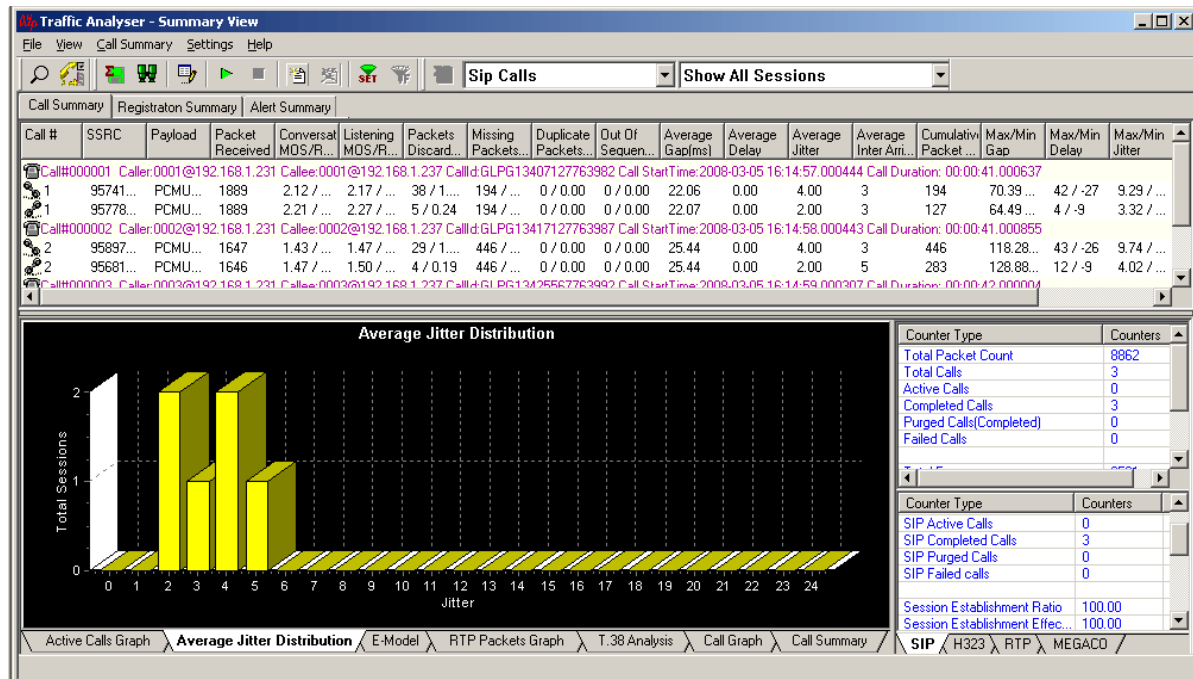


Figure 126: Packet Data Analysis – Traffic Analyzer Summary View

12.2 Summary View

Summary View can be divided into three main parts.

- Call Summary
- Call Quality Parameters
- Graphs

12.2.1 Call Summary

As the name indicates, it gives a summary of all the calls that are processed by PacketScan™. It gives a succinct introduction of all the captured SIP, MEGACO, RTP, H.323, GSMA, and IuCS packets.

The Call Summary part contains the description of the VoIP (SIP or MEGACO) calls and the RTP sessions associated with the call. This view is the primary gateway through which all the other call related options provided by VPA could be exercised. Below the Call Summary View are the Call Counters and various graphs. We will see below the details of each of these.

The primary item of display in the Call Summary View is an entry that uniquely identifies a call. VPA assigns a progressively increasing Call Number to each call it captures. A typical Call Summary entry looks like this.

Call#000001 Caller:271585@192.168.20.101 Callee:53001@192.168.20.101> CallId:55a0997-f2858fc8@192.168.20.247 Call StartTime:10:22:07.067 Call Duration: 00:01:18.830

Figure 127: Call Summary Entry of SIP Call

As is evident, this entry contains a string of ';' separated items. The first string being the Call number is assigned locally by PacketScan™. The second item is the 'From' address that appears in the SIP INVITE message, so is the third string, which is the 'To' address appearing in the INVITE message, the fourth string is the 'Call ID' from the INVITE message. The final string is the Call start time and the Call duration. Call start time is the time when the SIP INVITE message was received and the Call duration is calculated with reference to the start time and the time when the last packet corresponding to the call was received. In its default state the Call Summary will have one such entry for each call processed.

The Call Summary entry is added immediately after an INVITE message is received. In the strict sense this does not qualify as a call even though we refer it as a Call Summary entry.

In case of MEGACO calls, the second item, Caller gives the value of the 'Physical Termination' (a termination which is provisioned in the Media Gateway) that appears in the MEGACO Add Request command. The third string, Callee denotes the 'Ephemeral Termination' (a logical termination that exists in the Media Gateway towards the IP network), that appears in Add Reply to Add Request, initially Ephemeral Termination is set to \$(CHOOSE) until it is created. The fourth string, Call ID, shows the value of the 'Context ID' from the Add Reply command. Refer to the RFC 3525 for more information on terminations and context in MEGACO.

Call#000001 Caller:tgw/s1/c2 Callee:tgwrtp/2 CallId:4 Call StartTime:2009-05-21 12:40:44.000636 Call Duration: 00:00:31.000634

Figure 128: Call Summary Entry of MEGACO Call

The Call Summary displays the RTP/RTCP sessions associated with the SIP Call (whose 'From', 'To' and 'Call Id' are displayed in the first row) or MEGACO call (whose 'Physical Termination', 'Ephemeral Termination', and 'Context ID' are displayed in the first row).

Each line represents a RTP/RTCP session. A host of statistics collected about that session is displayed here in a tabular format. An entry is added to the session's list irrespective of whether a RTP packet has been received or a RTCP packet has been received. In case a session (pertaining to a call) has received only RTCP packets then only received columns will have valid information, the rest will reflect a default (zero) value.

Call #	SSRC	Payload	Packet Received	Alert Summary	Conversional MDS/R-Factor	Listening MDS/R-Factor	Packets Discarded(%)	Missing Packets(%)	Duplicate Packets(%)	Out Of Sequence Packets(%)	Average Gap(ms)	Average Delay	Average Jitter	Average Inter A.	Cumulative Packet...	Max/Min Gap	Max/Min Delay	Max/Min Jitter	Max/Min RTDela...	Average RTDela...
1	27...	PCM...	7632	1.30 / 23	1.33 / 24	133 / 1.30	2955 / 25...	0 / 0.00	0 / 0.00	0 / 0.00	26.75	0.00	8.00	3	0	143.18...	86 / 45	16.48 ...	0.217 ...	0.127
1	27...	PCM...	10250	3.91 / 82	3.98 / 84	208 / 2.03	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	20.01	0.00	1.00	8	1658	219.84...	199 / ...	23.51 ...	4.805 ...	0.896
4	27...	PCM...	8474	1.18 / 19	1.21 / 20	1180 / 9.86	3510 / 29...	0 / 0.00	2076 / 17.34	0 / 0.00	28.24	0.00	24.00	4	0	617.00...	600 / ...	92.66 ...	1.394 ...	0.502
4	27...	PCM...	12001	3.95 / 83	3.98 / 84	207 / 1.73	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	20.01	0.00	1.00	23	3470	220.38...	200 / ...	23.97 ...	53.846...	6.721
5	27...	PCM...	12942	1.43 / 27	1.50 / 29	294 / 1.78	3553 / 21...	4510 / 2...	0 / 0.00	0 / 0.00	18.48	0.00	22.00	4	0	514.98...	482 / ...	89.48 ...	0.589 ...	0.325
5	27...	PCM...	12002	3.98 / 84	4.01 / 85	195 / 1.63	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	20.01	0.00	1.00	21	-955	224.97...	204 / ...	24.22 ...	33.247...	4.208

Figure 129: Call Summary

One notable exception with the Call Summary entry discussed above is the display of Non SIP RTP sessions in the Call Summary. PacketScan™ has this flexible option of capturing and identifying RTP streams that do not have SIP messages associated with them. These streams may be part of very loosely established RTP sessions wherein all the information required for creating and maintaining the session are exchanged externally (Via E-Mail etc), or the streams may belong to Non-SIP VoIP calls like those using H.323 or MGCP or MEGACO etc. The columns relating to the RTP stream will not be changed, the only change would be in the first line / row, which would reflect the absence of SIP messages. As a result of this, no call number would be allocated to the call. But a PacketScan™ generated unique Call Id would be assigned to assist in distinguishing the call.

**Note:**

Users have the option to select the Traffic Summary information (along with Call Detail Records, and Frame/Packet information) to be sent over TCP/IP to a central database. For more details refer to [Connecting to Remote Database](#).

Call summary displays the following information in tabular format from left to right as shown in the figure below:

Call #: Call # represents the unique call number allocated to this call by RRA.

SSRC: SSRC (Synchronization Source) identifier associated with this RTP session. In case of RTCP only sessions, this will be the SSRC of the Sender (the side which generates the RTCP packet. For more information about SSRC and SSRC of Sender, please refer RFC 1889).

Payload: This tells the type of Traffic inside the RTP packet. This is mainly the Codec type used for sending the traffic.

Packets Received: It gives the total number of RTP and RTCP packets received in this session.

Conversational-MOS: Mean Opinion Scores (MOS) is a way of estimating how good or bad a call will sound to a user based on packet metrics, primarily loss and jitter. For uncompressed voice a score of 5 is perfect and a score of 1 is completely unintelligible. Each codec has its own theoretical maximum though, (4.2 for G.711, 3.92 for G.729 etc). These values are calculated as per ITU-T G.107 E-Model. CMOS (Conversational MOS) is a bidirectional metric which does account for delay/echo

Conversational R-Factor: The voice quality metric that measures quality based on transmission delay, burst packet loss, and burst loss recency. Same as CMOS but measured on a scale of 0 to 100

Listening-MOS: LMOS is a unidirectional metric that does not account for things like delay and echo

R-Factor: The voice quality metric based on burst packet loss and codec selection. Same as LMOS but measured on a scale of 0 to 100.

Packets Discarded/%: Packets that are received but arrived very late or early. As a result they are discarded by jitter buffer while calculating MOS/R-Factor. It also provides discarded packets over total RTP packets expressed in percentage.

Missing Packets/%: It gives the total RTP Packets that have not been received by PacketScan™ in this session. Also, displays the percentage of packets not received to the total number of packets received.

Duplicate Packets/%: It gives the count and percentage of total duplicate RTP packets received on this session.

Out of Sequence Packets/%: It provides the count and percentage of total RTP Packets in this session that has been received out of sequence.

Average Gap (ms): Gap is the time interval between two consecutive RTP packets. This interval is calculated based on the time when PacketScan™ received the packet. It is in milliseconds. Average gap is calculated as the mean of the gaps for all the packets received.

Average Delay: It is the difference in packet spacing at the receiver compared to the sender for a pair of packets. Average Delay is the mean of the delays observed for all the packets.

Average Jitter: Variation in packet arrival times. Discrepancy in milliseconds between when a packet is expected to arrive and when it actually arrives. Average Jitter gives the mean of the jitters observed for all the packets received.

Average Inter Arrival Jitter (RTCP): The average Inter-Arrival Jitter is calculated as a mean of the Inter-Arrival Jitter field appearing in the Sender Report and Receiver Report of RTCP packets

Cumulative Packets Lost (RTCP): The total number of RTP data packets from source SSRC_n that have been lost since the beginning of reception. This will be reported by RTCP SR/RR packets

Max/Min Gap (ms): Maximum and Minimum Gap observed for the session.

Max/Min Delay: Maximum and Minimum Delay observed for the session.

Max/Min Jitter: Maximum and Minimum Jitter observed for the session.

Max/Min RTDelay (ms): It gives the maximum and minimum RTD observed for the session.

Average RTDelay (ms): Round-trip delay on one session is the time taken (in milliseconds) for the packet to travel from PacketScan™ to the other end destination (either caller or callee) and back to PacketScan.

Round Trip Delay (RTD) Calculation

Consider a sip call with traffic on both sides. When a sender report (say SRs) is received on left RTP channel, the packet received time for that sender report will be recorded in PacketScan™ and this time is denoted as R1. When the SR or RR packet (say RRr, which carries information corresponding to SRs packet on left RTP channel) is received on right RTP channel, the received time for that packet will be recorded and this time is denoted as R2. The reception report carried in RRr packet on right RTP channel gives the DLSR (Delay Since Last Sender Report) value. Now, RTD is calculated as below:

$$RTD = R2 - R1 - DLSR$$

The RTD between PacketScan™ and the called party will be displayed on left RTP channel. Follow the same procedure to calculate RTD between PacketScan™ and calling party which is displayed on right RTP channel. The following figure depicts the RTD between the PacketScan™ and the other end. RTD1 is displayed on left RTP channel and RTD2 is displayed on right RTP channel.

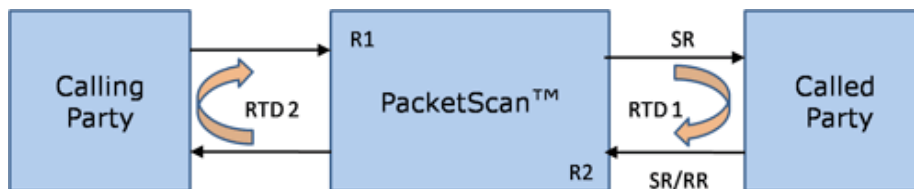


Figure 130: RTD Calculation



Note:

This RTD is from wherever PacketScan™ is to where the called/calling party is and not the RTD as seen by the Caller. For example, if PacketScan™ is in the middle of the network between Calling and Called party, then PacketScan™ can only see half the RTD. For more information about calculating RTD, please refer to RFC 1889.

12.2.2 Graphs

Various graphs related to the RTP session(s) selected are displayed at the bottom of the Summary View. User can select these graphs by using the 'Tab' at the bottom of the Summary View. The different graphs available in Summary View are:

- Active Calls Graph
- Average Jitter Distribution
- E-Model
- RTP Packets Graph
- T.38 Fax Analysis
- Call Graph

12.2.2.1 Active Calls Graph

The Active Calls Graph is a simple line graph, depicting the Number Of Calls Vs Time. A sample (Active calls count) is taken at every 30 seconds.

Functions Invoked By Right Click:

When right-clicked on the graph you get the options to Print, Save the Graph and show 2D view as shown in the figure below:

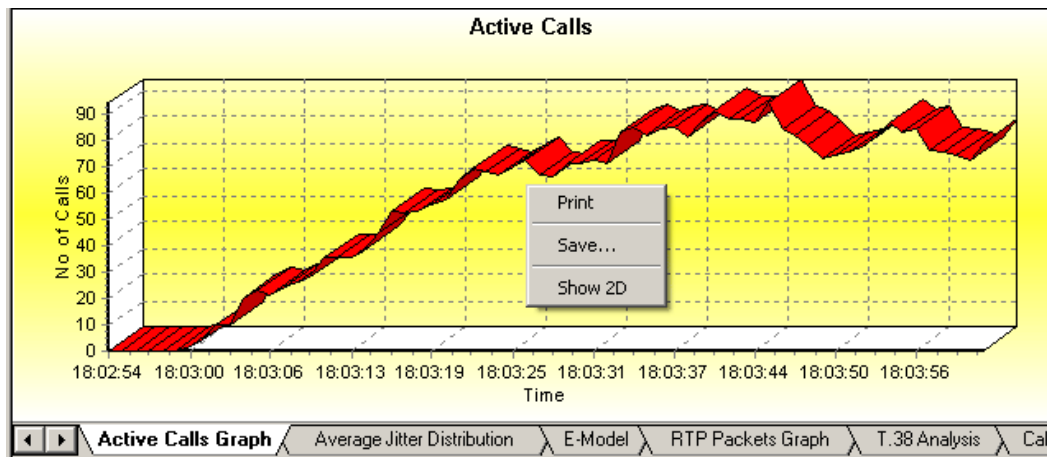


Figure 131: Active Calls Graph

12.2.2.2 Average Jitter Distribution

This is a Bar Graph that plots distribution of the Average Jitter values across the Total Sessions. When right-clicked on the graph you get the options to Print, Save the Graph and shows 2D view. This graph gives a visual representation of the number of sessions having a particular Average Jitter value.

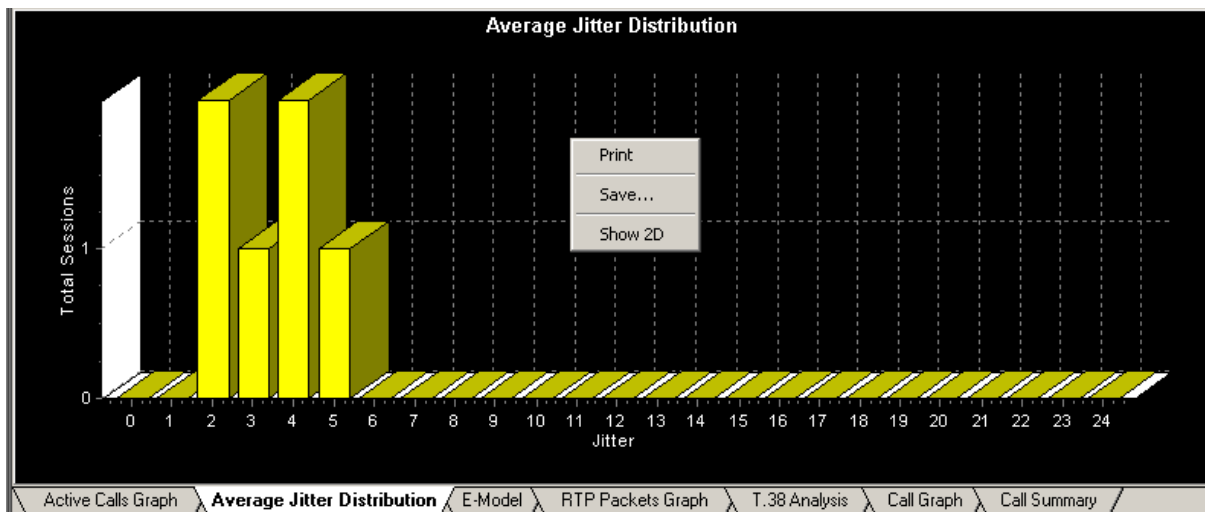


Figure 132: Average Jitter Distribution

12.2.2.3 E-Model

This is part of the statistical pane in Summary View. This graph provides R-factor, MOS and packets discarded against number of sessions. User can select desired graph using the respective buttons provided on top left corner of the graphical pane. Note that all these three graphs show statistics of terminated calls. For more details on E-Model parameters, refer to E-Model.

R-Factor

This is a Bar Graph that plots R-Factor across No of Sessions as shown in the figure below. When right-clicked on the graph you get the options to Print, Save the Graph and shows 2D view. This graph gives a visual representation of the number of sessions having R-Factor value.

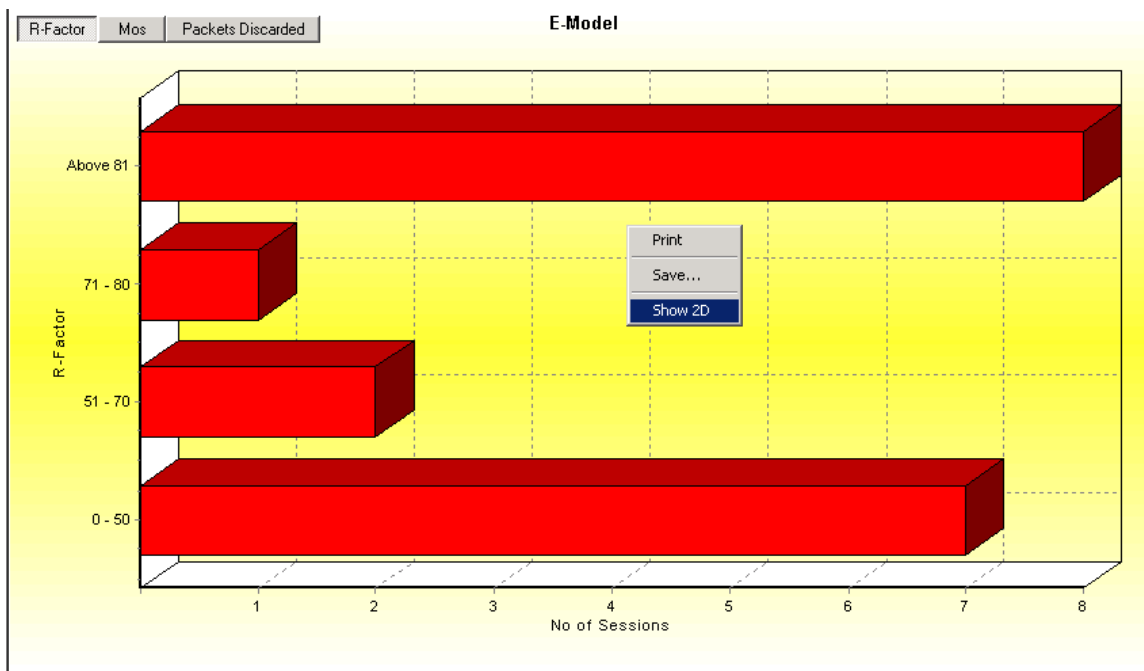


Figure 133: R-Factor

Mean Opinion Score (MOS)

This is a Bar Graph that plots Mean Opinion Score across No. of Sessions as shown in the figure below. When right-clicked on the graph you get the options to Print, Save the Graph and shows 2D view. This graph gives a visual representation of the number of sessions having Mean Opinion Score value.

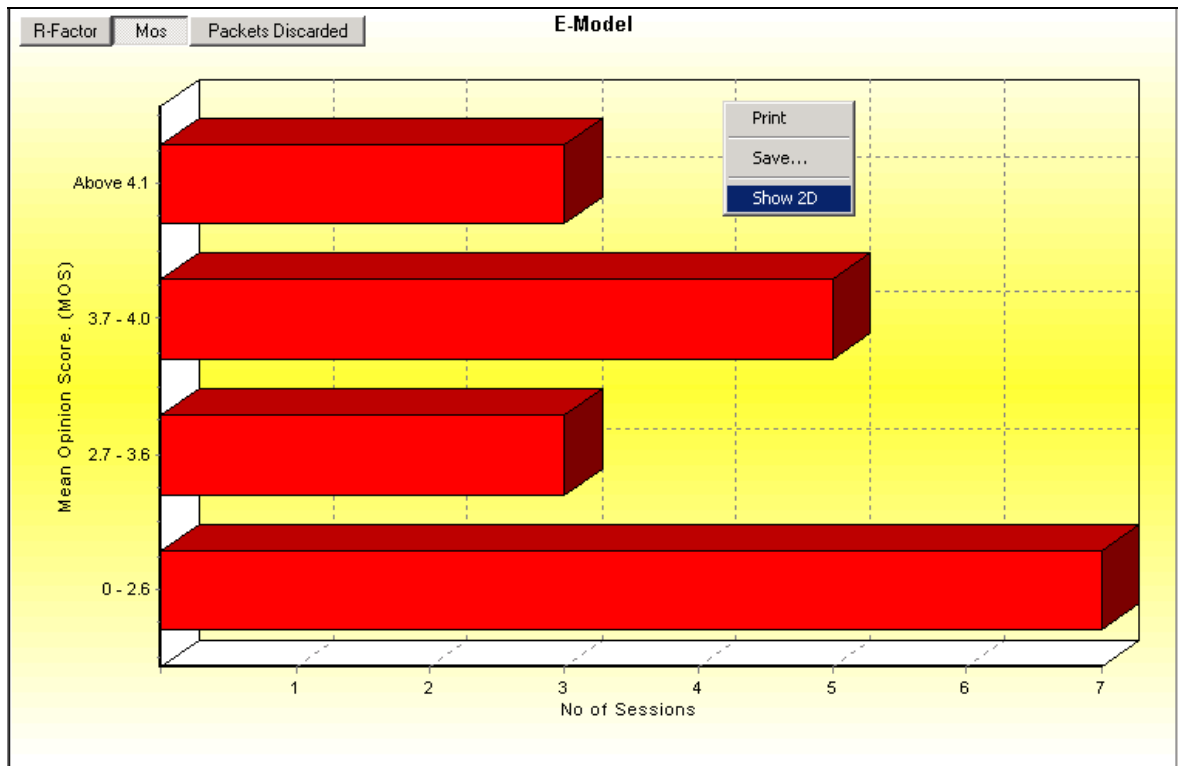


Figure 134: Mean Opinion Score

Packets Discarded

Packets that are received but arrived very late or early. As a result they are discarded by jitter buffer while calculating MOS/R-Factor. This Bar Graph plots Packets Discarded across No. of Sessions as shown in the figure below. When right-clicked on the graph you get the options to Print, Save the Graph and shows 2D view. This graph gives a visual representation of the number of sessions having Packets Discarded value.

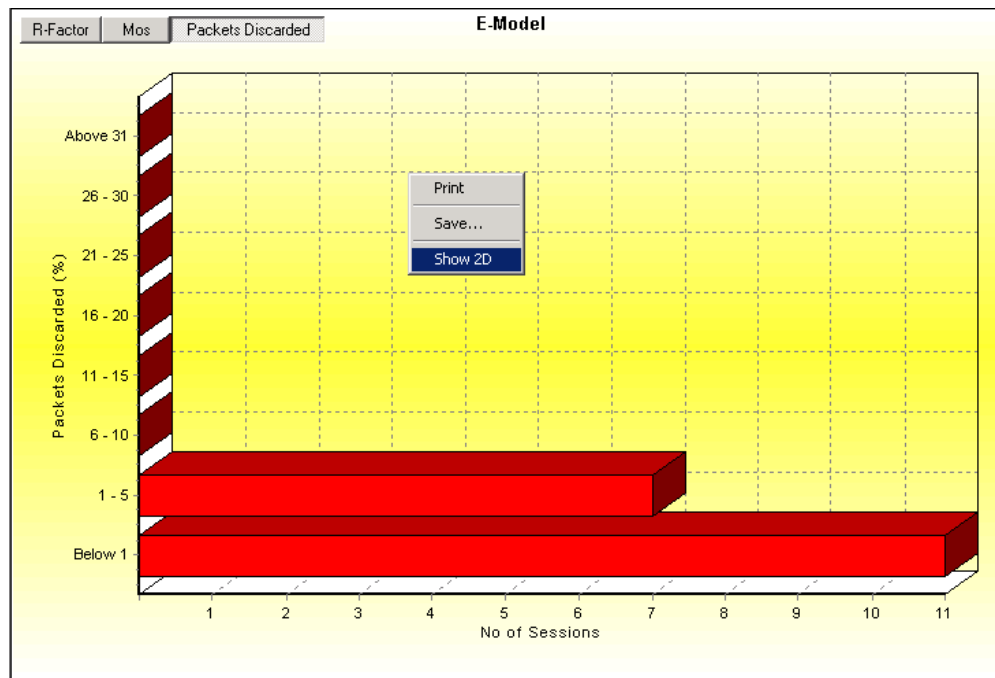


Figure 135: Packets Discarded

12.2.2.4 RTP Packets Graph

This is a Pie Chart that visually compares **Total Audio Packets** against out of ordered packets, missing packets and duplicate packets as shown in the figure below.

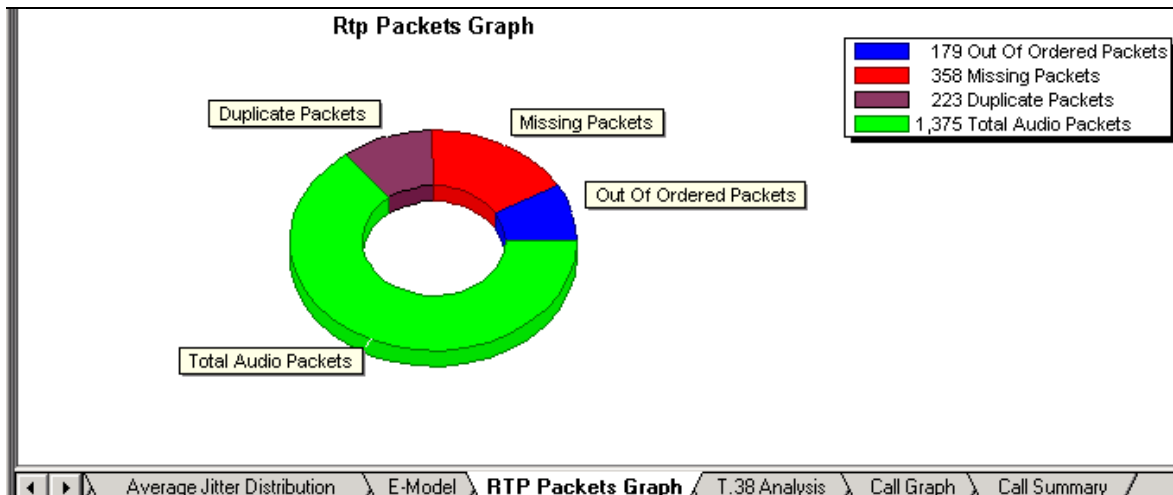


Figure 136: RTP Packets Graph

12.2.2.5 Analysis of Fax over IP (T.38)

PacketScan™ provides Fax (T.38 data) over VoIP monitoring and decoding capability. All the captured fax calls are prefixed with **F** symbol as shown in the figure below. This graph shows the flow of T.38 traffic for the selected Fax call. User can view the decoded message by selecting the messages displayed in the graph as shown in the figure below.

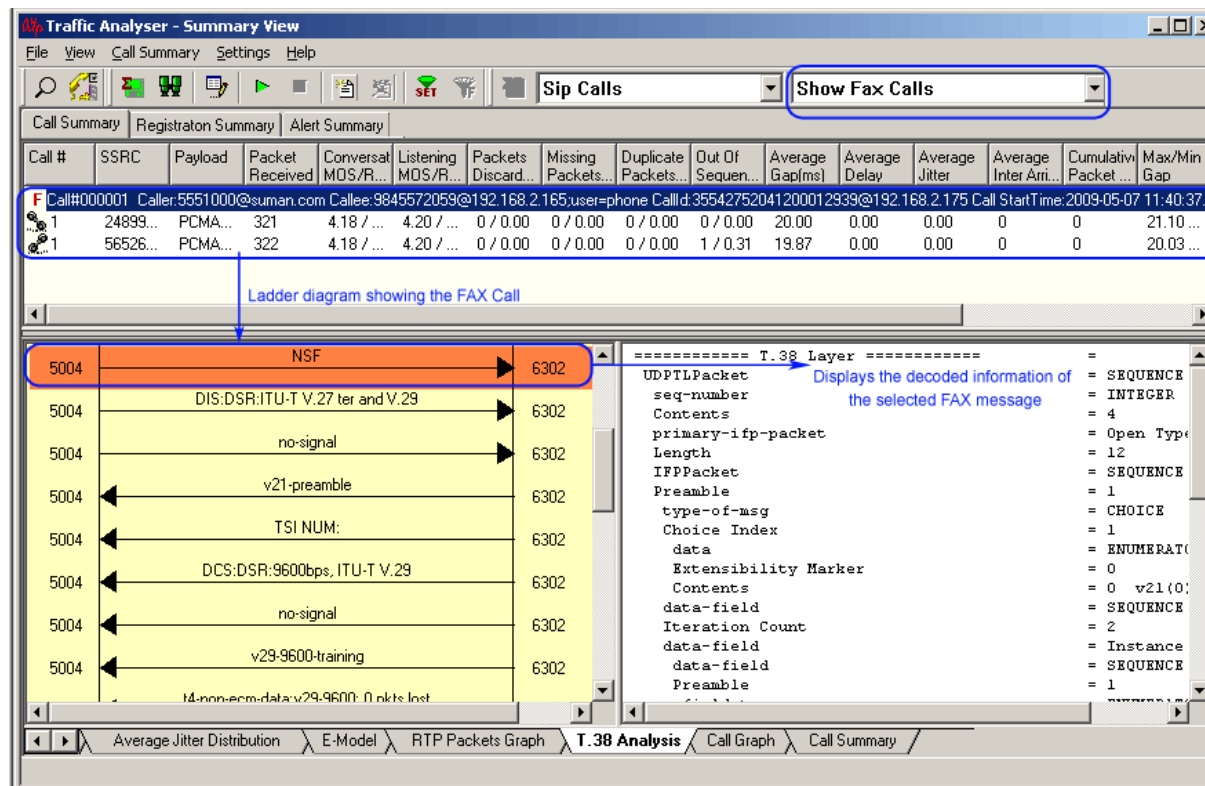


Figure 137: Fax analysis over IP (T.38) Ladder Diagram

To investigate more about the quality of fax captured in the network, users can save the output to a file either in GL proprietary file format (*.HDL) or Ethereal format (*.PCAP). Select **Call Summary > Save Call** menu item or the corresponding tool button shown to invoke Save Call dialog.

User can select the call of interest to save into *.HDL pr *.PCAP file format. For more details, refer to section Save Call explained in Summary View.

The captured fax calls in *.PCAP format can be directly used with GL’s software – **GLInsight™** (Item number – FXT002, MDT002), a tool for Fax & Modem Analysis software to decode the captured fax &

modem files over IP. To analyze the captured Fax calls by PacketScan™ using GLInsight™, users can either save the selected call directly as *.PCAP file format using Save Call feature or convert the *.HDL file format to Ethernet *.PCAP file format using an additional utility **HDLFileConversion.exe** (available in PacketScan™ installation directory). This utility is capable of converting GL's file format *.HDL to Ethernet format file *.PCAP and vice-versa. Refer to [Appendix E: Additional Utilities](#) for more details.

The figure below illustrates the decoding of the PacketScan™ captured Fax over IP call in GLInsight™:

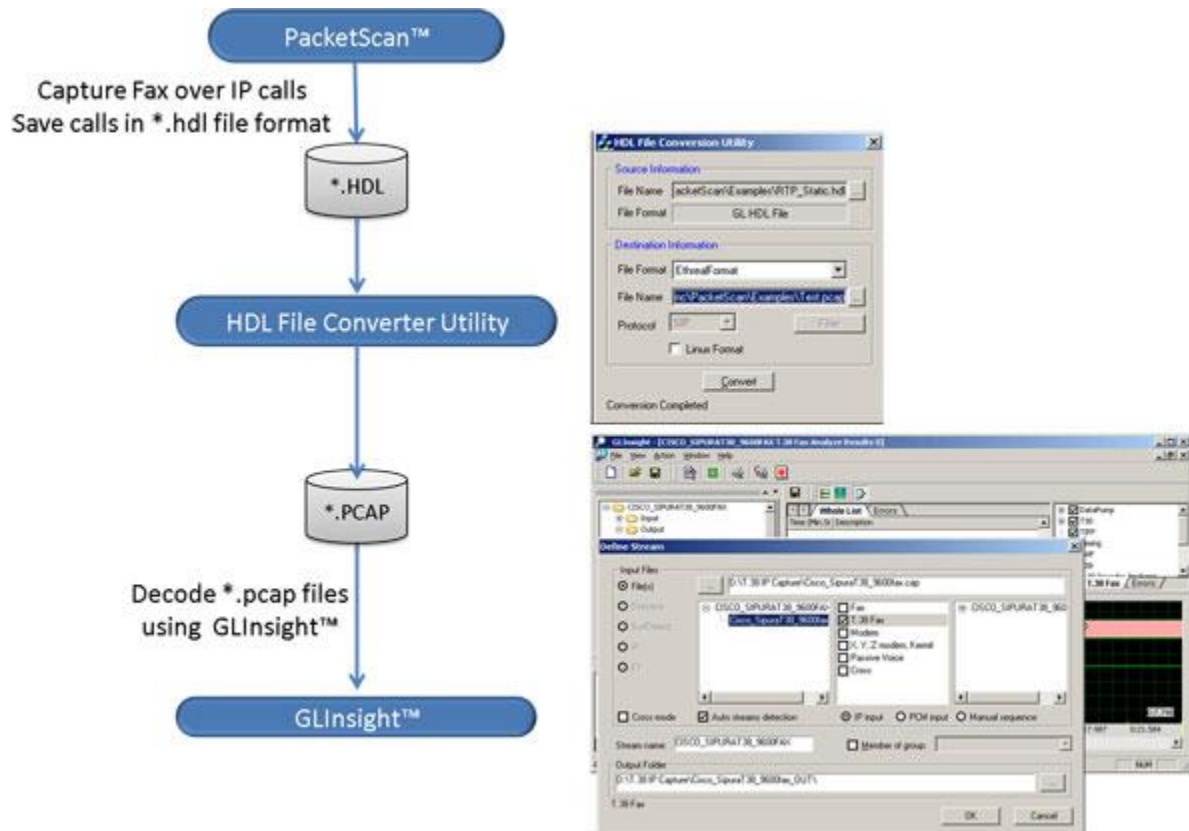


Figure 138: Decode PacketScan™ Captured Fax files in GLInsight™

12.2.2.6 Call Graph

The Call Graph displays the message sequence of captured SIP, H323, MEGACO, IuCS, and GSM A) calls. This includes RTP information such as the Codec type, SSRC, Total RTP packets, and Duration of RTP.

Message sequence pictorially displays the messages exchanged for a particular scenario with relative time stamp of the frame from call start time. For example, in the following figure, the call capture between two IP entities shows that, the call is placed from IP entity 1 (192.168.1.231) to the IP entity 2 (192.168.0.237). User can also view the decoded message by selecting a message displayed in the graph.

SIP Call Graph

The following screen displays a SIP call graph, with decode of the selected message displayed to the right of message sequence.

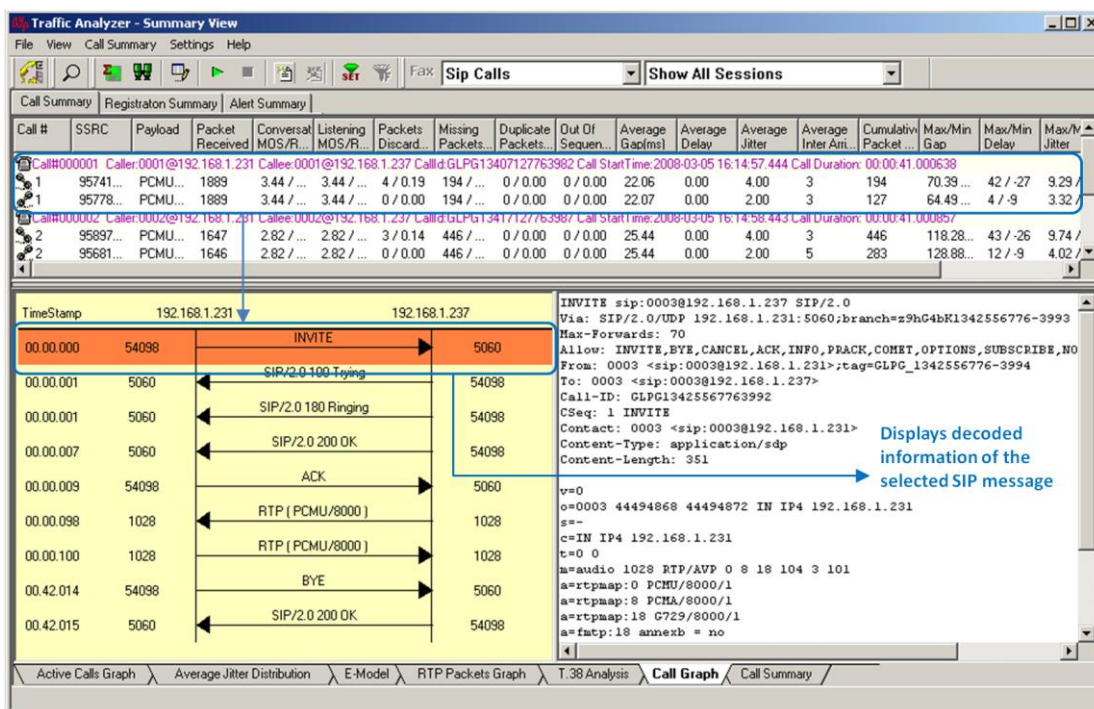


Figure 139: Call Flow Ladder Diagram for SIP Call

MEGACO Call Graph

The following screen displays a MEGACO call graph, with decode of the selected message displayed to the right of message sequence.

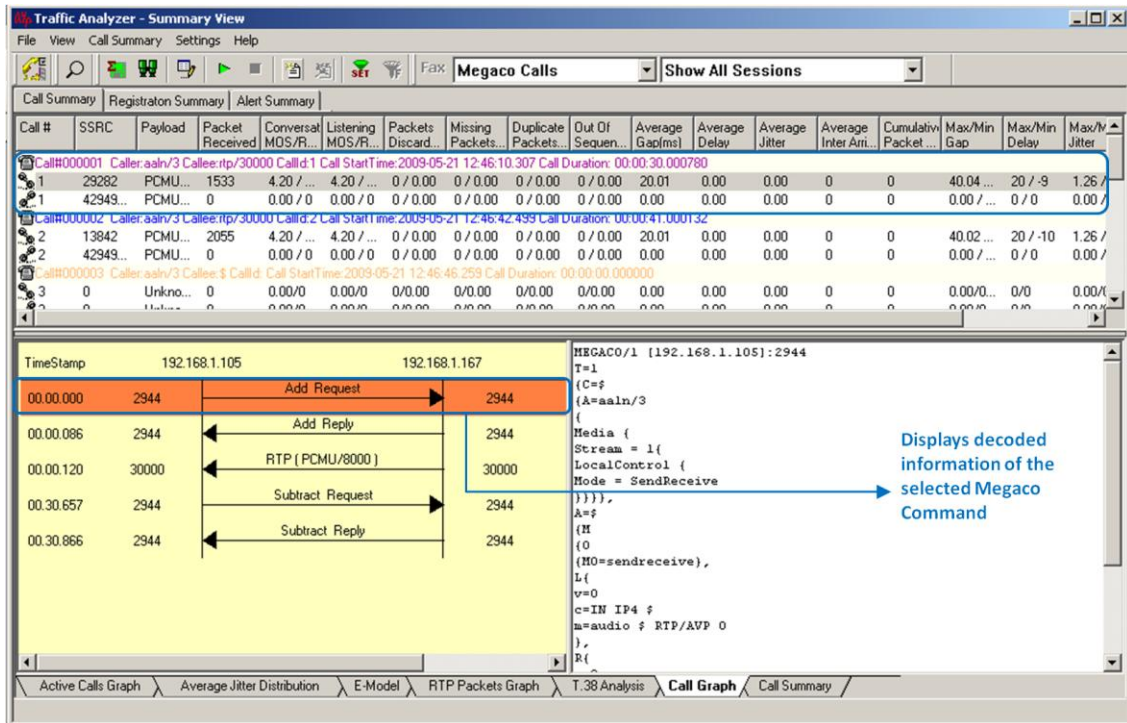


Figure 140: MEGACO Call Flow Ladder Diagram

H.323 Call Graph

The following screen displays a H.323 call graph, with decode of the selected message displayed to the right of message sequence.

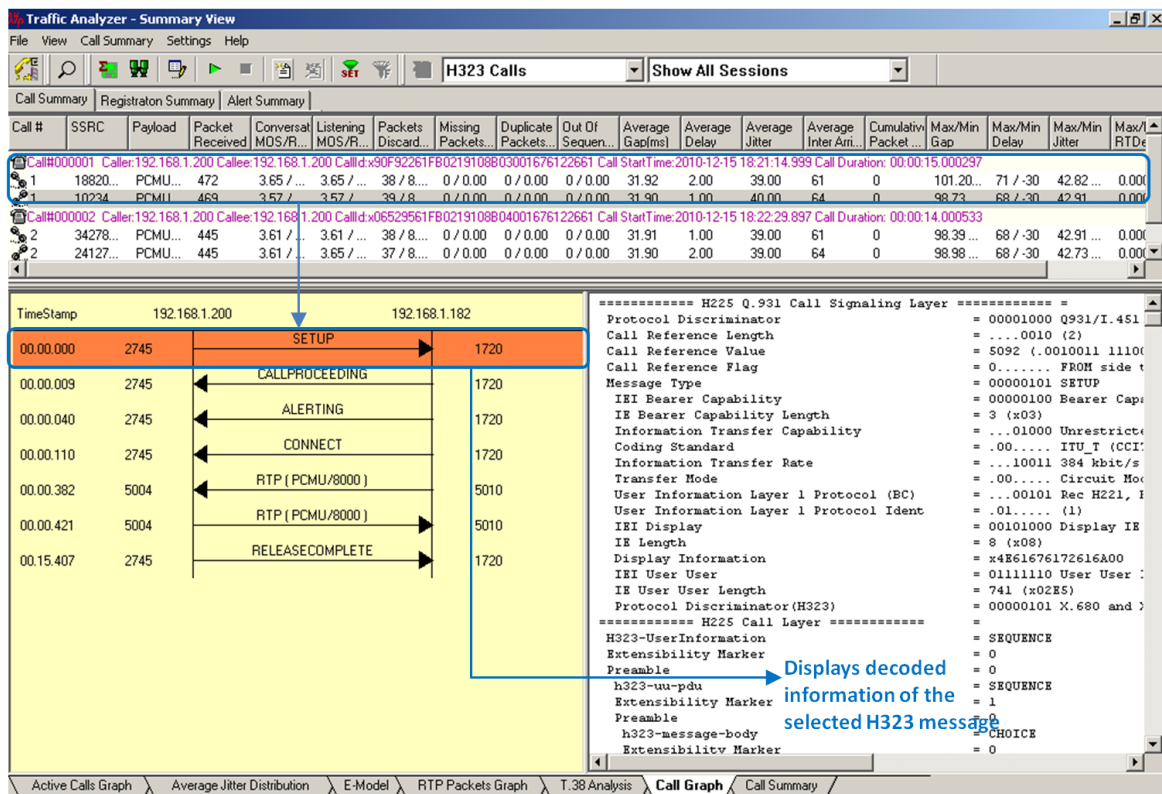


Figure 141: H.323 Call Flow Ladder Diagram

GSM A IP Call Graph

The following screen displays a GSM A call graph, with decode of the selected message displayed to the right of message sequence.

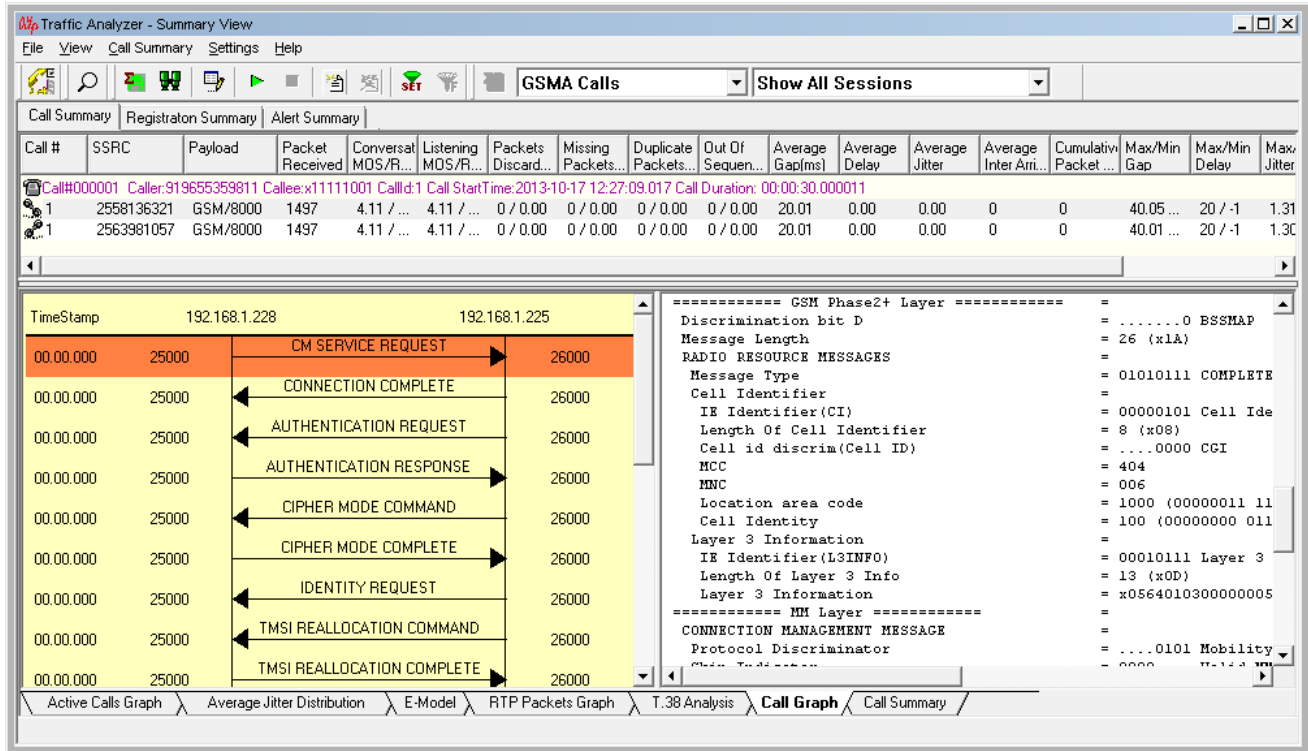


Figure 142: GSMA Call Flow Ladder Diagram

UMTS IuCs Call Graph

The following screen displays a IuCS call graph, with decode of the selected message displayed to the right of message sequence.

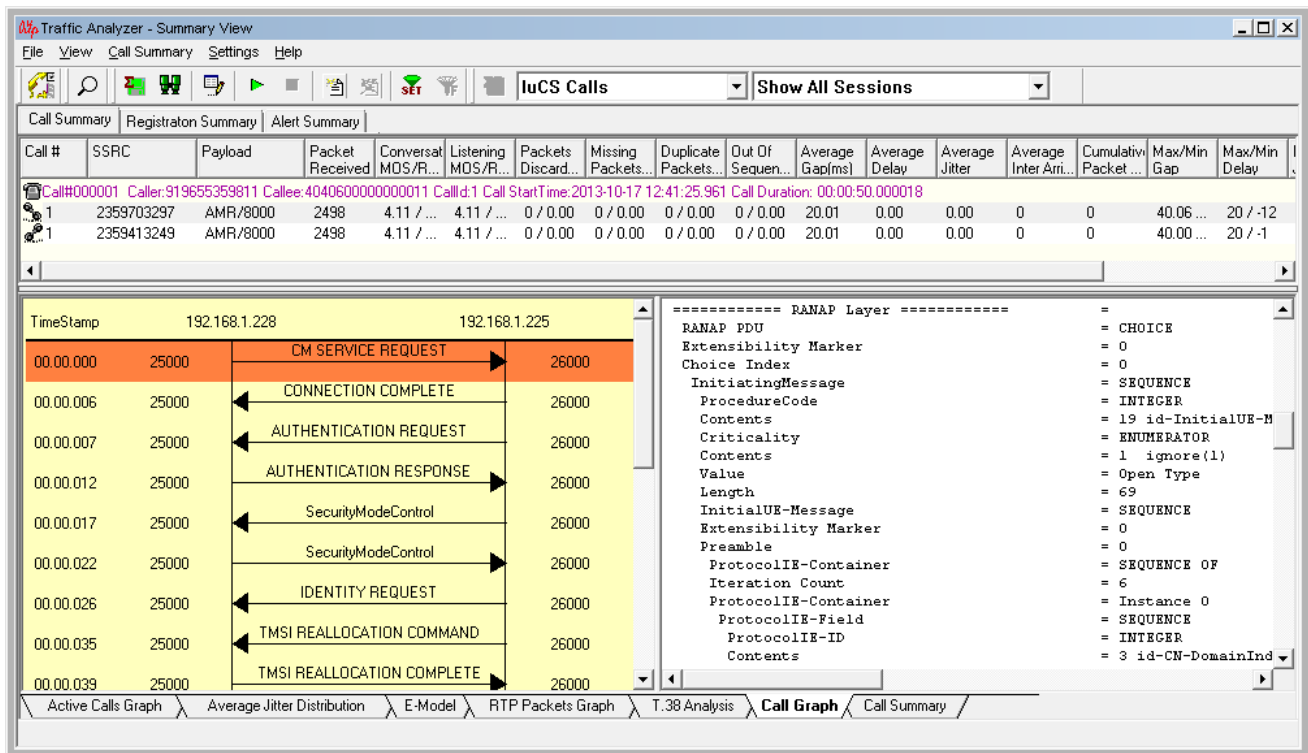


Figure 143: IuCS Call Flow Ladder Diagram

Call Summary – Signaling, Audio, & Video QoS Parameters

The Call Summary tab displays the signaling, audio, and video QoS parameters of each call for SIP, Megaco, RTP, and H.323 in a tabular format. Video QoS parameters are calculated and displayed for all video calls.

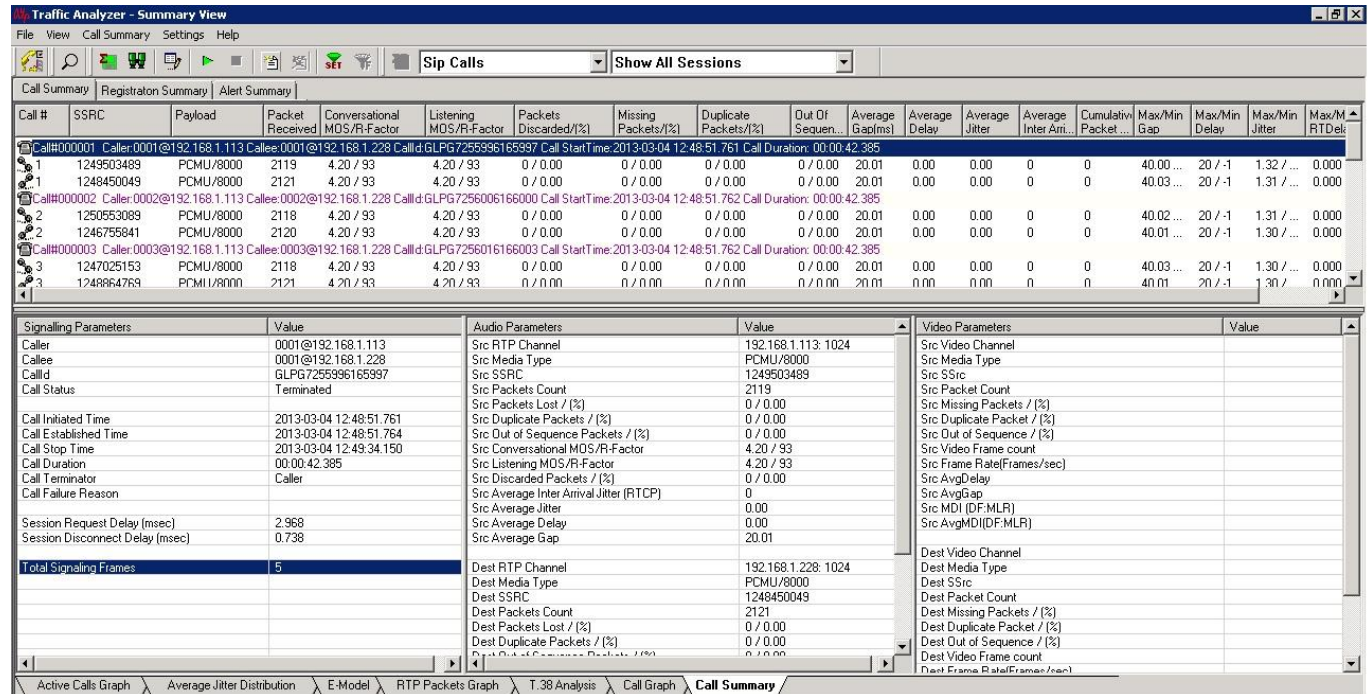


Figure 144: Signaling, Audio and Video Parameters

12.2.2.7 Signaling Parameters

The signaling information includes the following parameters [See Figure above].

- Caller:** It displays the address of the host user agent that sends the INVITE message for a SIP call, while for a MEGACO call; it displays the physical termination value that sends the Add command.
- Callee:** It displays the address of the destination user agent that receives the INVITE message for a SIP call and displays the Ephemeral termination value that sends the Add command for a MEGACO call.
- CallId:** It displays the Call Id for the call that is present in INVITE message for a SIP call, while for a MEGACO call, it displays the context ID for the call that is present in the Add command.
- Call Status:** It displays the status of each call such as terminated, established, and so on.
- Call Initiated Time:** It displays the time when the call initiation message is received.
- Call Established Time:** It displays the call established time.
- Call Stop Time:** It displays the call terminated time.
- Call Duration:** Duration of the call. Represented in hh:mm:secs format.
- Call Terminator:** It displays the terminator of the call, either caller or callee.
- Call Failure Reason:** It displays the failure cause for the failed calls. For example, SIP error cause codes such as 4xx message will be displayed for the failed call.
- Session Request Delay (msec):** Time interval between the moment the Session Initiating message is sent by the originating agent and the first provisional response received by the called party. It is utilized to detect failures or impairments causing delays in responding to a session request. Represented in msec.
- Session Disconnect Delay (msec):** Time interval between the moment the Session Ending message is sent and response received for it. This metric is utilized to detect failures or impairments delaying the time necessary to end a session. Represented in msec.
- Total Signaling Frames:** It Displays the total number of signaling frames received in the selected call.

12.2.2.8 Audio Parameters

The audio parameters [See Figure above] include the source and destination information displayed in the summary pane in a tabular format. These include RTP Channel, Media Type, SSRC value, Packets Count, Missing Packets, Duplicate Packets, Out of Sequence Packets, Conversational MOS/R-factor, Listening MOS/R-factor, Discarded Packets, Average Inter Jitter Arrival, Average Gap, Average Jitter, and Average Delay. Refer to the section [Summary View](#) for more details on these fields.

12.2.2.9 Video QoS Parameters

Video Parameters	Value
Src Video Channel	192.168.1.231 : 8092
Src Media Type	h263-2000/90000
Src SSrc	4257195096
Src Packet Count	2297
Src Missing Packets / (%)	0 / 0.00
Src Duplicate Packet / (%)	0 / 0.00
Src Out of Sequence / (%)	0 / 0.00
Src Video Frame count	512
Src Frame Rate(Frames/sec)	8
Src AvgDelay	38.00
Src AvgGap	125.85
Src MDI (DF:MLR)	116.38 : 0
Src AvgMDI(DF:MLR)	16.82 : 0
Dest Video Channel	192.168.1.254 : 10576
Dest Media Type	h263-2000/90000
Dest SSrc	1125539973
Dest Packet Count	2654
Dest Missing Packets / (%)	0 / 0.00
Dest Duplicate Packet / (%)	0 / 0.00
Dest Out of Sequence / (%)	0 / 0.00
Dest Video Frame count	581
Dest Frame Rate(Frames/sec)	9
Dest AvgDelay	34.00
Dest AvgGap	103.06
Dest MDI (DF:MLR)	128.18 : 0
Dest AvgMDI(DF:MLR)	19.69 : 0

Figure 145: Video QoS Statistics

Video QoS parameters pane displays [See Figure above] the calculated video statistics for each video call in a tabular format. The video QoS parameters include the following source and destination information;

Source / Destination Video Channel: This displays the source and destination IP address along with the port number of the channel.

Source / Destination Media Type: This displays the type of traffic inside the RTP packet. This is mainly the Codec type used for sending / receiving the traffic.

Source / Destination SSRC: SSRC (Synchronization Source) identifier associated with this RTP session. For more information about SSRC and SSRC of Sender, please refer RFC 1889).

Source / Destination Packet Count: This displays the total number of RTP packets received in this session.

Source / Destination Missing Packets / %: This displays the total RTP Packets that have not been received by PacketScan™ in this session. Also, displays the percentage of packets not received to the total number of packets.

Source / Destination Duplicate Packets / %: This gives the count and percentage of total duplicate RTP Packets in this video session.

Source / Destination Out Of Sequence / %: This gives the count and percentage of out sequence packets for the session.

Source / Destination Video Frame Count: This gives total number of video frames received on the session.

Source / Destination Frame Rate (Frames /sec): This gives the number of video frames received per second.

Source / Destination Average Delay: Displays the average (Mean) delay for the session.

Source / Destination Average Gap: This displays the average (Mean) Gap for the session in milliseconds.

Source / Destination MDI (DF:MLR): Media Delivery Index (MDI) parameter displays the appropriate value of DF (Delay Factor) and MLR (Media Loss Rate) separated by a colon only during real-time analysis. **Media Delivery Index (MDI)** measurement is used as a diagnostic tool or as a quality indicator for monitoring a network intended to deliver applications such as streaming media, MPEG video, Voice over IP, or other information sensitive to arrival time and packet loss.

Source / Destination Average MDI (DF:MLR): This gives the average value of DF and MLR.

This method of measuring network jitter is effective for both constant bit rate (CBR) and variable bit rate (VBR) media streams. To achieve this, the RTP protocol must be used, because the measurement correlates the time-stamp field in the RTP header with the arrival time of the IP packets.

Delay Factor (DF): This is based on correlating arrival times of network packets with the time-stamp field in the RTP header and also measurement is based on the Relative Transit Time. The chosen measurement period is 1 second.

In this algorithm, the first packet at the start of the measurement period is considered to have no jitter and is used as a reference packet.

For each subsequent packet, I , which arrives within the measurement period, the Relative Transit Time between this packet and the reference packet is calculated as;

$D(i,0) = (R(i) - R(0)) - (S(i) - S(0))$, where;

$S(i)$ and $S(0)$ are RTP timestamp of packet 'i' and reference packet respectively.

$R(i)$ and $R(0)$ are the time of arrival in RTP timestamp units for packet i and reference packet respectively.

At the end of the measurement period, the maximum and minimum values of D are extracted from the list of D values, and the time-stamped Delay Factor is calculated as:

$TS-DF = D(Max) - D(Min)$

MLR (Media Loss Rate): This is the count of lost or out-of-order flow packets over a selected time interval (1 second), where the flow packets are packets carrying streaming application information.



Note:

Importance of MDI:

The MDI combines the Delay Factor, which indicates potential for impending data loss, and Media Loss Rate as the indicator of lost data. Media Delivery Index (MDI) is a set of measures that can be used to monitor both the quality of a delivered video stream and to show system margin for IPTV systems by giving an accurate measurement of jitter and delay at network level (Internet Protocol, IP), which are the real causes for quality loss.

12.2.3 Counters (Call Quality Parameters)

Counters (Call quality parameters) gives the total count related to the entire sessions. The counters display the count up of the packet details, call session details, and bandwidth consumption details for all protocols as shown in the figure below.

Counter Type	Counters
Total Packet Count	2550
Total Calls	1
Active Calls	0
Completed Calls	1
Purged Calls(Completed)	0
Failed Calls	0
Calls Per Second	0
Total Frames	2550
Last Frame Processed	2550
Total Processed Frames	2550
Frames Purged Before Processing	0
VoIP Bandwidth	0.00
SIP Bandwidth	0.00
H323 Bandwidth	0.00

Counter Type	Counters
Total SIP Packets	7
SIP Calls	1
SIP Active Calls	0
SIP Completed Calls	1
SIP Purged Calls	0
SIP Failed calls	0
SIP Timed Out Calls	0
SIP ForceClosed Calls	0
Session Establishment Ratio	100.00
Session Establishment Effectiveness Ratio	100.00
Session Defects	0.00
Ineffective Session Attempts	0.00
Session Completion Ratio	100.00

SIP \ H323 \ RTP \ MEGACO \ GSMA \ IUCS /

Figure 146: Counter Type

Total Packet Count is the total number of packets Captured by Analyzer which includes both the Signaling packets and RTP, RTCP packets.

Total Calls is a count of total calls processed by PacketScan™, which includes both Active, and Completed calls.

Active Calls is a count of total calls that are presently active.

Completed Calls is a count of total calls that are completed. For a SIP call, this is updated when a BYE packet is received thus indicates the total SIP calls that VPA has processed till its completion.

Purged Calls (Completed) is a count of total calls that are complete and are purged.

Failed Calls is a count of total calls that have failed and timed-out. This counter is updated for all the failure reason’s like INVITE timed out, Call Rejects etc.

Calls Per Second: It displays the number of call attempts per second during real time capture.

Total Frames is the total number of frames the analyzer has captured.

Last Frame Processed is the frame number the analyzer has processed.

Total Processed Frames is the total number of frames the analyzer has processed.

Frames Purged Before Processing is the total number if frames got purged before analyzer could process.

VoIP Bandwidth displays the total bandwidth consumption for VoIP traffic.

SIP Bandwidth displays the total bandwidth consumption for SIP protocol.

H.323 Bandwidth displays the total bandwidth consumption for H.323 protocol.

MEGACO Bandwidth displays the total bandwidth consumption for MEGACO protocol.

IuCs Bandwidth displays the total bandwidth consumption for IuCs protocol.

GSM A Bandwidth displays the total bandwidth consumption for GSM A protocol.

RTP Bandwidth displays the total bandwidth consumption for RTP protocol.



Note:

The VoIP bandwidth and protocols bandwidth consumption values are displayed only in real-time.

12.2.3.1 SIP

Counter Type	Counters
Total SIP Packets	7
SIP Calls	1
SIP Active Calls	0
SIP Completed Calls	1
SIP Purged Calls	0
SIP Failed calls	0
SIP Timed Out Calls	0
SIP ForceClosed Calls	0
Session Establishment Ratio	100.00
Session Establishment Effectiveness Ratio	100.00
Session Defects	0.00
Ineffective Session Attempts	0.00
Session Completion Ratio	100.00

SIP \ H323 \ RTP \ MEGACO \ GSMA \ IUCS

Figure 147: SIP Counters

Total SIP Packets is a count of Total number of SIP Packets captured.

SIP Calls is a count of total SIP calls processed by RRA, which includes both Active, and Completed calls.

SIP Active Calls is a count of total SIP calls that are presently active.

SIP Completed Calls is a count of total SIP calls that are completed. This is updated when a BYE packet is received thus indicating the total SIP calls VPA has processed till its completion.

SIP Purged Calls is a count of total SIP calls that are complete and are purged.

SIP Failed Calls is a count of total SIP calls that have failed. This counter is updated for all the failure reasons like INVITE time out, Call Rejects etc.

SIP Timed Out Calls is a count of number of SIP timed out calls. A call is considered timed out if no packets are received on the call for the specified time out period.

SIP Force Closed Calls is a count of number of SIP forced closed calls. A call can be force closed if an existing call uses same IP:Port pair for media used by any new incoming call. In this case existing call will be force closed to make way for new call.

Session Establishment Ratio (SER) is defined as the ratio of the number of new session INVITE requests resulting in a 200 OK response, to the total number of attempted INVITE requests less INVITE requests resulting in a 3XX response. This gives the percentage of successfully established sessions.

SER = ((# of INVITE Requests w/ associated 200 OK / Total # of INVITE Requests)-(# of INVITE Requests w/ 3XX Response)) x 100

Session Establishment Effectiveness Ratio (SEER) is complimentary to SER, but is intended to exclude the potential effects of the terminating UAS from the metric. SEER is defined as the ratio of number of INVITE requests resulting in a 200 OK response and INVITE requests resulting in a SIP codes 480, 486, or 600 to the total number of attempted INVITE requests less INVITE requests resulting in a 3XX, 401, 402, and 407 response. This gives the percentage of successfully established sessions less common UAS failures.

SEER = ((# of INVITE Requests w/ associated 200 OK, 480, 486, or 600) / (total # of INVITE Requests)-(# of INVITE Requests w/"" Response)) x 100

Session Defects provide a subset of SIP failure responses, which consistently indicate a failure in dialog processing. This is calculated as percentage of the number of INVITE Requests with associated SIP codes 500, 503, or 504 to the total number of INVITE requests. This gives the percentage of defective sessions.

SDR = (# of INVITE Requests w/ associated 500, 503, or 504/ Total # of INVITE Requests) x 100

Ineffective Session Attempts (ISA) occur when a proxy or agent internally releases a setup request with a failed or overloaded condition. This is calculated as the percentage of ineffective session attempts to the total number of INVITE requests. This gives the percentage of ineffective session attempts.

ISA % = (# of ISA / Total # of Session Requests) x 100

Session Completion Ratio (SCR) is a calculated as the percentage of number of successfully completed sessions to the total number of session request. A session completion is defined as a SIP dialog, which completes without failing due to a lack of response from an intended proxy or UA.

SCR % = (# of Successfully Completed Sessions / Total # of Session Requests) x 100

SIP Invites shows the number of SIP Invites in a captured session.

SIP Acknowledgements gives the number of SIP Acknowledges in a captured session.

SIP Byes shows the number of SIP Byes in a captured session.

SIP Cancels provides the number of SIP Cancels in a captured session.

SIP Registers is the number of times registering to a register –SIP Proxy Server running on third machine.

12.2.3.2 H323

Counter Type	Counters	
Total H323 Packets	29	
H323 Calls	2	
H323 Active Calls	0	
H323 Completed Calls	0	
H323 Purged Calls	0	
H323 Failed calls	0	
SetUp messages	2	
Connect Messages	2	
Release Complete Messages	4	

SIP \ **H323** \ RTP \ MEGACO \ GSM \ IUUCS \

Figure 148: H.323 Counters

Total H.323 Packets is a count of Total number of H.323 Packets captured.

H.323 Calls is a count of total H.323 calls processed by RRA, which includes both Active, and Completed calls.

H.323 Active Calls is a count of total H.323 calls that are presently active.

H.323 Completed Calls is a count of total H.323 calls that are completed. This is updated when a BYE packet is received thus indicating the total H.323 calls that VPA has processed till its completion.

H.323 Purged Calls is a count of total H.323 calls that are complete and are purged.

H.323 Failed Calls is a count of total H.323 calls that have failed. This counter is updated for all the failure reasons like SETUP timed out, Call Rejects etc.

Setup messages show the total number of H.323 SETUP messages captured.

Connect Messages shows the total number of H.323 CONNECT messages captured.

Release Complete Messages shows the total number of H.323 RELEASE COMPLETE messages captured.

12.2.3.3 MEGACO

Counter Type	Counters
MEGACO Calls	1
MEGACO Active Calls	0
MEGACO Completed Calls	1
MEGACO Purged Calls	0
MEGACO Failed calls	0
MEGACO Adds	2
MEGACO Modifys	2
MEGACO Subtracts	2
MEGACO AuditValues	0
MEGACO AuditCapabilitys	1

SIP | H323 | RTP | **MEGACO** | GSMA | IUCS

Figure 149: MEGACO Counters

Total MEGACO Packets is a count of Total number of MEGACO Packets captured.

MEGACO Calls is a count of total MEGACO calls processed by RRA, which includes both Active, and Completed calls.

MEGACO Active Calls is a count of total MEGACO calls that are presently active.

MEGACO Completed Calls is a count of total MEGACO calls that are completed. This is updated when a Subtract command is received thus indicating the total MEGACO calls that VPA has processed till its completion.

MEGACO Purged Calls is a count of total MEGACO calls that are complete and are purged.

MEGACO Failed Calls is a count of total MEGACO calls that have failed. This counter is updated for all the failure reasons like timed out, Call Rejects etc.

MEGACO Adds shows the number of Add commands in a captured session.

MEGACO Modifys shows the total number of Modify command in a captured session.

MEGACO Subtracts shows the total number of Subtract command in a captured session.

MEGACO Audit Values shows the total number of Audit Value command in a captured session.

MEGACO Audit Capabilities shows the total number of Audit Capability command in a captured session.

12.2.3.4 RTP

Counter Type	Counters
Total RTP Sessions	1
Active RTP Sessions	0
Completed RTP Sessions	2
RTP Bytes	237280
Total RTCP Packets	4
RTCP Sender Reports	4
RTCP Receiver Reports	0
RTCP Bye Packets	1
Total Missing Packets /(%)	0/0.00
Total Out of Sequence Packets /(%)	0/0.00
Total Duplicate Packets /(%)	0/0.00
Total Discarded Packets /(%)	0/0.00

SIP \ H323 \ **RTP** \ MEGACO \ GSM \ IUCS

Figure 150: RTP Counters

Total RTP Packets is a count of total RTP packets captured across all calls.

Total RTP Session is a count if RTP session's that are active and RTP sessions completed.

Active RTP Session provides the total number of RTP sessions that are active presently.

Completed RTP session gives the total number of RTP sessions completed.

RTP Bytes this gives the number of Bytes of RTP data received.

Total RTCP Packets is the total RTCP packets captured across all calls.

RTCP Sender Reports is the total RTCP Sender Reports captured across all calls.

RTCP Receiver Reports is the total RTCP Receive Reports captured across all calls.

RTCP Bye Packets gives the total RTCP Bye Packets captured across all calls.

Total Missing Packets /(%) is total count and percentage of RTP packets missing across all calls.

Total Out of Sequence Packets /(%) is total count and percentage of RTP packets received out of sequence across all calls.

Total Duplicate Packets/(%) is total count and percentage of duplicate RTP packets received across all calls.

Total Discarded Packets/(%) is total count and percentage of RTP packets discarded by jitter buffer while calculating MOS/R-Factor scores across all calls.

12.2.3.5 GSM A

Counter Type	Counters	
Total GSMA Packets	30	
GSMA Calls	1	
GSMA Active Calls	0	
GSMA Completed Calls	1	
GSMA Purged Calls	0	
GSMA Failed Calls	0	
Voice Calls	1	
SMS Calls	0	
Location Update Calls	0	
Setup Messages	1	
Connect Messages	1	
DisConnect Messages	1	

◀ ▶ RTP MEGACO **GSMA** IUCS

Figure 151: GSMA Counters

Total GSMA Packets is the total GSM A packets captured across all calls.

GSMA Calls is the total of all GSM A calls.

GSMA Active Calls provides total number of GSM A calls that are active presently.

GSMA Completed Calls provides total number of GSM A completed calls.

GSMA Purged Calls provides total number of Purged GSM A calls.

GSMA Failed Calls provides total number of GSM A failed calls.

Voice Calls provides total number of GSM A voice calls.

SMS Calls provides total number of SMS calls.

Location Update Calls provides total number of GSM A location updated calls.

Setup Messages provides total number of GSM A calls that are active presently.

Connect Messages provides total number of connected messages.

DisConnect Messages provides total number of disconnected messages.

12.2.3.6 IuCS

Counter Type	Counters
Total IuCS(RANAP)Packets	30
IuCS Calls	1
IuCS Active Calls	0
IuCS Completed Calls	1
IuCS Purged Calls	0
IuCS Failed Calls	0
Voice Calls	1
SMS Calls	0
Location Update Calls	0
Setup Messages	1
Connect Messages	1
DisConnect Messages	1

◀ ▶ RTP MEGACO GSMA IUCS /

Figure 152: IuCS Counters

Total IuCS (RANAP) Packets is the total IuCS packets captured across all calls.

IuCS Calls is the total of all IuCS calls.

IuCS Active Calls provides total number of IuCS calls that are active presently.

IuCS Completed Calls provides total number of IuCS completed calls.

IuCS Purged Calls provides total number of Purged IuCS calls.

IuCS Failed Calls provides total number of IuCS failed calls.

Voice Calls provides total number of IuCS voice calls.

SMS Calls provides total number of SMS calls.

Location Update Calls provides total number of IuCS location updated calls.

Setup Messages provides total number of IuCS calls that are active presently.

Connect Messages provides total number of connected messages.


DisConnect Messages provides total number of disconnected messages.

12.3 File Menu Options

12.3.1 Export Displayed Summary

The Export option allows user to save the call records and statistics to a comma-separated (comma-delimited) file. The exported summary can be imported into a database or spreadsheet for post processing.

To open the Export Displayed Summary screen:

- Select **File > Export Displayed Summary** from the main menu as shown in the figure below or
- Click  from the toolbar

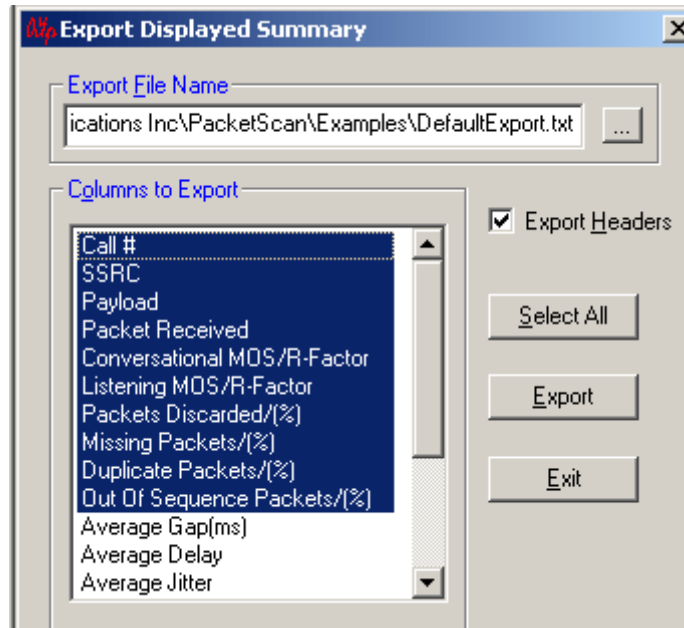


Figure 153: Export Displayed Summary

- Select a directory to export the statistics using the browse button under the **Export File Name** pane
- Select the columns to be exported under **Columns to Export** pane in order to export them
- Select/Check **Export Headers** option to select the names of the headers that are selected by the user. These names will appear at the top of the comma-separated file
- Click **Select All** to select all the columns at once
- Click **Export** to start the actual process of writing the columns to the comma-separated file. A status at the bottom indicating that the application is busy exporting is indicated by the Exporting status message that appears at the bottom
- Click **Exit** to close the screen

The Export option can be invoked both in Online and Offline mode. In online mode, the most recent values collected will be exported. The fact that the comma-separated file can be opened in spreadsheet etc will allow easier and more powerful search/find techniques to be used on the gathered data.

12.3.2 Export Terminated Calls

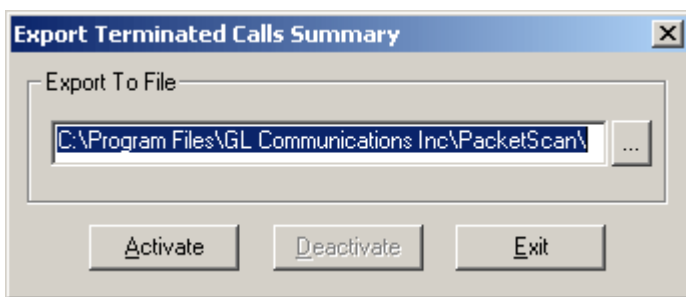


Figure 154: Export Summary Calls Summary

The PacketScan™ PDA can export terminated call details from the live capture in text files (csv format). This feature requires activating the **Export Terminated Calls** option from PDA prior to live capturing.

Choose the destination folder where the file is to be exported and click **Activate**. As the capture is proceeding, the details of these calls such as Caller, CallID, Start time, Call duration, Payload, Packet Received, Missing, Duplicate, and Out of sequence Packets, Average Gap, Jitter, Delay, Arrival and so on are exported to the text file.

This structured text (csv) file can be imported easily into Excel® using the custom Excel® addin (**Excel-Dashboard-Tool-IP.xlsm**) to generate different chart types, such as call volumes, call duration, call failure causes, CMOS, LMOS, packet loss, and more.

Excel-Dashboard-Tool-IP.xlsm addin is a custom application developed by GL Communications to leverage from the Microsoft® Excel's capability to handle large volumes of data, filter for specific calls, use the inbuilt statistics, automation and graphical features to analyze the call detail records (CDRs). Refer to [PacketScan Excel Report Quick Start Guide](#) for more details.

12.4 View Menu Options

12.4.1 Toolbar/Status Bar

These options enables user to select/deselect the required toolbars. VPA has three toolbars as shown below.

- Main Bar
- Play Sound

The Main Bar contains shortcut buttons for moving between Summary and Detail window, and bringing VPA into foreground. The icon for the Summary View and Detail View changes according to the change in the selection respectively.

The 'Play Sound' bar contains shortcut buttons for the Audio options. These include, Play Audio to Sound Card, Pause Audio and Stop Audio. It also contains the Write to Audio File and Stop Write to Audio File options. Also it contains Find, Single Call Statistics, Export shortcut buttons and Saving Completed Calls as separate HDL files as shown in the figure below.



Figure 155: Play Sound Toolbar

12.4.2 Find

The Find option is used to search for a particular item from the three tables, Summary Table in Summary View and the Detail RTP Session (left) and Detail RTP Session (right) in the Detail View.

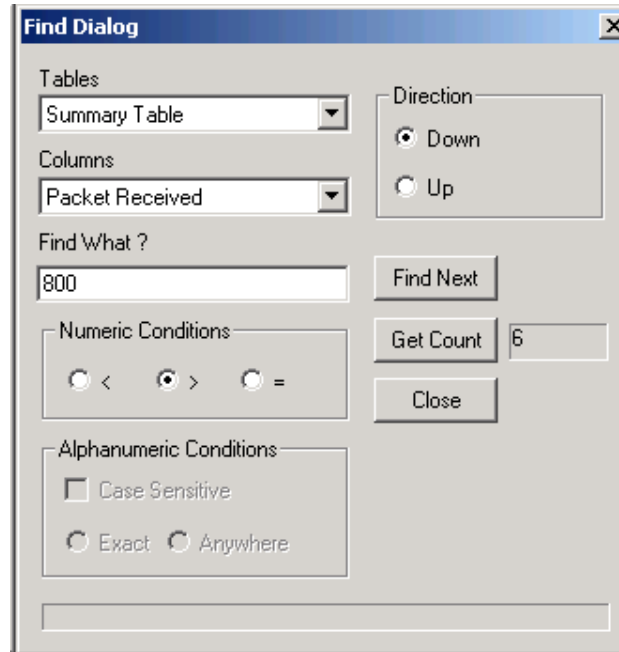


Figure 156: Find Dialog

Tables: Select a table from the Tables dropdown menu in which a search has to be done, which are listed below:

- Summary Table
- Detail RTP Session (left)
- Detail RTP Session (right)

Columns: The columns of the above mentioned tables could be searched for any value using the dropdown menu.

Example: Columns in the summary table such as From, To, SIP Call Id, Call #, SSRC, Payload, Packets received ...

Find What: Enter the value, which is to be searched in this field.

Find Next: Click this to find the next item that matches the criteria.

Get Count: This is an additional feature provided here, which shows the count of the number of times the value has occurred in the selected table instead of searching for a particular value and selecting the entry.


Direction: This option allows the user to select either upwards using the Up radio button, from the current selected item in the table (If no selection is made search starts from the first item) or downwards using the Down radio button. Whenever a match is found, the particular item (row) is highlighted.

Close: Click **Close** to exit this dialog box.


From the Tables combo box, user can decide which table he wants to search, the options being Summary Table in Call Summary View, Detail RTP Table (left) for the left table and Detail RTP Table (right) for the right table in the Call Detail View. Once user selects the table, the Columns combo box will be updated to reflect the selection. The user then has to select/edit the selection to be searched.

One additional feature provided with the Find dialog of RRA, is that the user can get the Count of the number times the "search item" occurs in the table (this depends on the Direction option as well).

12.4.3 Call Detail View

- Select **View > Call Detail View** from the main menu to open the Detail View screen or
- Click  from the tool bar

12.4.4 Go To Analyzer

- Select **View > Go To Analyzer** from the main menu to open the VPA screen or
- Click **GoTo Analyzer**  from the toolbar

12.5 Call Summary Menu Options

12.5.1 Protocols

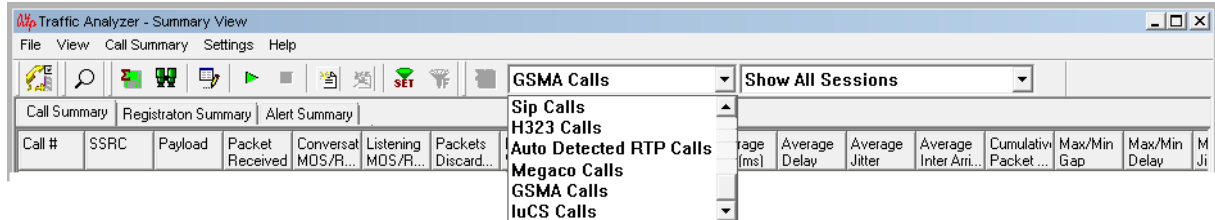


Figure 157: Protocols

Protocols supported in PacketScan™ are as follows:

- Sip Calls
- H.323 Calls
- Auto Detect RTP Sessions
- Megaco Calls
- GSMA Calls
- IuCS Calls

Sip Calls

Select **Call Summary > Protocol > Sip Calls** to open the Sip calls pane or select Sip Calls option from the dropdown box on the Extra tool bar. Calls that are attempted, failed, established using SIP signaling and summary regarding the Traffic flow pertaining to that call is displayed.

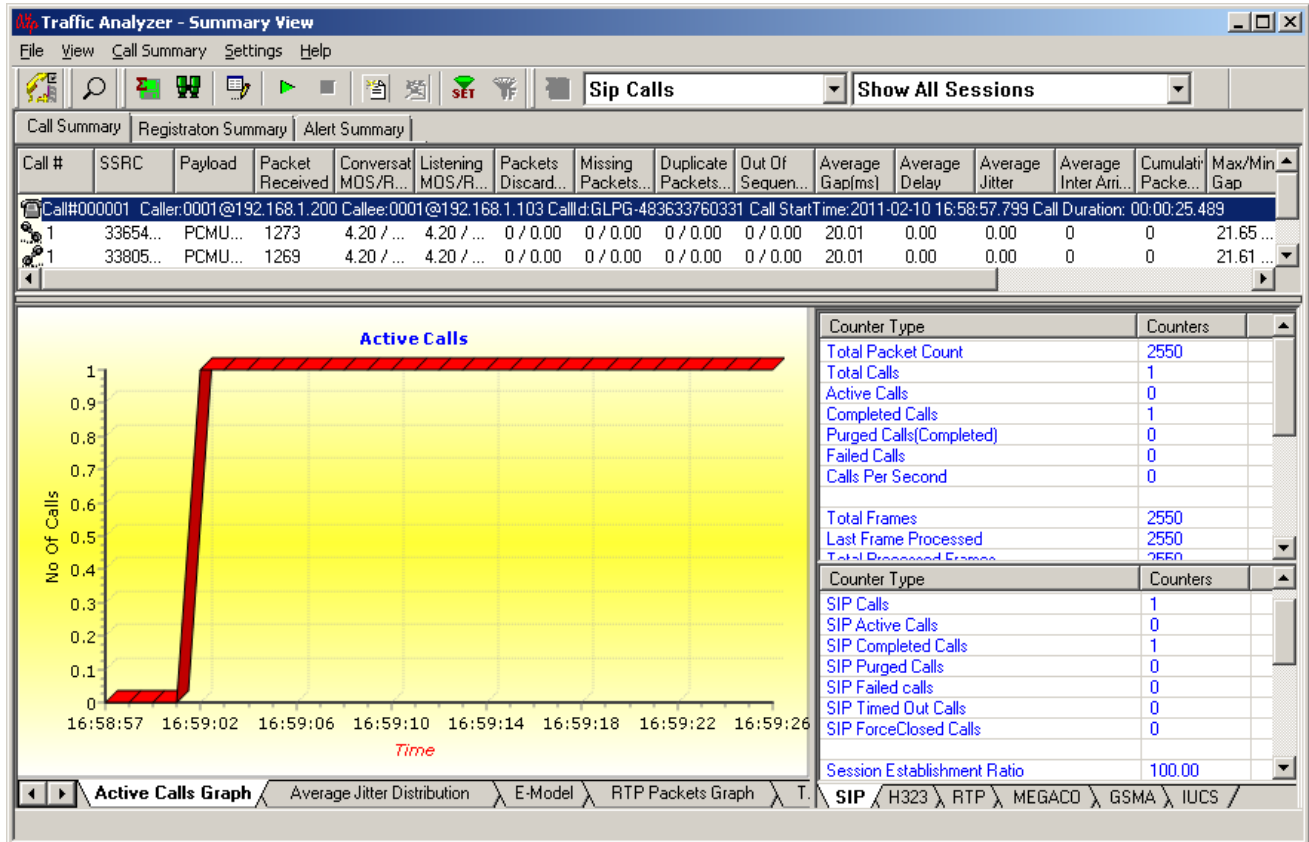


Figure 158: SIP Calls

H.323 Calls

Select **Call Summary > Protocol > H.323 Calls** to view the H.323 calls or select H.323 Calls option from the drop-down box on the Extra tool bar.

Calls that are attempted, established, failed using H.323 signaling and the summary regarding Traffic flow pertaining to that call is shown.

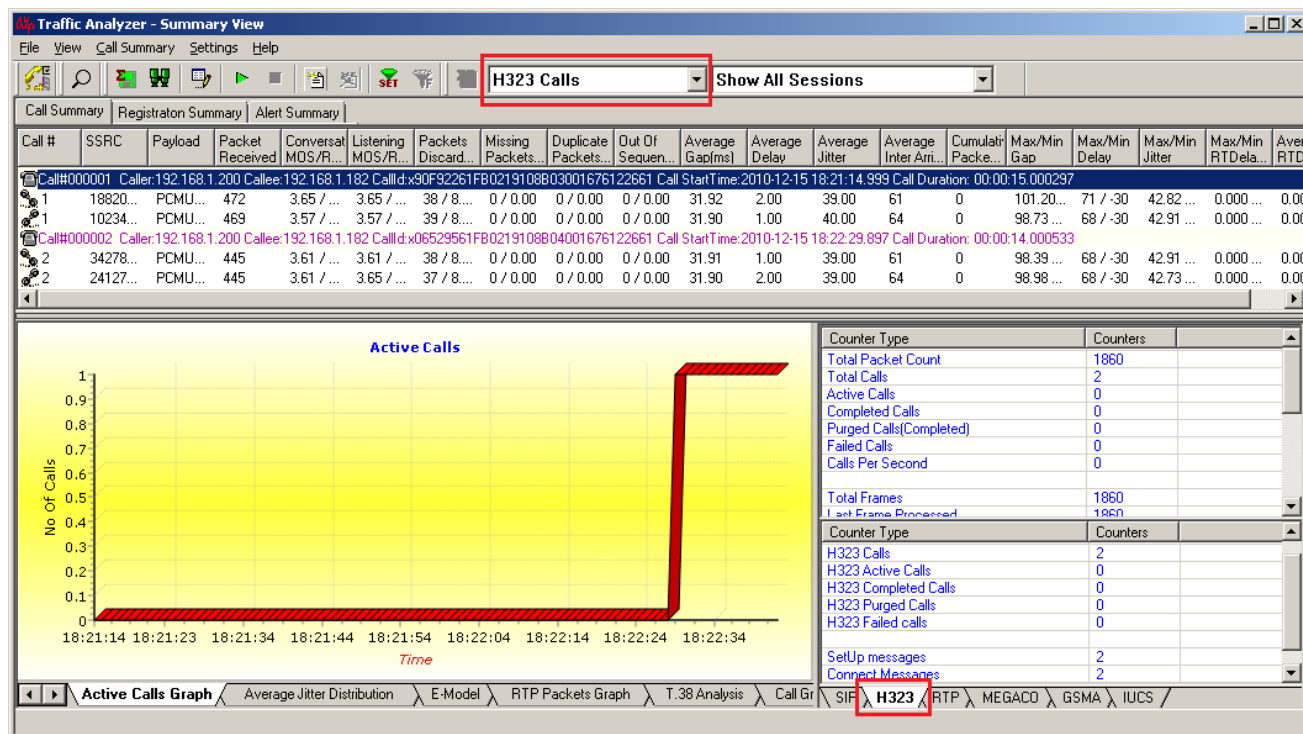


Figure 159: H.323 Calls

Auto Detect RTP

Select **Call Summary > Protocol > Auto Detect RTP** to view the Auto Detect RTP pane or select Auto Detect RTP Calls option from the dropdown box on the Extra tool bar. If the Auto Detect RTP is checked in Capture Filter, then any traffic that is flowing and Signaling information is not provided to Analyzer are shown in this window. PDA associates Left and Right auto Detected RTP sessions to a single call.

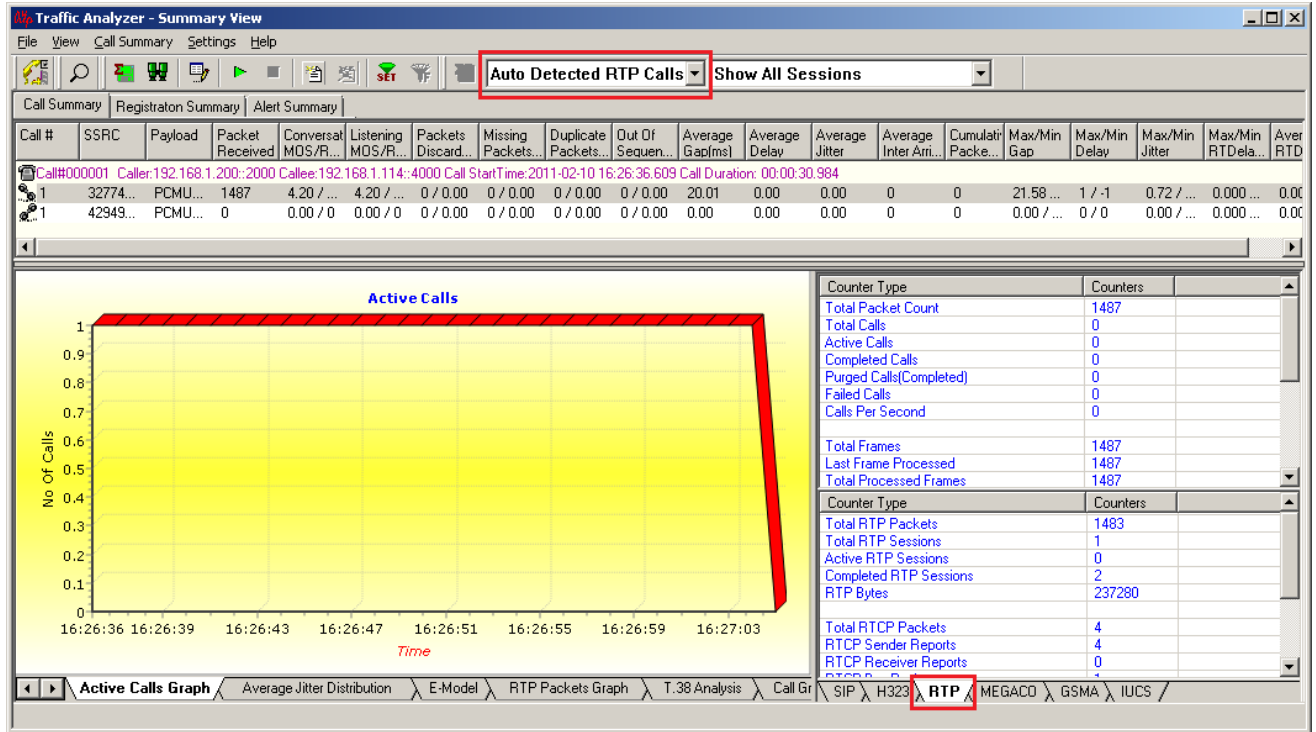


Figure 160: Auto Detected RTP Calls

Megaco Calls

Select **Call Summary > Protocol > Megaco Calls** to open the Megaco calls pane or select Megaco Calls option from the dropdown box on the Extra tool bar. Calls that are attempted, failed, established using Megaco signaling and summary regarding the Traffic flow pertaining to that call is displayed.

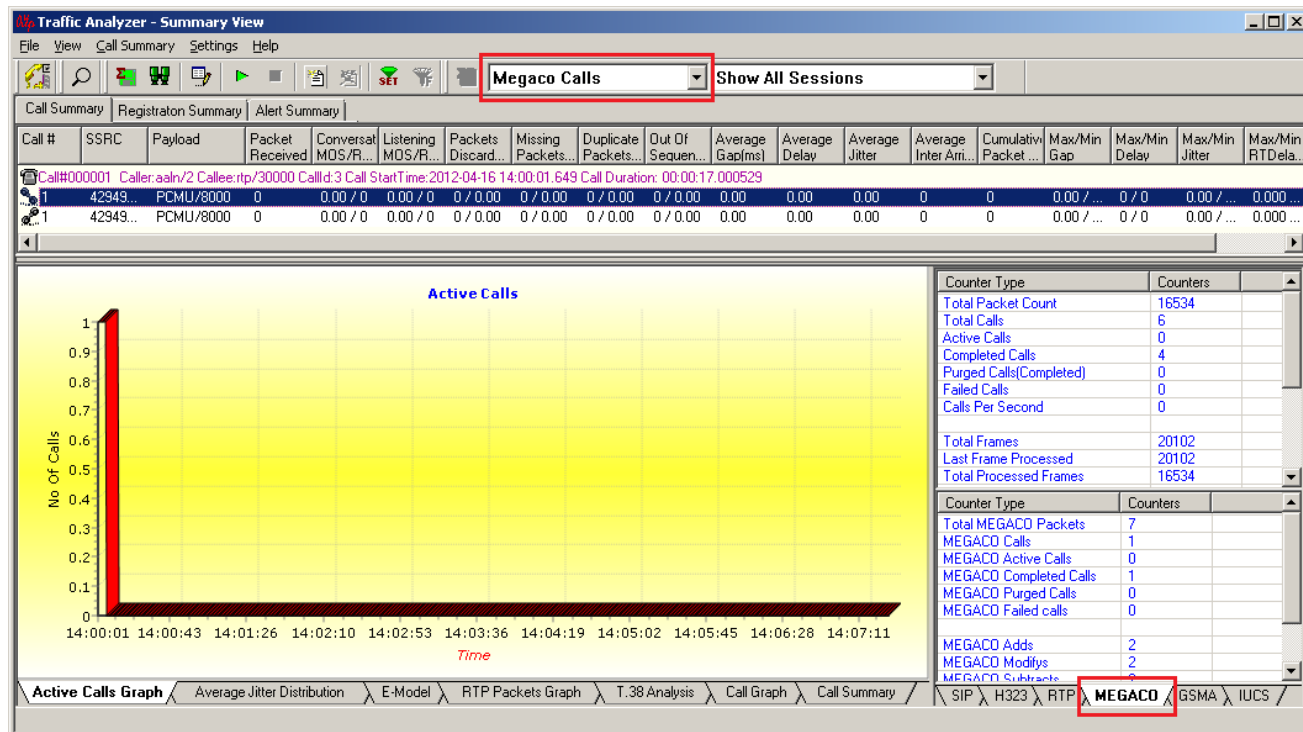


Figure 161: MeGaCo Calls

GSM A Calls

Select **Call Summary > Protocol > GSM A Calls** to open the GSM A calls pane or select GSM A Calls option from the dropdown box on the Extra tool bar. Calls that are attempted, failed, established using GSM A signaling and summary regarding the Traffic flow pertaining to that call is displayed.

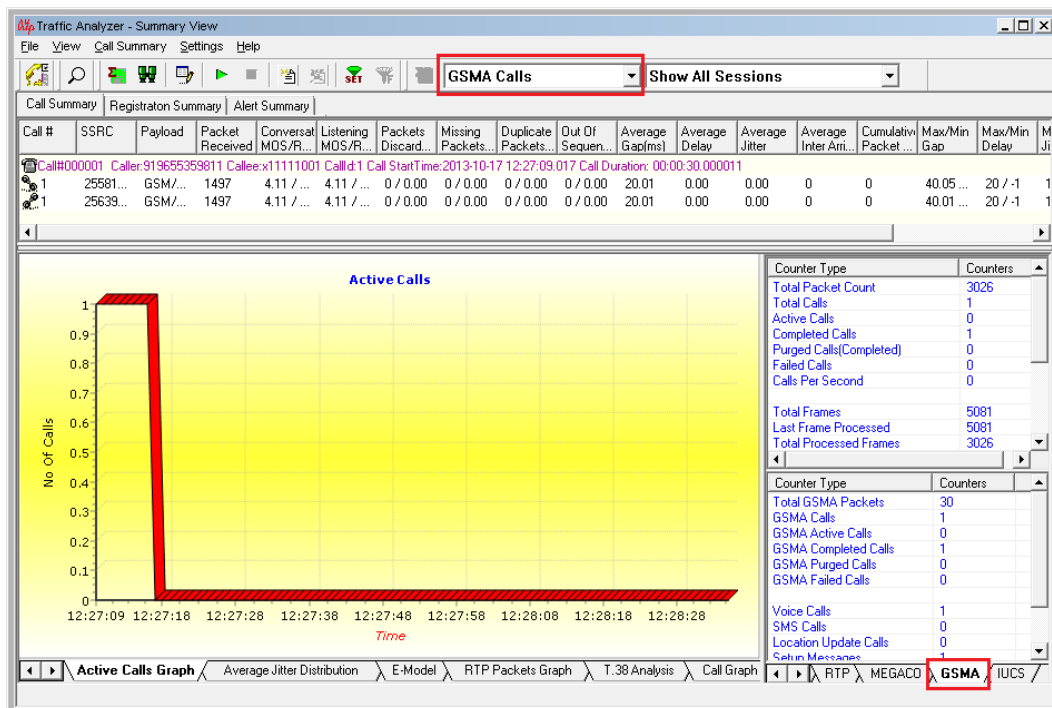


Figure 162: GSM A Calls

IuCS Calls

Select **Call Summary > Protocol > IuCS Calls** to open the IuCS calls pane or select IuCS Calls option from the dropdown box on the Extra tool bar. Calls that are attempted, failed, established using IuCS signaling and summary regarding the Traffic flow pertaining to that call is displayed.

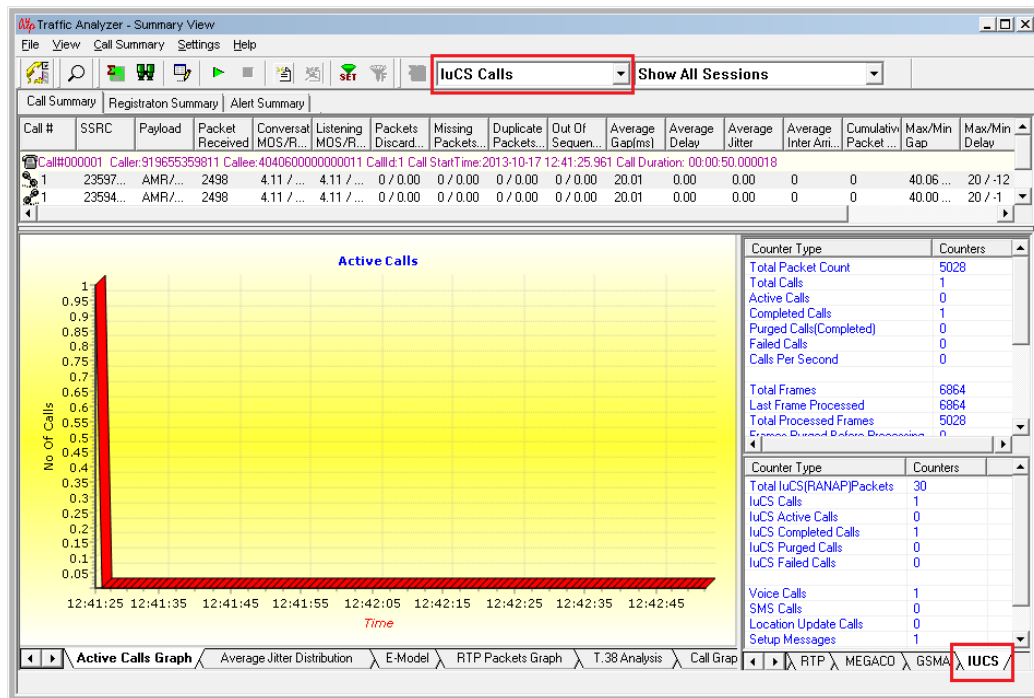


Figure 163: IuCS Calls

12.5.2 Filters

Filter option provides the user with the following types of sessions as explained below:

- **Show All Sessions:** Displays all the sessions that are traced
- **Show Active Sessions Only:** Displays only active sessions
- **Show Completed Sessions Only:** Displays only completed sessions
- **Show Video Sessions Only:** Displays only video sessions. Video sessions are marked with symbol 'V' and they also display the video traffic channels
- **Show User Defined Sessions:** Displays only filtered calls. Filtering criteria should be set in 'Triggers And Actions Settings' dialog. (Refer to the section [Triggers and Action Settings](#) for more details)
- **Show Fax Sessions Only:** Displays only fax sessions. Fax sessions are marked with symbol 'F'
- **Show Failed Calls:** Displays only failed sessions
- **Show GSM Voice Calls:** Displays only GSM Voice Calls
- **Show SMS Calls:** Displays only SMS Calls
- **Show Location Update Calls:** Displays only Location Updated Calls

The different types of sessions available are shown in the figure below.


The screenshot shows the 'Traffic Analyser - Summary View' interface. At the top, there is a menu bar with 'File', 'View', 'Call Summary', 'Settings', and 'Help'. Below the menu is a toolbar with various icons, including a search icon, a play icon, and a 'SET' button. A dropdown menu is open, showing 'Sip Calls' and a list of session filtering options: 'Show All Sessions', 'Show Active Sessions Only', 'Show Completed Sessions Only', 'Show Video Sessions Only', 'Show User Defined Sessions', 'Show Fax Calls', 'Show Failed Calls', 'Show GSM Voice Calls', 'Show SMS Calls', and 'Show Location Update Calls'. Below the toolbar, there are tabs for 'Call Summary', 'Registraton Summary', and 'Alert Summary'. The main area contains a table with the following data:

Call #	SSRC	Payload	Packet Received	Conversational MOS/R-Factor	Listening MOS/R-Factor	Packets Discarded/(%)	Missing Packets/(%)
Call#000001 Caller:0001@192.168.1.231 Callee:0001@192.168.1.237 CallId:GLPG13407127763982 Call StartT							
1	957412353	PCM...	1889	2.12 / 43	2.17 / 44	38 / 1.83	194 / 9.33
1	957785601	PCM...	1889	2.21 / 45	2.27 / 46	5 / 0.24	194 / 9.32

Figure 164: Sessions

12.5.3 Save Call

The Save Call feature enables the user to save a particular call in either GL's proprietary *.HDL file format or in Ethereal *.PCAP file format. Call Summary details could also be saved for a particular call and this will be saved as a *.rtf file. This is especially useful to get data from real-time traffic locations to the lab for detail analysis of a flawed call. By using this option, user can save the call that needs to be analyzed as a **HDL file** or as a **PCAP file** and transport it using temporary media to the lab for detail analysis. The whole call with all the SIP, H323, MEGACO, and RTP / RTCP packets that are part of the call are saved under the new filename. To open Save Call Screen:

- Select **Call Summary > Save Call** from the main menu or
- Click  from the toolbar.

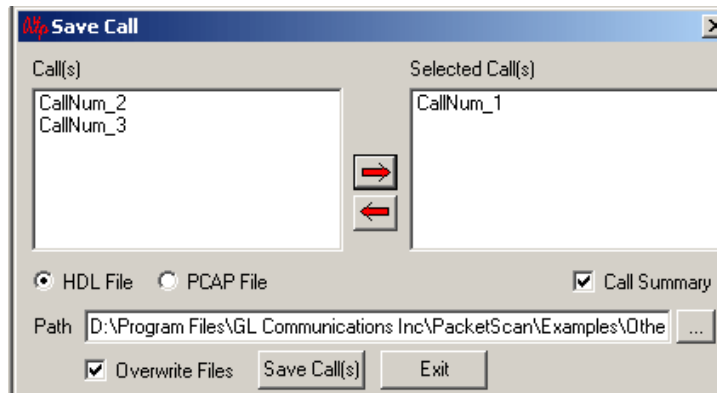



Figure 165: Save Call

Select the calls to be saved from the list of calls and click  button to appear in the Selected Call (s) pane. By default, HDL file will be selected. Select the PCAP option to save the file in Ethereal *.PCAP format.



Note:

The selected calls will be saved by the same name as appeared in the Selected Call(s) pane. For example, in the above figure, the file will be selected as CallNum_1.hdl and CallNum_1.rtf in the user-defined directory.

Call Summary – Select this option to save the summary details of a particular call to a *.rtf file format. The figure below shows a sample call summary file. The call summary file comprises of signaling and audio / video / fax session parameters of the call.

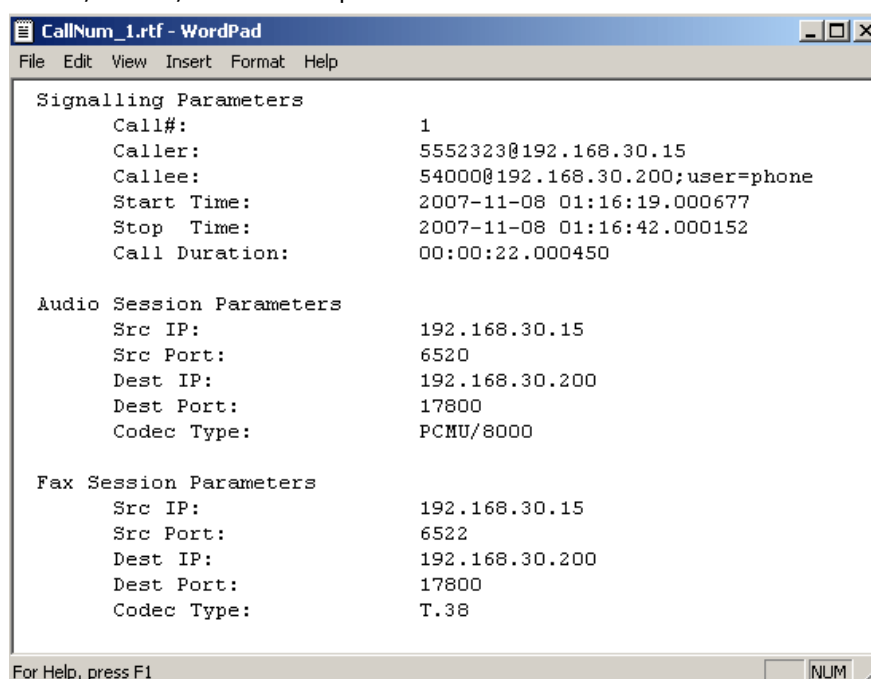


Figure 166: Call Summary File

If HDL option is selected, the user can either check or uncheck the **Call Summary** option. When PCAP option is selected, then by default, the call summary will be saved in the user-defined directory.

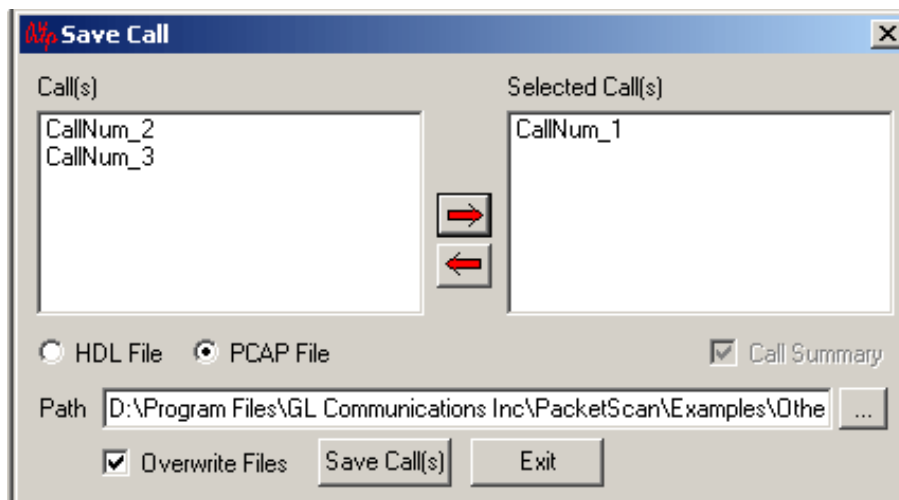


Figure 167: PCAP Option Selected

Path – This option allows the user to save a call in the desired location. Use the browse button to save a call in the desired file path.

Save Call(s) – Click this button to save the selected calls.

Exit – Click this button to exit from the Save Call dialog.

Overwrite-- When checked, this will overwrite the file if they exist with same file name in chosen directory, without prompting to the user.

12.5.4 Reports

This option provides the ability to generate PDA summary report of selected or all calls in PDF file format.

To export generated call summary reports in PDF (Portable Data Format) format, do the following:

- 1) Select **Call Summary** → **Reports** from the main menu
- 2) Select **All Calls**
 - **All Calls** – Generates reports for all the displayed calls in PDA
 - **Current Calls** – Generates reports for the selected call in PDA
 - **Call Range** – Reports are generated for the specified call ranges. For **Ex**: 1–10 30–40 60–70
 - **File Name** – Click on browse button to navigate and select the required path and specify the file name for the PDF file.
 - **Overwrite Files** – It will overwrite the existing PDF file with same name in the same path.
- 3) Choose format as **PDF**
- 4) Select the required RTP headers, as shown in the figure below:

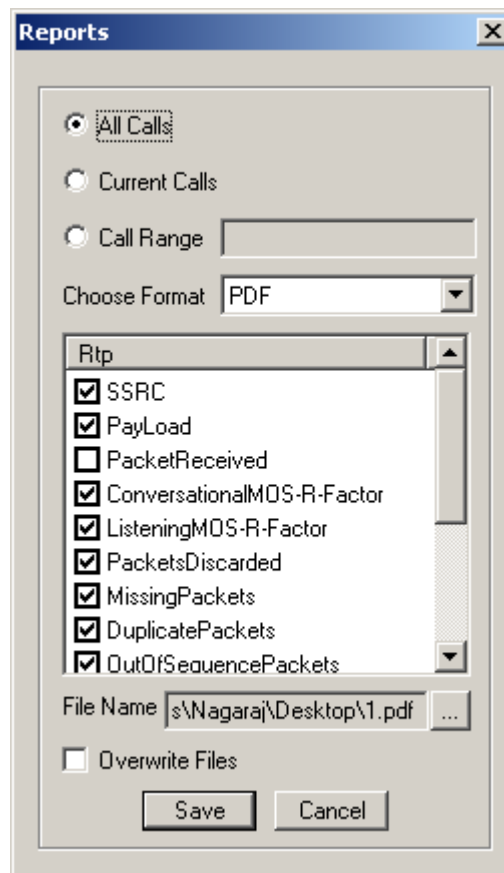

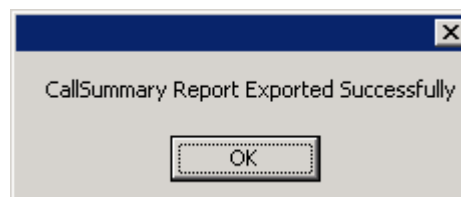


Figure 168: Selection of RTP Headers

- 5) Click on browse button  to navigate and select the file location and enter the file name for the PDF file.
- 6) Click **Save** to export the report in PDF format.



7) The exported PDF file is displayed as shown below:

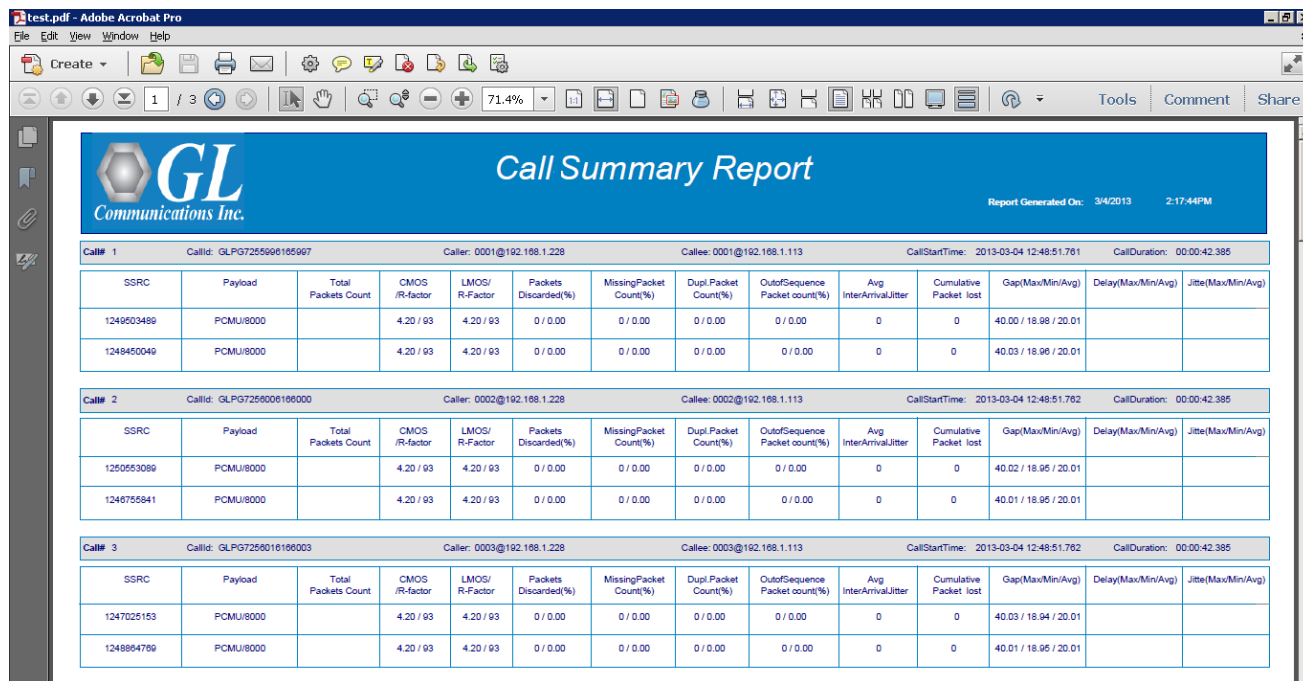



Figure 169: Packetscan Call Summary Report in PDF Format

12.5.5 Extract Fax Image

The Extract Fax Image feature enables the user to extract the image in the TIFF format from the selected fax call.

To Extract the Fax image, do the following:

- 1) Click  from the toolbar. This displays 'Extract Fax Image from Call' window as shown below:

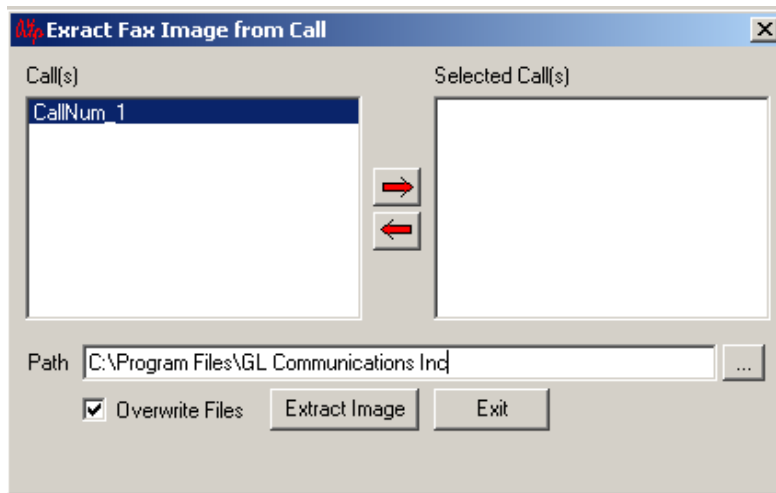




Figure 170: Extract Fax Image from Call

- 2) Select the Calls from the Call(s) pane and Click  to appear in the Call(s) pane
- 3) Click browse button to Choose the path for the TIFF image
- 4) Click Extract Image. This will extract the TIFF image in the specified path.

12.5.6 Play Audio

The Play Audio plays the selected call to the PC speaker. A host of options are provided to the user before the actual play is started.

To open Play Audio screen:

- Select **Call Summary > Play Audio > Start** to open the screen as shown below or
- Click  from the toolbar.

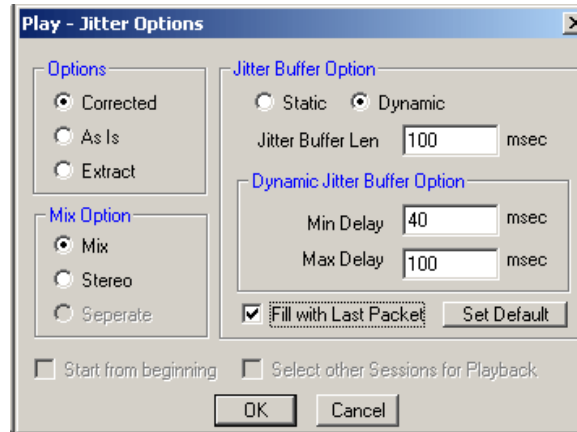


Figure 171: Play Jitter Options

Play to Sound Card Options

Following are the Different Option's to Play to Sound Card as Shown in the figure above.

Options:

- **Corrected with Jitter Buffer:** In this case, a two-stage correction is affected before a packet is played. First is that the packets are passed through a Jitter Buffer that adjusts those packets that arrived out of sequence, in the correct order before playing. The second stage is that, the RTP timestamp present in the RTP frame header is used as the basis for playing the audio (instead of the frame capture time as in the above case), thereby eliminating the delay induced by the network and allowing the user to listen to the audio with the same quality at the generator's side. By default, this option will be selected.
- **As Is:** The packets are not re-arranged in this case based on their RTP sequence numbers. The packets are just played based on their order of arrival at the point of capture by PacketScan™. In this case, time of capture of the frame will be the basis and the output audio will be reflective of this. Any delay induced by the network etc will be visible (rather audible) here.
- **Extract:** This is similar to 'As Is', except for the fact that capture time or RTP timestamp is not considered for generating the output. The contents of the RTP payload are extracted in sequence and played to the Sound Card.

Mix Options: This option allows users to play the audio files as a single stream, or to two different channels.

- **MIX:** The packets flowing in both the direction are mixed and played as single stream.
- **Stereo:** The packets flowing in two different directions are played as two different channels.

Jitter Buffer Options: The Jitter Buffer Option is used for playing as Corrected. Jitter buffer holds the incoming packets temporarily to minimize the Delay Variations.

- **Static:** size set in Jitter Buffer is fixed
- **Dynamic:** size varies between minimum and maximum values depending upon the network conditions in jitter buffer
- **Fill With Last Packet:** If the incoming packet stops for some duration, silence is played to soundcard, with this option being checked.

Set Default: Click this button to set the parameters to the default values and options.

Start From Beginning: This is applicable only in real-time. If the audio play is set on then normally it plays the packets that are presently in flow, but if we check this option then the Audio Play application starts playing the packets from beginning of captured.

Stop Play: To stop the Play Audio, user can select **Call summary > Play Audio > Stop** menu item or the corresponding tool button as shown in the figure.

12.5.7 Write to File

To open Write to File screen:

- Select **Call Summary > Write to File > Start** to open the screen as shown in the figure below or
- Click  from the toolbar

This is similar to the Play Audio option. The basic difference being that the output is written to a file instead of the Sound Card. Various options are provided so that the user can save the file in a required format, and use the files with voice quality analysis software to investigate more about the quality of voice in the network.

When user selects a Call/Session to be written to a file, a window appears from which user can select the output format, locations, number of files etc. The various options provided to the user are as follows.

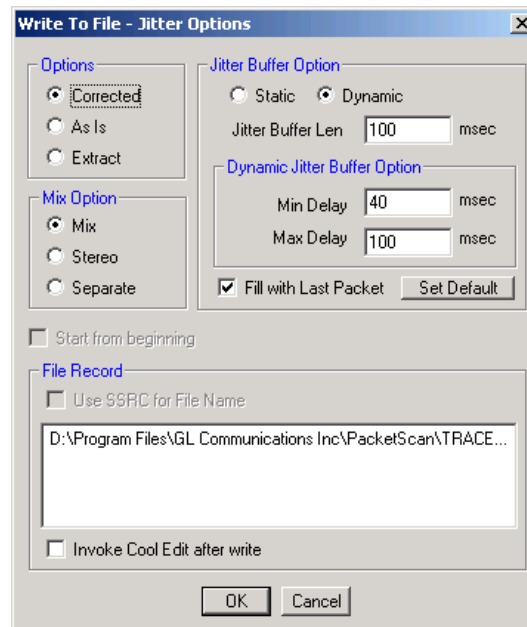


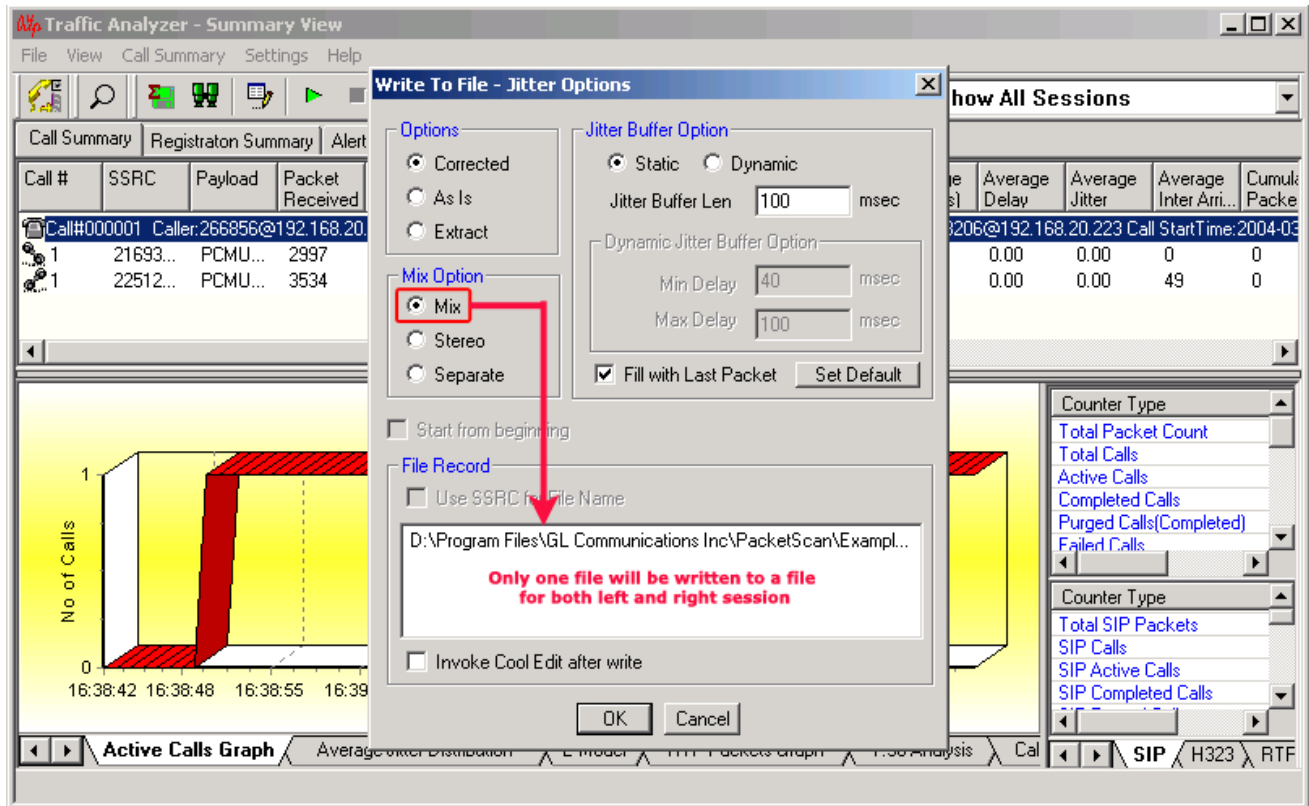
Figure 172: Write to File

Options:

- **Corrected with Jitter Buffer:** In this case a two-stage correction is affected before a packet is played. First is that the packets are passed through a Jitter Buffer that adjusts those packets that arrived out of sequence, in the correct order before playing. The second stage is that, the RTP timestamp present in the RTP frame header is used as the basis for playing the audio (instead of the frame capture time as in the above case), thereby eliminating the delay induced by the network and allowing the user to listen to the audio with the same quality at the generator's side.
- **As Is:** The packets are not re-arranged in this case based on their RTP sequence numbers. The packets are just played based on their order of arrival at the point of capture by PacketScan™. In this case time of capture of the frame will be the basis and the output audio will be reflective of this. Any delay induced by the network etc will be visible (rather audible) here.
- **Extract:** This is similar to 'As Is', except for the fact that capture time or RTP timestamp is not considered for generating the output. The contents of the RTP payload are extracted in sequence and played to the Sound Card.

Mix Options: This option allows users to write to a single file, or two different files. It has three options – Mix, Stereo, and Separate.

- **Mix** – This option mixes and writes to a single file when a call is selected as shown below. The audio data are converted to linear PCM (from their native format), then mixed based on the timestamps, and then the resultant output is written to a user-selected file. When either left or right session of a call is selected, a single file of the selected session will be written to a file.



- **Stereo**-- If this option is selected, the output stream will be written as stereo.

- Separate**-- This option writes into two different files when a call is selected, i.e., the left and the right sessions in a call are written into two different files as shown below.

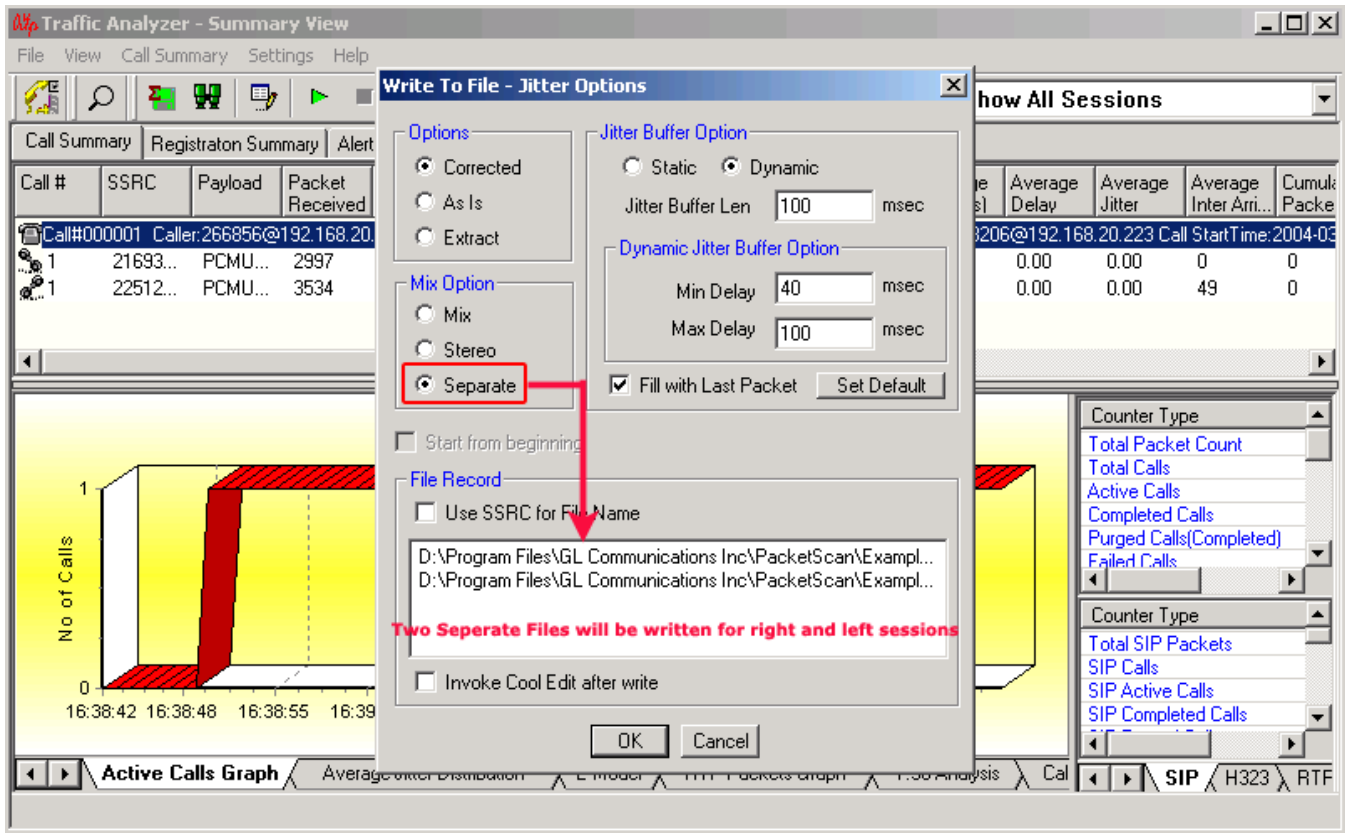


Figure 173: Write to File with Separate Option Selected

Observe that in the above figure, two different files will be created for left and right session of a call.

Start from beginning: This is applicable only in Real-time. When this option is selected, the stream would be written from the beginning. If not selected the stream would be written from the time the choice was made, all previous frames would be ignored.

Jitter Buffer Options: The Jitter Buffer Option is used for Playing as Corrected. Jitter buffer holds the incoming packets temporarily to minimize the Delay Variations.

- Static**-- size set in Jitter Buffer is fixed
- Dynamic**-- size varies between minimum and maximum values depending upon the network conditions in jitter buffer
- Set Default:** Click this button to set the parameters to the default values.

File Record:

Use SSRC for File Name – This option allows users to select the output filename and its location and it gets enabled only when **Separate** option is selected. Check this option, and the filenames would be saved as 12345678.wav, where 12345678 are the SSRC of the session. These filenames will be unique for the selected session.

Invoke Adobe Audition (or Goldwave) after Write: Selecting this option would automatically launch the **Adobe Audition (or Goldwave)** application once user stops the write operation or the stream(s) that is been written to file it will terminate.

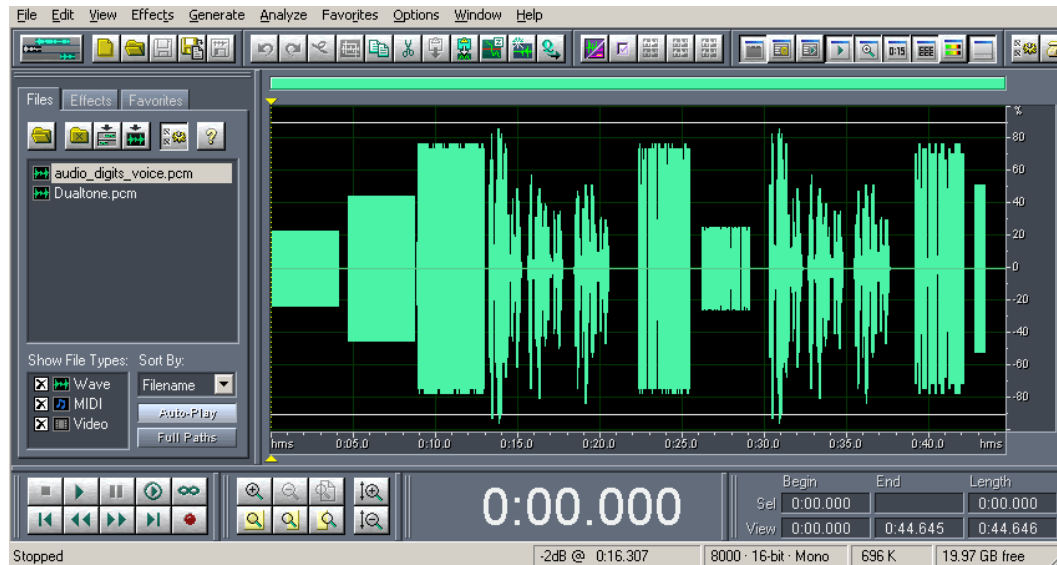



Figure 174: Invoke Adobe Audition after Write

Stop Write to File: To Stop write to file user can select **Call Summary > Write to File > Stop** or click  from the toolbar. Write to file stops on its own when the Call tears down.

12.5.8 Record Video

This option will allow the user to record audio and video data of a session to a file in QuickTime format. PacketScan™ can monitor video calls and display both audio and video RTP streams in Summary View. There is a provision to view video calls using a filter. Video calls will be marked with symbol 'V' at the left corner as shown in the figure below.

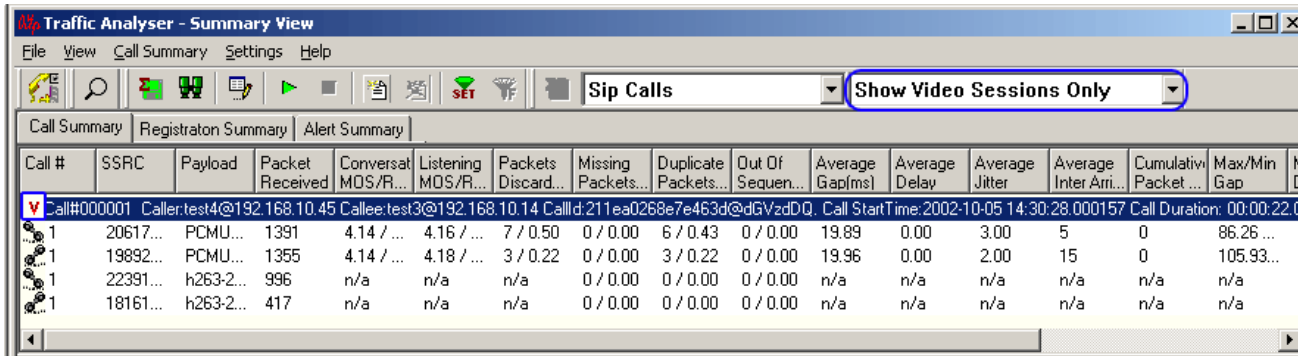
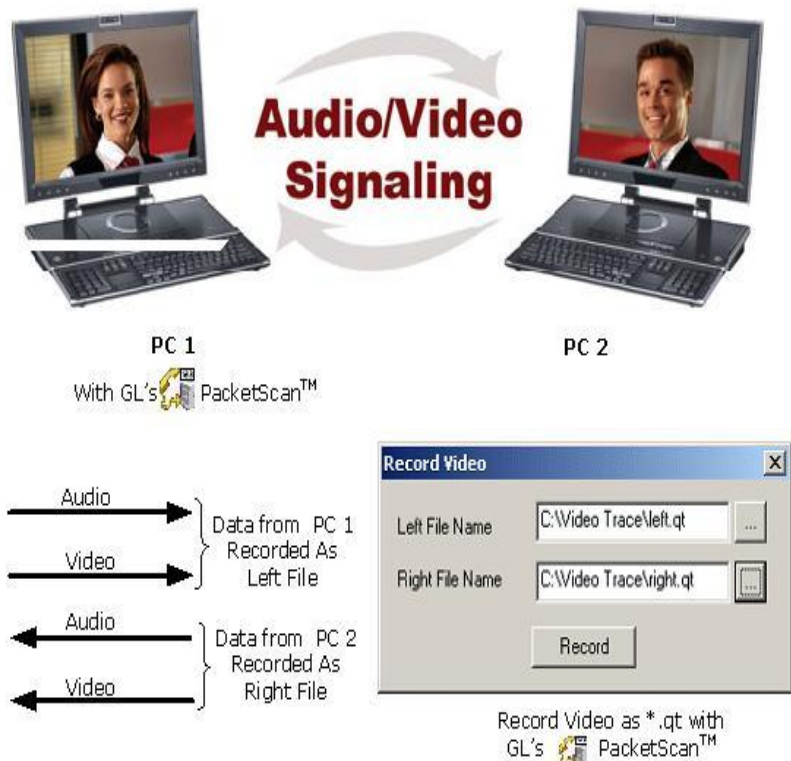


Figure 175: Summary View Displaying Video Calls

Users can record video calls to a file in QuickTime format (*.qt), which can be viewed by VLC player. PacketScan™ may be installed in either of the system to record the video data as depicted in the figure below.



Record video option is available for both Auto Detected RTP Calls and SIP Calls.

12.5.8.1 Video Codecs

Supported Video Codecs are:

- H263+
- H263++ CIF 190 kbps
- H263++ CIF 350 kbps
- H263++ CIF 512 kbps
- H263++ QCIF 128 kbps
- H263++ QCIF 64 kbps
- H263++ QCIF 80 kbps
- H264

**Note:**

Video recording is supported only for H263+ codec. However, video QoS statistics is available for all codecs.

H.263- is a video codec designed by the ITU-T as a low-bit rate encoding solution for video conferencing. It was first designed to be utilized in H.324 based systems (PSTN and other circuit-switched network video conferencing and video-telephony applications), but has since found use in H.323 (RTP/IP-based video conferencing), H.320 (ISDN-based videoconferencing), RTSP (streaming media) and SIP (Internet conferencing).

H.263 was developed as an evolutionary improvement based on experience from H.261, the previous ITU-T standard for video compression, and the MPEG-1 and MPEG-2 standards.

QCIF- Quarter Common Intermediate Format, a videoconferencing format that specifies data rates of 30 frames per second (fps), with each frame containing 144 lines and 176 pixels per line. This is one-fourth the resolution of Full CIF.

CIF-- A video format used in videoconferencing systems that specifies a data rate of 30 frames per second (fps), with each frame containing 288 lines and 352 pixels per line.

H.264 is the latest video coding standard of the ITU-T Video Coding Experts Group (VCEG) and the ISO/IEC Moving Picture Experts Group (MPEG). **H.264** is an industry standard for video compression, the codec offers better compression performance over previous standards.

It has demonstrated the following features significantly relative to its predecessors;

- improved coding efficiency
- lower compressed bit rate for the same image quality
- substantially enhanced error robustness
- increased flexibility and scope of applicability

Wide application of H.264 includes;

- Mobile TV broadcasting
- Internet video
- Videoconferencing

Video parameters such as Video Channels, Codec Info, SSRC, Frame Count, Packet Count, Packets Lost, Frame Rate, Media Delivery Index (Delay Factor : Media Loss Rate), Average Media Delivery Index are calculated for all video calls. For more details, refer to section [Video Parameters](#).

12.5.8.2 Procedure

Select the SIP call to be recorded and open the **Record Video** dialog by selecting **Call Summary > Record Video**. Enter left file name (i.e. for source side traffic) and right file name (i.e. for destination side traffic) using the browse buttons. Click on **Record** button to start recording.

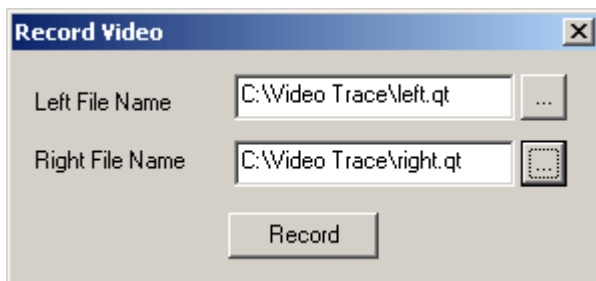


Figure 176: Record

For Auto Detected RTP Calls, select the call to be recorded and open the **Record Video** dialog by selecting **Call Summary > Record Video**. Enter the audio and video session id's to be recorded. Click on browse to select the file name and click on **Record** button to start recording.

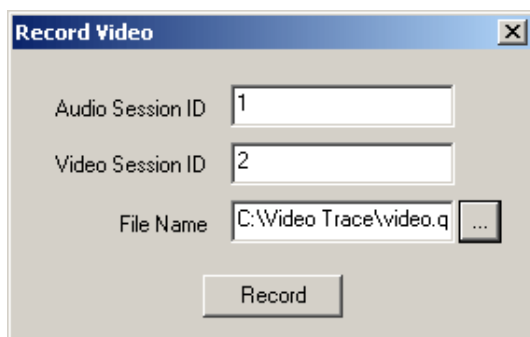


Figure 177: Record Video

12.6 Additional Settings

12.6.1 E-Model Parameters

The E-Model (ITU-T Rec. G.107 [1]) is a transmission-planning tool that provides a prediction of the expected voice quality. E-Model takes many basic parameters into consideration for **Estimation of Voice Quality**.

Following are the E-model Base parameters.

SLR	Send Loudness Rating
RLR	Receive Loudness Rating
OLR	Overall Loudness Rating1
STMR	Sidetone Masking Rating2
LSTR	Listener Sidetone Rating2
Ds	D-value of telephone at send-side
Dr	D-value of telephone at receive-side2
TELR	Talker Echo Loudness Rating
WEPL	Weighted Echo Path Loss
T	Mean one way delay of the echo path
Tr	Roundtrip delay in a closed 4-wire loop
Ta	Absolute one-way delay in echo free connections
Qdu	Number of quantization distortion units
Ie	Equipment impairment factor
Ppl	Random packet-loss probability
Bpl	Packet-loss robustness factor
Nc	Circuit noise referred to the 0 dBr-point
Nfor	Noise floor at the receive-side
Ps	Room noise at the send-side
Pr	Room noise at the receive-side
A	Advantage factor

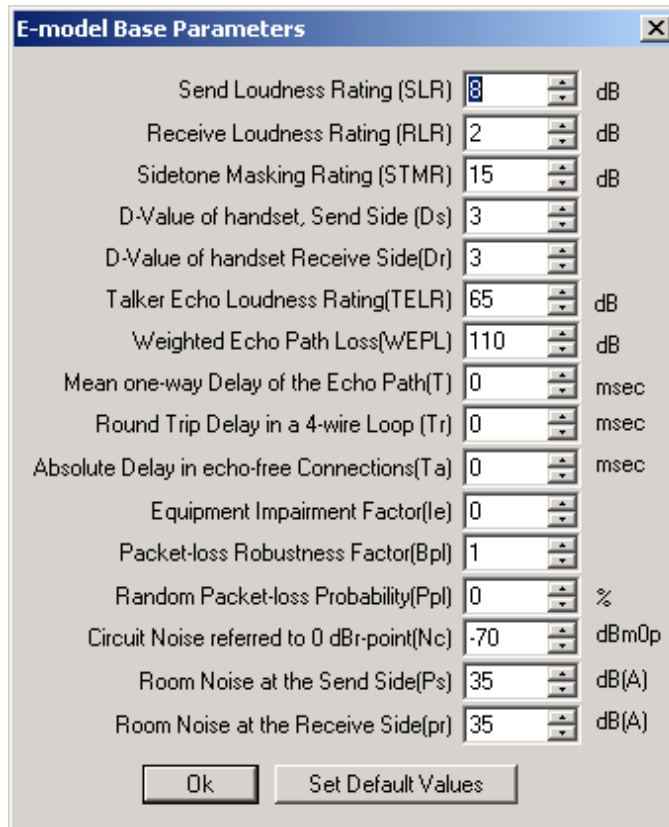


Figure 178: E-model Parameters

12.6.2 VQMon Settings

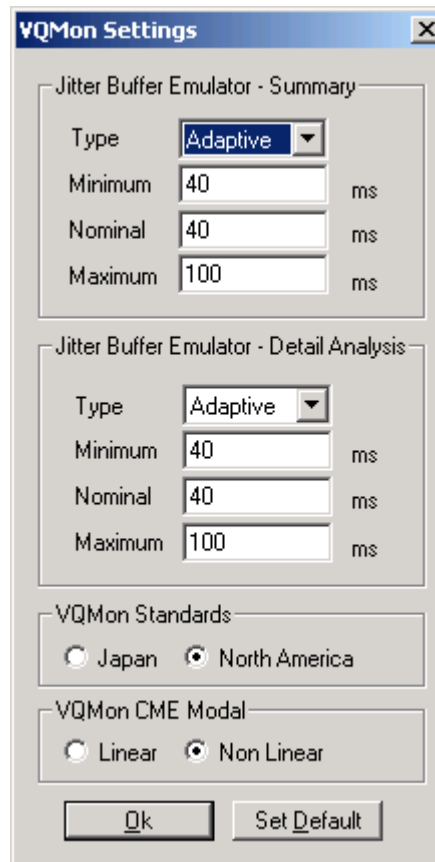


Figure 179: VQMon Settings

User should set Jitter Buffer Emulator settings in PDA - Summary and PDA-Detail View to emulate received VoIP Call. The buffer can be set static or dynamic depending upon the requirement. For both

these options, users can set Minimum, Nominal, and Maximum buffer size in msec. The R-Factor and MOS are calculated in summary and detail views depending upon the **Jitter Buffer Emulator** settings.

VQMon Standards: This provides an option to select an International standard code Japan or North America, PacketScan™ uses these standards to adjust the MOS scores based upon R-Factor scores.

VQMon CME Model: This provides an option to select 'Linear' or 'Non Linear' Calculate Metrics Engine Model to calculate Quality metrics.

- Linear and Non-Linear CME model gives similar quality scores for the voice stream which primarily have only one kind of impairments (e.g. packet loss).
- It is observed that Non-Linear CME model gives more accurate quality scores when more than one kind of impairments at the higher level existed on the stream.
- For Linear CME model voice metrics are calculated using the linear engine model
- For Non-Linear CME model voice metrics are calculated using newer Non-linear engine model.



Note:

This 'Linear CME' option is provided only to have compatibility with values of older version of PacketScan™.

12.6.3 Payload Map Table

Dynamic Payload Mapping is used to define payload type for supported codecs. Payload type mapping is performed during session setup, often using SDP. If the sender uses a particular payload type number for a codec, then same payload number should be set for that codec in PacketScan™ before we actually begin capturing frames. This helps in identifying the codec type for the RTP session, if the signaling information is not available for that call properly.

Select **Settings > Payload Map Table** from the main menu to open the window as shown in the figure below:

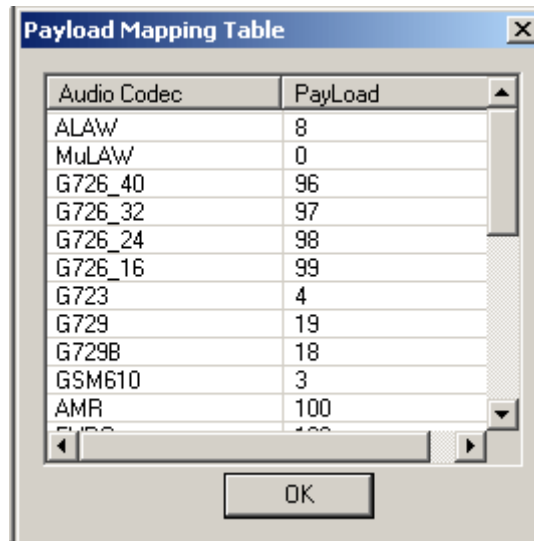


Figure 180: Dynamic Payload Mapping Table

The payload type ranges from 0 to 127 and each codec should have unique payload number.

12.6.3.1 Codec Type

PacketScan™ supports the following codecs:

- G711 MuLaw (64kbps)
- G711 aLaw (64kbps)
- G726_40 (40kbps)
- G726_32 (32kbps)
- G726_24 (24kbps)
- G726_16 (16kbps)
- G726_40 (40kbps) with Voice Activity Detection
- G726_32 (32kbps) with Voice Activity Detection

- G726_24 (24kbps) with Voice Activity Detection
- G726_16 (16kbps) with Voice Activity Detection
- GSM (13.2kbps)
- GSM EFR (12.2 kbit/s)
- GSM HR
- G729 (8kbps)
- G729B (8kbps)
- AMR (Narrow band codec-- 4.75kbps, 5.15kbps, 5.9kbps, 6.7kbps, 7.4kbps, 7.95kbps, 10.2kbps, 12.2 kbps) (optional codec)
- ILBC_15_2 (for 20 msec)
- SPEEX (Narrowband)
- EVRC, EVRC0 (Rates – 1/8, 1/2 and 1) (optional codec)
- SMV (Modes – 0, 1, 2 and 3)
- ILBC_13_33 (for 30 msec)
- G722
- G722.1 (24 kbps)
- G722.1 (32 kbps)
- SPEEX_WB (Wideband)
- AMR_WB (Wideband - 6.60kbps, 8.85kbps, 12.65kbps, 14.25kbps, 15.85kbps, 18.25kbps, 19.85kbps, 23.05kbps, 23.85 kbps) (optional codec)
- EVRCB, EVRCB0 (Rates – 1/8, 1/2 and 1) (optional codec)
- EVRC_C (optional codec)
- G711 application II (A-law and μ -law with Voice Activity Detection).
- [H.263+](#) providing video capture and videoconference monitoring capability.
- [H.264](#) is an industry standard for video compression, the codec offers better compression performance over previous standards

**Note:**

- The SMV codec will not be installed during the regular installation of PacketScan™. To know further details on using these codec, contact GL Communications Inc.
- AMR, EVRC, EVRC-B, and EVRC-C are separate optional Codecs. These must be purchased individually as a separate dongle extension.

12.6.4 Codec Parameter Settings

User can set additional parameters to codecs such as G726, AMR, EVRC, EVRCB, EVRCC, G722.1, AMR_WB and G726_VAD as shown in the figures below.

G726 Codec type provides two types of packing **RTP** and **AAL**. Click on the radio button to select the desired packing type. Click on **Save** to set the G726 Codec type.

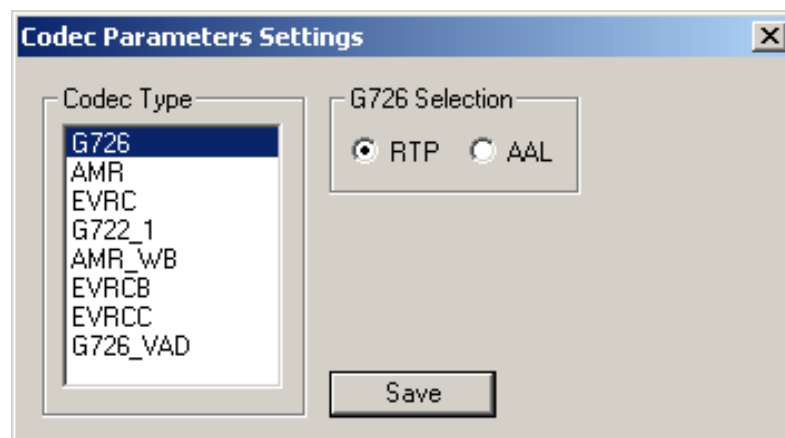


Figure 181: G726 Codec Type

In **AMR Codec** type the user can set the **RTP Packet Format** by selecting the option from the drop down menu. AMR Codec type provides packet formats namely **Band Width Effective Mode** and **Octate Aligned Mode**. To save the selected packet format the user has to click on the **Save** button to save the settings.

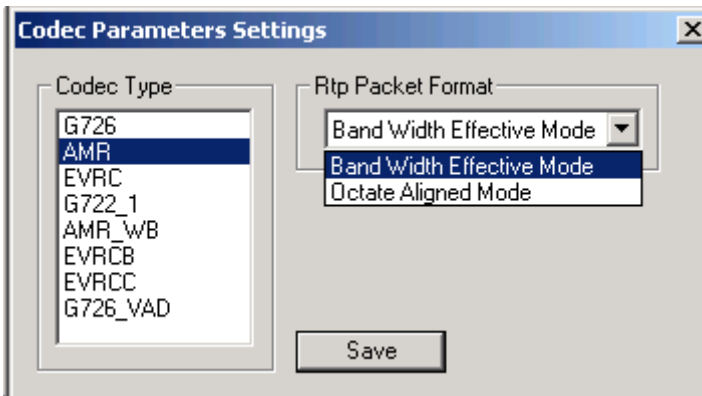


Figure 182: AMR Codec Type

In **EVRC / EVRC0 Codec** type, the user can set the **RTP Packet Format** and **Payload Packing Format** by selecting the option from the drop down menu. EVRC Codec type provides packet formats namely **Bundled Format** and **Header Free Format**. To save the selected packet format the user has to click on the **Save** button to save the settings.

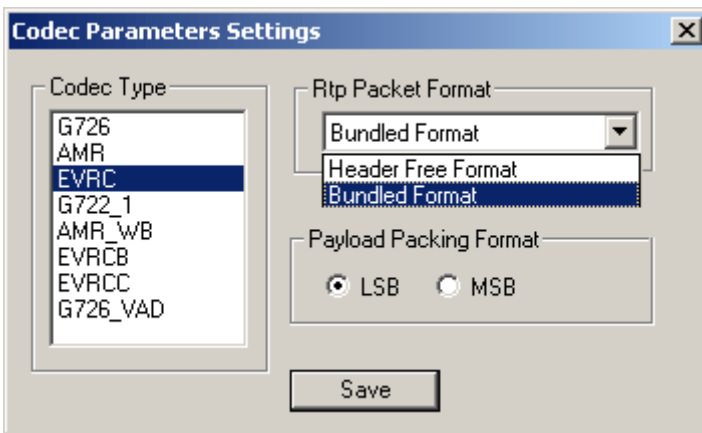


Figure 183: EVRC Codec Type



Note:

The default packing for EVRC is set to Bundled Format. EVRC0 is the EVRC codec with Header Free RTP Packing format. By selecting the Header Free Format for EVRC codec we can have calls for these codecs.

In **G722.1 Codec** type, the user can set the **Bit Rate**. G722.1 codec provides 24 kbps or 32 kbps bit rates. By default, 32kbps is selected. To save the selected packet format the user has to click on the **Save** button to save the settings.

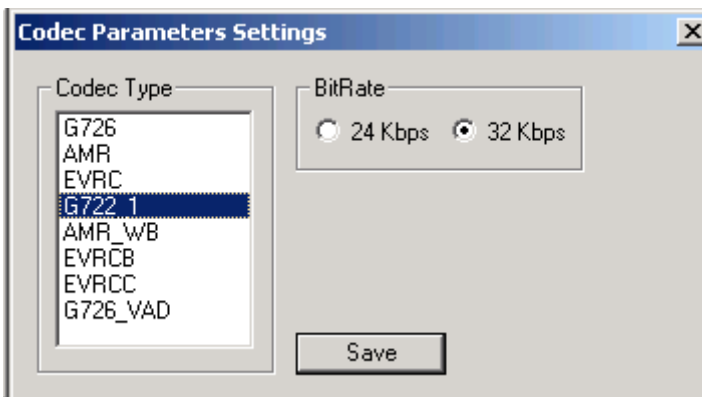


Figure 184: G722.1 Codec Type

In **AMR_WB Codec** type, the user can set the **RTP Packet Format** by selecting the option from the drop down menu. AMR_WB Codec type provides packet formats namely **Band Width Effective Mode** and **Octate Aligned Mode**. To save the selected packet format the user has to click on the **Save** button to save the settings.

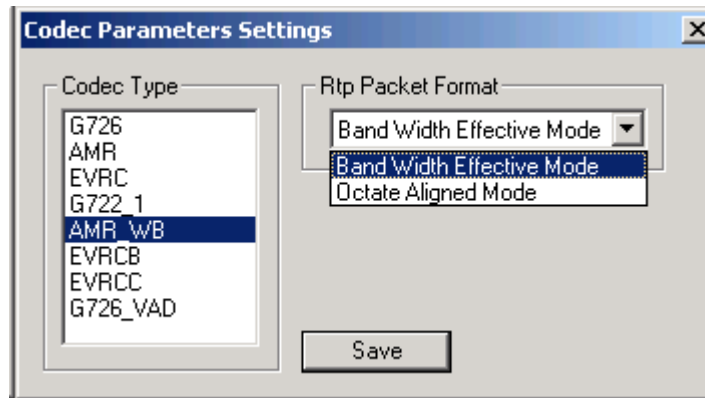


Figure 185: AMR_WB Codec Type

In **EVRCB / EVRCB0 Codec** type, the user can set the **RTP Packet Format** by selecting the option from the drop down menu. EVRCB Codec type provides packet formats namely **Bundled Format** and **Header Free Format**. To save the selected packet format the user has to click on the **Save** button to save the settings.

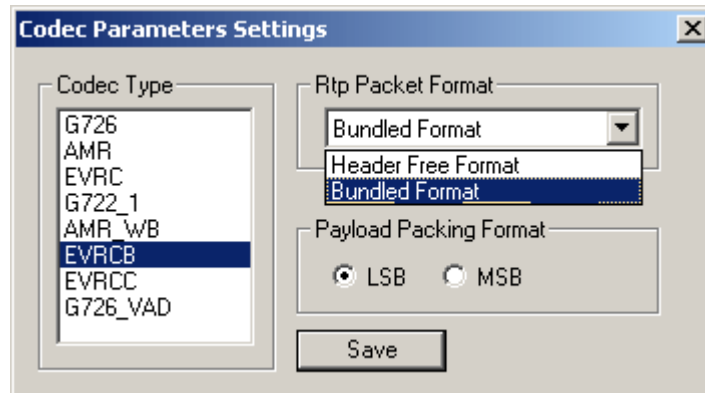


Figure 186: EVRCB Codec Type



Note:

The default packing for EVRCB is set to Bundled Format. EVRCB0 is the EVRCB codec with Header Free RTP Packing format. By selecting the Header Free Format for EVRCB codec, we can have calls for these codecs.

In **EVRC_C Codec** type, the user can set the **RTP Packet Format** by selecting the option from the drop down menu. EVRC_C Codec type provides packet formats namely **Bundled Format** and **Header Free Format**. To save the selected packet format the user has to click on the **Save** button to save the settings.

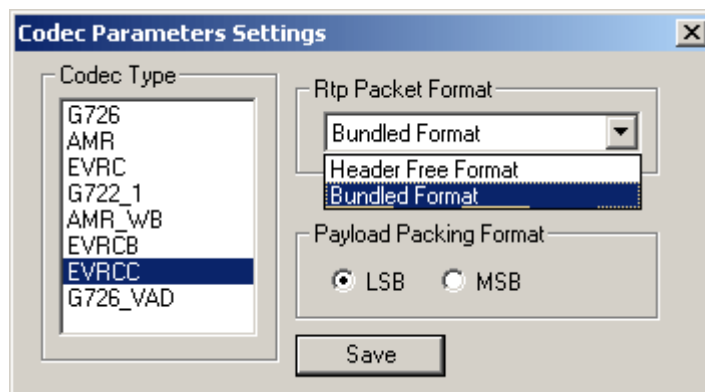


Figure 187: EVRC_C Codec Type

G726_VAD codec type provides two types of packing **RTP** and **AAL**. Click on the radio button to select the desired packing type. Click on **Save** to set the G726VAD Codec type.

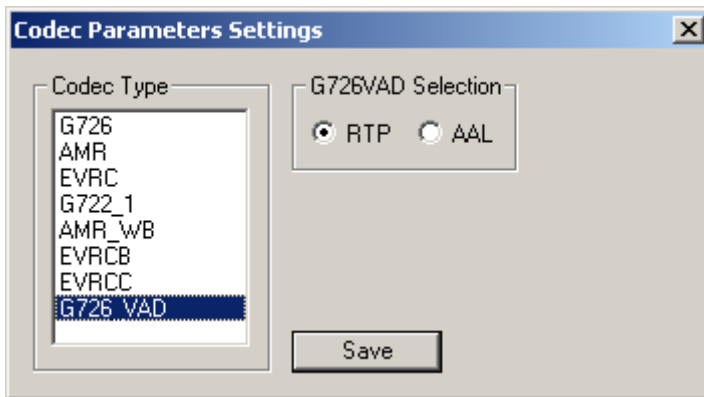


Figure 188: G726_VAD Codec Type

12.6.5 Triggers and Action Settings

PacketScan™ supports triggers and action settings as shown in the figure below:

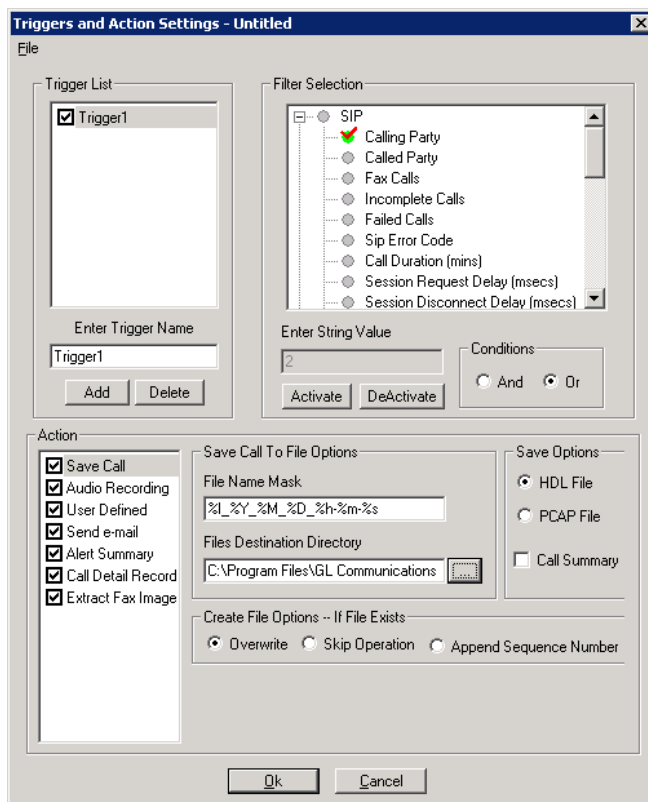


Figure 189: Triggers and Action Settings

Triggers and Action Settings allow the user to filter calls based on certain SIP, RTP, MEGACO and H.323 parameters followed by a set of actions for the completed calls. Action column lists one or more actions to be performed on the filtered calls. The actions include saving call to a file, recording audio to a file, sending an email, posting alert summary, viewing custom calls in summary view, creating Call Detail Records in CSV file format, and extracting Fax from calls in TIFF format.

12.6.5.1 Trigger List

For setting Trigger and action feature, first add the trigger name, for ex: Enter 'Trigger1' and click on **Add** button to add the trigger name into the trigger list.

12.6.5.2 Filter Selection

This option allows the users to specify the parameters for SIP, RTP, MEGACO, and/or H.323 protocols to filter out the calls. The parameters for each protocol can take either String, Integer or Floating values depending on the type of parameter. For String value, exact value has to be entered to filter out the calls of interest.

Integer values should be real numbers with no decimal value, while Floating values could be real numbers with or without decimal values. For real and floating values, users can enter either an exact value and/or specify the range to filter out the calls.

For example,

- 1) To filter out the calls ranging between any two integers or float values, then specify the range.
- 2) To filter out calls for parameter with specific value, specify the exact value.

- **SIP (Session Initiation Protocol)**

This parameter is used to specify the calling party, called party, fax calls, incomplete calls, failed calls, SIP error code, call duration, session request delay, and /or session disconnect delay as trigger conditions.

For example, if Calling party is chosen as the trigger, enter the calling party URI in the String value text box, and click on **Activate** to activate the filter.

Ex: 271585@192.168.20.10

If **Fax Calls** is chosen as the trigger, a value '1' should be entered to enable filtering. Click on **Activate** to activate the filter. This will filter out the Fax Calls.

If **Incomplete calls** is chosen as the trigger, a value '1' should be entered to enable filtering. Click on **Activate** to activate the filter to filter out the incomplete calls.

If **Failed Calls** is chosen as the trigger, a value '1' should be entered to enable filtering. Click on **Activate** to activate the filter to filter out the failed calls.

For **SIP Error Code** trigger condition, enter the sip error codes such as 404, 500-600. Click on **Activate** to activate the filter to filter out the calls with SIP error codes.

For **Call Duration**, specify the integer value in minutes, according to which the filtering takes place. Click on **Activate** button to activate the filter.

For **Session Request Delay** chosen as triggering condition, specify the integer value range in msec. Click on **Activate** button to activate the filter. For example, specify the integer value range as 25-30 to filter out the calls with the session request delay value between 25 and 30.

For **Session Disconnect Delay** chosen as triggering condition, specify the integer value range in msec. Click on **Activate** button to activate the filter. For example, specify the integer value range as 5-10 to filter out the calls with the session request delay value between 5 and 10.

All Calls - If All Calls are chosen as triggering condition, a value '1' should be entered to enable filtering. Click 'Activate' to activate the filter to filter All SIP Calls i.e., Successful, failed, incomplete, timed out calls and so on.

- **RTP (Real-time Transmission Protocol)**

- Average Jitter**

This parameter is used to specify the float value, according to which the filtering takes place. Click on **Activate** button to activate the filter.

For ex: To filter out the calls with Average Jitter less than 5 and greater than 2, specify the range as 2-5.

- Duplicate packets**

This parameter is used to specify the percentage value range, according to which the filtering takes place. Click **Activate** button to activate the filter.

For ex: To filter out the calls with the value less than 50, specify the range as 0-50.

Missing packets

This filter setting is same as the settings for the duplicate packets but this gives the missing packets in the range specified. Click **Activate** button to activate the filter.

R-Factor

This parameter is used to specify the integer value range, according to which the filtering takes place. Click **Activate** to activate the filter.

For ex: To filter out the calls with R-Factor value less than 100 and greater than 1, specify the range as 1-100.

MOS (Mean Opinion Score)

This parameter is used to specify the float value ranging between 1 to 5 to enter, according to which the filtering takes place. Click **Activate** to activate the filter.

For ex:

- 1) To filter out calls with MOS less than 3 specify the range as 0-3.
- 2) To filter out calls with MOS greater than 3.5 specify the range as 3.5-5.
- 3) Specify the exact score to filter out calls which match the specified value.

Discarded Packets

This parameter is used to specify the percentage value range, according to which the filtering takes place. Click **Activate** button to activate the filter.

- **MEGACO**

This parameter is used to specify the calling party, called party, fax calls, incomplete calls and/or failed calls as trigger conditions.

For example, if Calling party is chosen as the trigger, enter the calling party value in the String value text box, and click **Activate** to activate the filter. Ex: tgw/s1/c2

If Fax Calls is chosen as the trigger, a value '1' should be entered to enable filtering. Click on **Activate** to activate the filter.

If **Incomplete Calls** is chosen as trigger condition, specify a value '1' to enable filtering. Click on **Activate** to activate the filter.

If **Failed Calls** is chosen as trigger condition, specify a value '1' to enable filtering. Click on **Activate** to activate the filter.

For **Call Duration**, specify the integer value in minutes, according to which the filtering takes place. Click on Activate button to activate the filter.

- **H323**

This parameter is similar to SIP (used for signaling) to specify the calling party and/or the called party as trigger settings. Enter the String value and click on **Activate** button to activate the filter.

- **GSMA**

This parameter is used to specify the calling party, the called party and/or All Calls as trigger settings. Enter the String value and click on **Activate** button to activate the filter.

- **IUCS**

This parameter is similar to GSMA used to specify the calling party, the called party and/or All Calls as trigger settings. Enter the String value and click on **Activate** button to activate the filter.

12.6.5.3 Save Call to File

This allows the users to save the filtered files either in *.HDL or *.PCAP format. The user has to select this option as shown in the figure below.

When user selects the PCAP option, then the call summary options gets checked and disabled, by default and saves the call summary parameters to *.rtf file.

When HDL option is selected, the user can either check or uncheck the Call Summary option.

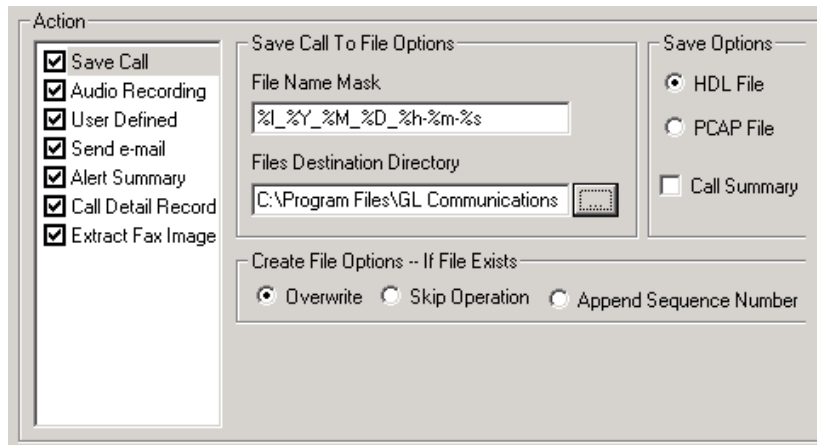


Figure 190: Save Call Options

File Name Mask – The users have to specify the desired file name in this field. If users don't specify any file name, by default, the file will be saved in the timestamp format as **%1_%Y_%M_%D_%h-%m-%s**. For example, the file will be saved as **1_2009_05_20_16-39-14.hdl**, which denotes the 1_YY_MM_DD_HH_MIN_SEC.

Files Destination Directory – Use the browse button to save the file in the desired directory.

If file with the same name already exists in the directory, users have options such as **Overwrite**, **Skip Operation**, and **Append Sequence Number**.

12.6.5.4 Audio Recording

The user can save the filtered files as the voice files in *.wav format by selecting this option as shown in the figure below.

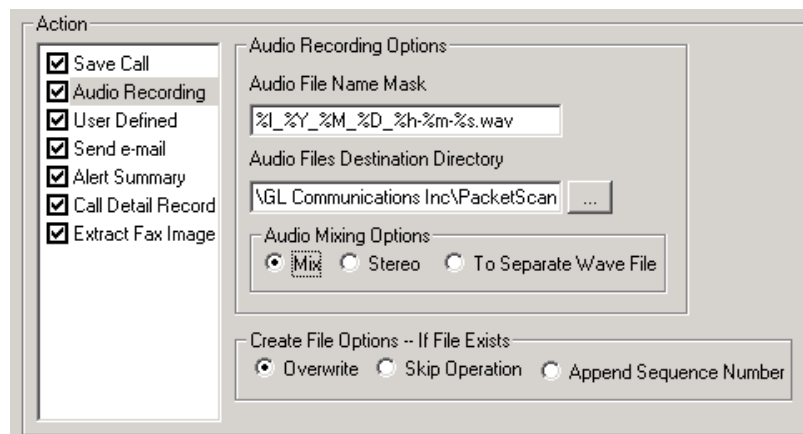


Figure 191: Audio Recording

File Name Mask – The users have to specify the desired file name in this field. If users don't specify any file name, by default, the file will be saved in the timestamp format as **%1_%Y_%M_%D_%h-%m-%s**. For example, the file will be saved as **1_2009_05_20_16-39-14.hdl**, which denotes the 1_YY_MM_DD_HH_MIN_SEC.

File Destination Directory-- Use the browse button to save the file in the desired directory.

If file with the same name already exists in the directory, users have options such as **Overwrite**, **Skip Operation**, and **Append Sequence Number**.

The files saved in **.wav** format can be further specified with the audio mixing options such as **To Separate Wave File**, **Stereo**, and **Mix**.

12.6.5.5 User Defined

The user has to check this option in order to view the filtered calls in a separate pane. The filtered calls can be viewed by selecting 'Show User defined Sessions' from Call Summary > Filters menu.

12.6.5.6 Send e-mail

With this option, the PacketScan™ sends an e-mail containing useful information about each filtered call. User can check the options **Send Call Summary, HDLC File** and/or **Audio Recording** to send respective files. The audio record files will be written separately for left and right sessions and these files will be sent as an attachment with the mail. The user has to specify valid **Server name** and **e-mail ids** (From and To fields are mandatory) as shown in the figure below. The user can also specify multiple addresses in **To, Cc** and **Bcc** fields, but they should be separated by a comma (',') or semicolon (';').

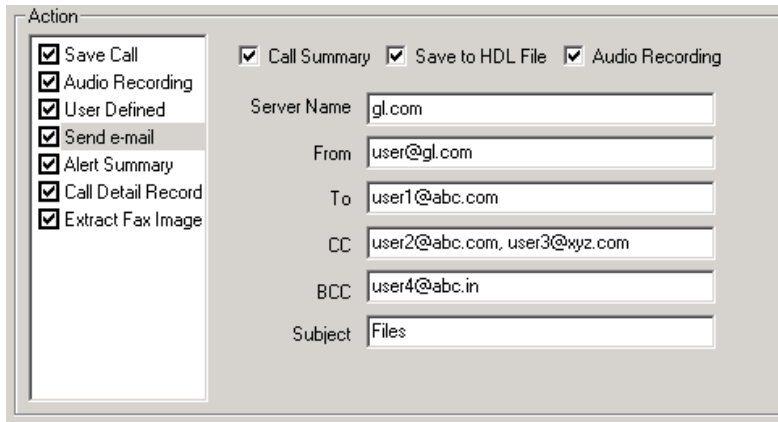


Figure 192: Send e-mail

12.6.5.7 Alert Summary

With this option, the user can set the alarm type and alarm message for the selected triggering type. Based on the specified criteria, the alerting summary will be displayed in the Alert Summary tab.

Alarm Type can be Critical, Major or Warning and the Alarm Message is the user specified message for the particular trigger type.

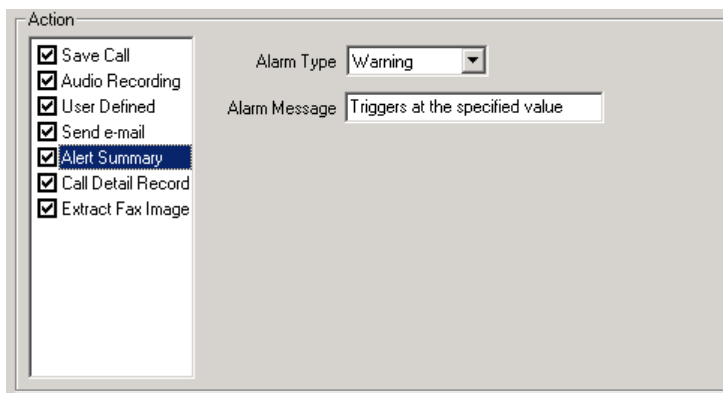


Figure 193: Alert Message

12.6.5.8 Call Detail Record

With this option, the PacketScan™ can output call detail records (CDR) in the form of three Comma Separated Value (CSV) files such as Call Side Record, Call Master Record, and Call Events Record along with the voice file recordings for each direction. PacketScan™ allows generating the CDRs for SIP and H.323 calls. These files are used by GL's [Call Data Records](#) and [Voice Band Application](#) for further processing and for each call it reports comprehensive information including a complete signaling information for each direction, all alarms and errors, detailed voiceband event information including dual tones (DTMF, MF, MFC-R2), fax tones, modem signals, and more, detailed analysis of the voiceband call including noise level, speech level, speech activity factor, echo measurements, and categorization of the call as voice, fax, modem, or data.

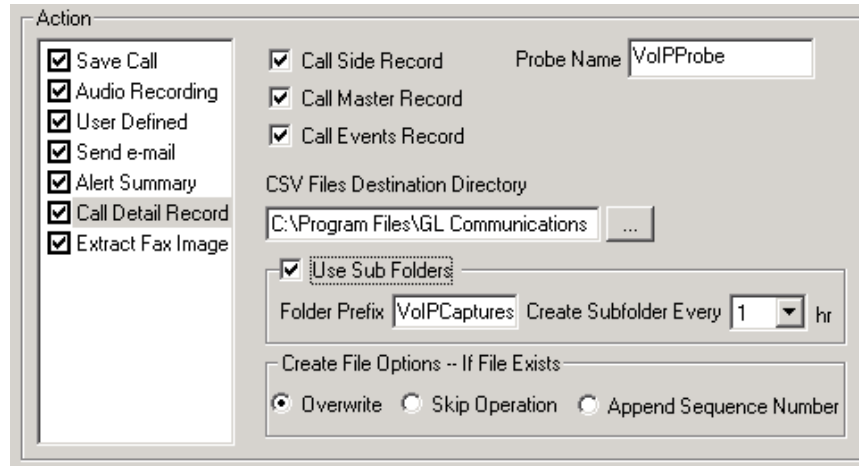


Figure 194: Call Detail Record

Call Side Record: This is a record concerning each party participating in the call, i.e., “endpoint”-specific data. Generally, there are two sides to a conversation, so there will be two records per call in this category. The figure below shows the Call Side Records file after having been loaded into an Excel spreadsheet. This record provides the following information:

• Probe ID	• Call ID
• Side	• Address
• File Name	• SSRC
• Codec	• Total Packets
• Missing Packets, Missing Packets Percentage	• Duplicate Packets, Duplicate Packets Percentage
• Reordered Packets, Reordered Packets Percentage	• Delay Packets, Delay Packets Percentage
• Conversational MOS, Listening MOS	• Conversational R, Listening R
• Average Gap	• Minimum Gap, Maximum Gap
• Average Delay	• Minimum Delay, Maximum Delay
• Average Jitter, Avg Inter Arrival Jitter	• Minimum Jitter, Maximum Jitter
• Cumulative Packets Lost	• Inband and Outband MC Digits

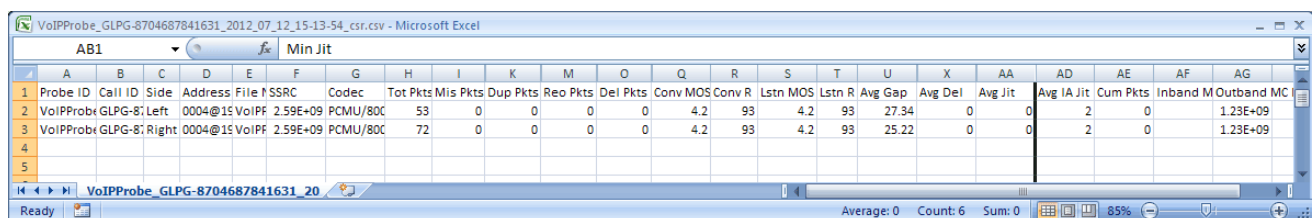


Figure 195: Call Side Record

Call Master Record: This is a record that contains fields concerning the call as a whole. In this category, there is one record per call. It provides summary of the call, that includes the following columns:

• Probe ID	• Call ID
• Side 1	• Side 2
• Protocol	• Start
• Released	• Duration
• Originating Side	• Terminating Side
• Release Code	• Source Directory
• Voice File Archive Directory	• PD (Post Dial) Delay and SD Delay(SessionDelay)

The figure below shows the Call Master Records file after having been loaded into an Excel spreadsheet.

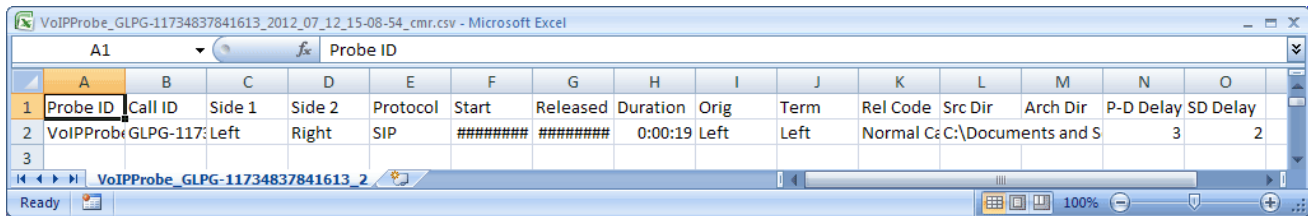


Figure 196: Call Master Record

Call Event Record: This might include call supervision events, mid-call digit events, alarms, and myriad other events. For Fax calls, segments regarding training, image transmission, etc. are important. Important event data such as the time, the duration of an event, the channel on which it occurred, an indication of the nature of the event, and information specific to the event itself are included in these records and collectively referred to as "Call Event Record".

This record gives an event-by-event account of the call. Events include the following:

• Probe ID	• Call ID
• Side	• Class ID
• Class	• Code ID
• Code	• Data
• Start	• Duration
• Source IP Address, Destination IP Address	• Source Port, Destination Port
• SIP Call Sequence	• Values

Probe ID	Call ID	Side	Class ID	Class	Code ID	Code	Data	Start	Dur	Src IP	Dest IP	Src Port	Dest Port	SIP CSeq	Values
VoIPProbe_G LPG-8704	Left		6	SIP		0 INVITE		0		192.168.1.1	192.168.1.1	54098	5060	1 INVITE	
VoIPProbe_G LPG-8704	Right		6	SIP		0 SIP/2.0 100 Trying		0.002351		192.168.1.1	192.168.1.1	54098	5060	1 INVITE	
VoIPProbe_G LPG-8704	Right		6	SIP		0 SIP/2.0 180 Ringing		0.002864		192.168.1.1	192.168.1.1	54098	5060	1 INVITE	
VoIPProbe_G LPG-8704	Right		6	SIP		0 SIP/2.0 200 OK		1.523548		192.168.1.1	192.168.1.1	54098	5060	1 INVITE	
VoIPProbe_G LPG-8704	Left		6	SIP		0 ACK		1.524939		192.168.1.1	192.168.1.1	54098	5060	1 ACK	
VoIPProbe_G LPG-8704	Right		7	Out-Band		0 MF 1		14.02465	0.1						pwr = 15.0
VoIPProbe_G LPG-8704	Right		7	Out-Band		0 MF 2		14.20425	0.1						pwr = 15.0
VoIPProbe_G LPG-8704	Right		7	Out-Band		0 MF 3		14.38393	0.1						pwr = 15.0
VoIPProbe_G LPG-8704	Right		7	Out-Band		0 MF 4		14.56462	0.1						pwr = 15.0
VoIPProbe_G LPG-8704	Right		7	Out-Band		0 MF 5		14.74442	0.1						pwr = 15.0
VoIPProbe_G LPG-8704	Right		7	Out-Band		0 MF 6		14.92498	0.1						pwr = 15.0
VoIPProbe_G LPG-8704	Right		7	Out-Band		0 MF 7		15.10461	0.1						pwr = 15.0
VoIPProbe_G LPG-8704	Left		7	Out-Band		0 MF 1		15.17658	0.06						pwr = 10.0
VoIPProbe_G LPG-8704	Left		7	Out-Band		0 MF 2		15.31625	0.06						pwr = 10.0
VoIPProbe_G LPG-8704	Right		7	Out-Band		0 MF 8		15.28423	0.1						pwr = 15.0

Figure 197: Call Event Record

Probe Name

User can define a Probe Name which is appended to file names to uniquely identify the device on which the capture is being done. Refer to the following example:

<Probe ID>_<Call ID>_<year>_<Month>_<Date>_<hour>-<minute>-<second>_csr.csv

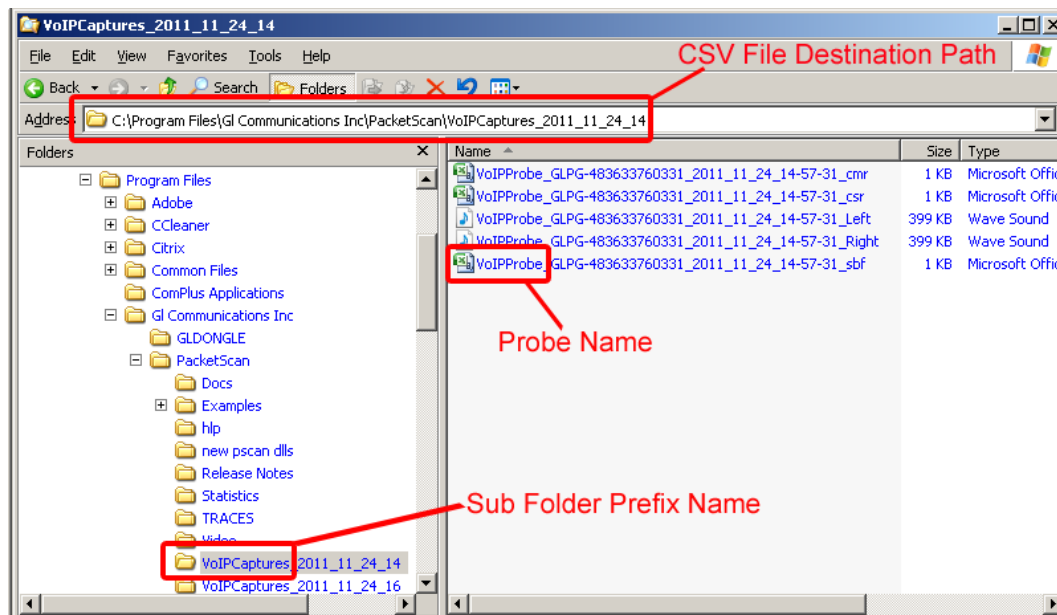
<Probe ID>_<Call ID>_<year>_<Month>_<Date>_<hour>-<minute>-<second>_cmr.csv

Example: VoIPProbe_G LPG-483633760331_2011_11_24_14-57-31_csr.csv

VoIPProbe_G LPG-483633760331_2011_11_24_14-57-31_cmr.csv

CSV Files Destination Directory – Use the browse button to save the file in the desired directory.

Use Sub Folders option allows creating sub folders automatically after the specified duration. Enable **Use Sub Folders** option to define Folder Name prefix and select time duration to create the subfolders. Refer to the figure below:



Additionally, if file with the same name already exists in the directory, users have options such as **Overwrite**, **Skip Operation**, and **Append Sequence Number**.

12.6.5.9 Extract Fax Image

This allows the users to extract the image in the TIFF format from all the fax calls. The user has to select this option as shown in the figure below. It also provide options to specify the file naming convention and the 'File Destination Directory' to save the extracted fax image.

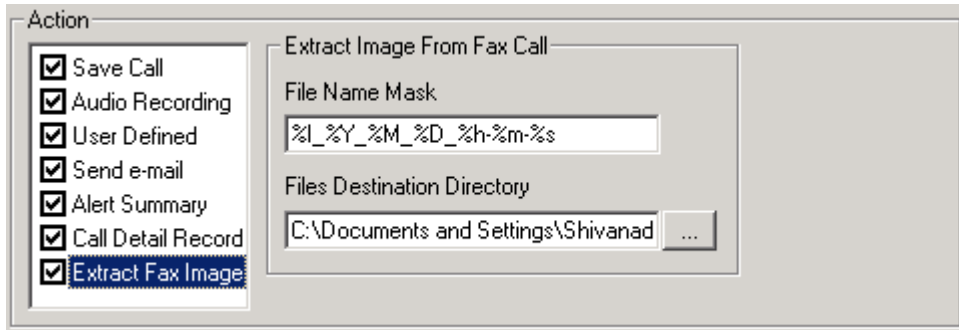


Figure 198: Extract Fax Image

12.6.5.10 File Menu Options

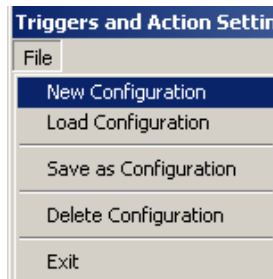


Figure 199: File Menu

New Configuration

Select **File > New Configuration** to select or enter file name from which new configuration has to be loaded. Default filter file extension is ***.tgr**.

Load Configuration

Select **File > Load Configuration** to select or enter file name from which configuration has to be loaded.

Save as Configuration

Select **File > Save as Configuration** to save current configuration to a different file. This will prompt to select or enter file name to save the configuration. This file can be used later by selecting '**Load configuration**' from menu to save the configuration to the file. Default filter file extension is ***.tgr**.

Delete Configuration

Select **File > Delete Configuration** to delete configuration set to a file. This will prompt to select or enter file name to delete the configuration.

Exit

Select **File > Exit** to exit from the Triggers and Actions Settings menu.

12.6.5.11 Example – Using Triggers and Action Feature

The example below explains the process of using **Triggers and Action** feature. The user has to provide proper parameters for settings. The same is applicable for online capture also.

- 1) Select **File > Offline** from PacketScan™ main menu and browse and select file 'PacketScan\examples\VoiceQuality\VoiceQualityTest.HDL'.
- 2) Invoke the Packet Data Analysis from View menu.
- 3) Select **Settings > Trigger and Action Settings** from Traffic Analyzer main menu.
- 4) Enter relevant Trigger name. E.g.: Trigger1 and click on **Add** button to add the name to the trigger list and check the box.
- 5) Note down the caller user agent of the desired session to be filtered. Now, select **Calling Party** under SIP from Filter Selection pane, and enter the user agent URL. Say for example, **0001@192.168.10.15**. Click **Activate** button to save the settings.
- 6) It is possible to filter the trace using either or both conditions (And, or), which is useful when specifying one or more criteria.
- 7) The filtered file can be saved as ***.HDL** or ***.PCAP** files and all the voice files can be saved in .wav format by checking **'Save Call'** and / or **'Audio Recording'** respectively.
- 8) Select and check **Save Call**, select the save option as **HDL**, check the **Call Summary** option, and browse for the desired directory to save the filtered file.
- 9) Select and check **Audio Recording** to save the file in ***.wav** format. Choose one of the audio mixing options, for example, select and option **To Separate Wave File**, and browse for the desired directory to save the filtered file.
- 10) Click 'OK' button to set the **Triggers and Action settings** and close the trace.
- 11) Now check for the option **'Enable Triggers'**, and **open** the trace.

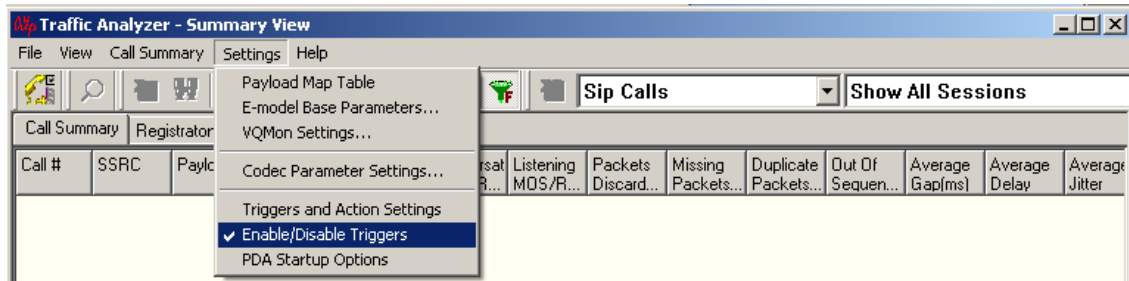


Figure 200: Enable Triggers

- 12) Then open the same file, and disable the trigger.
- 13) Observe the filtered files been created in the path mentioned in the trigger settings.



Note:

While using this **'Triggers And Action'** feature, one should check the option **'Enable Triggers'** under file menu. It is recommended to check this option before opening any offline file or before starting any real-time capture.

12.6.6 PDA Startup Options

This option allows user to configure startup tasks which will be started automatically whenever PDA is launched. It will also load the selected Triggers and Actions profile while invoking PDA.

- 1) Select **Settings** → **PDA Startup Options**
- 2) Enable **'Execute Tasks On PDA Startup'** and **'Enable Triggers and Actions'**

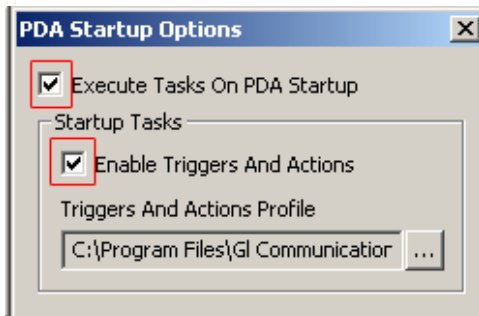


Figure 201: Enabling Startup Options

- 3) Browse and select **Trigger and Actions** profile file with an extension *.tgr

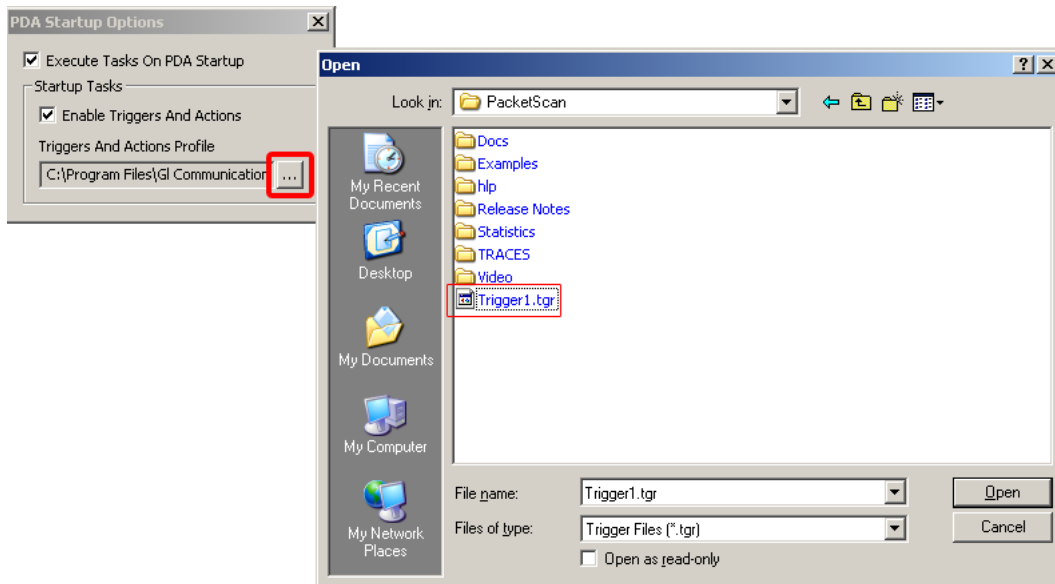


Figure 202: Loading tgr Profile File

The Trigger and Action profile path will be displayed in sipProt.ini file. Refer to the figure below:

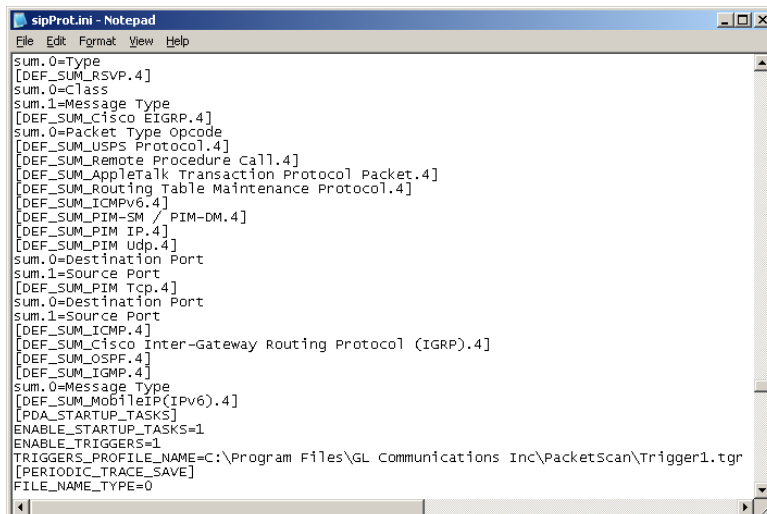


Figure 203: Trigger and Action Profile Path in sipProt.ini

12.7 Alert Summary

When something goes wrong with the call quality, it is important that the administrator is alerted on the same in order to initiate some corrective action. **PacketScan™** generates alerts when particular vital parameters go beyond a specified value. The user should specify the criteria in Triggers & Action Settings dialog and based on these the alerts are generated. For more details, refer to section Alert Summary Criteria.

Call#	Protocol	Message	Type	Threshold	Value	Caller	Callee	CallId
1	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.57	0005@192.168.1.236	0005@192.168.1.234	GLPG143457205760
2	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.39	0006@192.168.1.236	0006@192.168.1.234	GLPG143617205763
3	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.77	0008@192.168.1.236	0008@192.168.1.234	GLPG143617205769
3	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.36	0008@192.168.1.236	0008@192.168.1.234	GLPG143617205769
4	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.48	0009@192.168.1.236	0009@192.168.1.234	GLPG143617205772
5	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.30	0011@192.168.1.236	0011@192.168.1.234	GLPG143777205778
6	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.77	0012@192.168.1.236	0012@192.168.1.234	GLPG143927205781
6	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.31	0012@192.168.1.236	0012@192.168.1.234	GLPG143927205781
7	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.27	0001@192.168.1.231	0001@192.168.1.237	GLPG13407127763982
7	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.27	0001@192.168.1.231	0001@192.168.1.237	GLPG13407127763982
8	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	1.47	0002@192.168.1.231	0002@192.168.1.237	GLPG13417127763987
9	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	1.04	0003@192.168.1.231	0003@192.168.1.237	GLPG13425567763992

Figure 204: Alert Summary

The Alert Summary tab provides an active list of the alerts that have occurred during the test session. The notification list for the events that triggered the alerts is displayed in tabular columns. The alert summary has the following columns:

Call#: This displays the unique call number allocated by the VPA to each calls. These are similar to call numbers displayed in call summary .

Protocol: This displays the protocol type for the triggered call.

Message: This displays the user-defined alarm message set by the user in the Alert Summary action under Triggers and Action Settings.

Type: This displays the alarm type set by the user in Triggers and Action settings.

Threshold: This displays the threshold value set by the user for the particular triggering type in triggers and action settings.

Value: This displays the value at which the triggering is alerted.

Caller: This displays the address of the host user agent.

Callee: This displays the address of the destination user agent.

CallId: This displays the Call Id for the call that is present in INVITE message for a SIP call, while for a MEGACO call, it displays the context ID for the call that is present in the Add command.


To see the details of the call for which alert is generated; double-click on any summary I in the alert summary tab, which navigates to the particular call in the Call Summary tab for which the triggering has alerted. If call is purged, then message will pop-up saying call is purged.

(Intentional Blank Page)


Section 13.0 Packet Data Analysis-- Detail View (RTP Diagnostic View)

13.1 Overview

In order to open the Detail View:

- Select **View > Call Detail View** from the main menu or
- Click  from the tool bar.

RTP Detail View allows the user to have a detail look at the two (or one) RTP sessions that are part of a single call. The view is divided into two parts a left and a right pane to accommodate the two sessions. This distinction assists in any comparisons that are to be made between the two sessions. Here each frame of the selected session is dissected and its contents are displayed in a tabular form for easier viewing and to make comparisons. Vital aspects from the RTP frame needed for close analysis are included in the table. Once a session has been selected, it would be updated in real-time, i.e., as and when new packets pertaining to the call are received they are processed and added to the table(s).

The main toolbar contains shortcut buttons for moving between Summary and Detail window, and bringing VPA into foreground. Select a call/session from the Summary View and select **Call Summary > Call Detail View** from the main menu or click  from the tool bar.

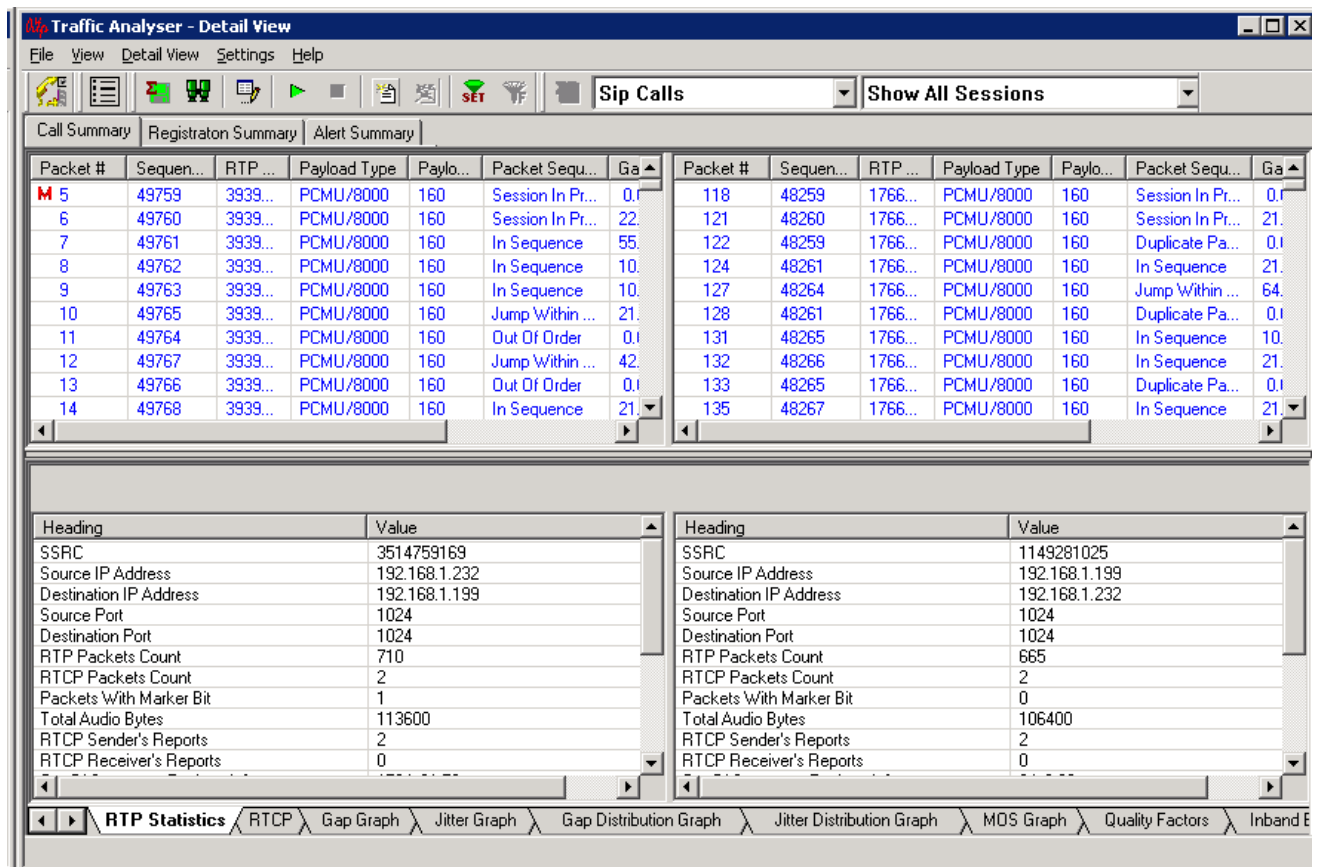


Figure 205: Detail View

13.2 Columns in Detail View

The detail view displays the following information in the tabular format from left to right as shown in the figure below.

Packet #	Sequence #	RTP Timestamp	Payload Type	Payload Len	Packet Sequence	Gap(ms)	Gap At Sender(ms)	Delay	Jitter
M 8	8020	1446566368	PCMU/8000	160	Session In Probat...	0.00	0.00	0	0.00
10	8021	1446566528	PCMU/8000	160	Session In Probat...	21.48	20.00	1	0.09
11	8022	1446566688	PCMU/8000	160	In Sequence	10.74	20.00	-9	0.67
13	8023	1446566848	PCMU/8000	160	In Sequence	22.47	20.00	2	0.77
15	8024	1446567008	PCMU/8000	160	In Sequence	21.49	20.00	1	0.81
17	8025	1446567168	PCMU/8000	160	In Sequence	21.45	20.00	1	0.85
19	8026	1446567328	PCMU/8000	160	In Sequence	21.49	20.00	1	0.88
22	8027	1446567488	PCMU/8000	160	In Sequence	21.47	20.00	1	0.91
24	8028	1446567648	PCMU/8000	160	In Sequence	21.49	20.00	1	0.94
26	8029	1446567808	PCMU/8000	160	In Sequence	21.48	20.00	1	0.97
27	8030	1446567968	PCMU/8000	160	In Sequence	10.78	20.00	-9	1.48
29	8031	1446568128	PCMU/8000	160	In Sequence	21.48	20.00	1	1.48
31	8032	1446568288	PCMU/8000	160	In Sequence	21.47	20.00	1	1.47
33	8033	1446568448	PCMU/8000	160	In Sequence	21.48	20.00	1	1.46
36	8034	1446568608	PCMU/8000	160	In Sequence	26.38	20.00	6	1.77

Figure 206: Detail View Columns

- **Packet #:** The packet number shows frame number in PacketScan™. This column is also used to indicate whether the Marker Bit is set in this particular RTP packet. This is reflected by the presence of a (red colored) M. If the marker is set, it is shown as 'M', as shown in the figure Marker Bit [Marker Bit](#).
- **Sequence #:** This column shows the RTP Sequence number of the packet. This sequence number is in sequential order from the particular RTP Packet to which Marker bit is set.
- **RTP Timestamp:** RTP Timestamp is the Time at which the particular RTP packet is initiated.
- **Payload Type:** For a RTP packet, this column contains the Payload Type description. It is a string that identifies the codec, whether the data is Audio or Video, the sampling rate and the number of channels employed. A glance at this will give the user complete information about the codec used and the data encoding parameters.
- **Payload Len:** This gives the length of the payload type.
- **Packet Sequence:** A string in this column gives the status of the RTP Packet Sequence. This column declares whether the packet is in sequence or not. The various possible strings in this column are explained below:

In Sequence

The Packet Sequence of the RTP Packet is In Sequence if the sequence # of the packet is incremented by 1 than the sequence # of the previous packet, then the string In Sequence is displayed in this column.

Out of Sequence

The Out of Sequence is shown in Packet Sequence Column when the sequence # in not in sequence.

Wrap Around

The RTP Sequence number wraps around after 65535 packets. Once the sequence number reaches 65535, the sequence number counter is restarted from 0. Whenever this happens the Packet Sequence column displays Wrap Around.

Duplicate Packet

If a packet is received again (due to retransmission at the source or due to some irregularities in the network), which means the particular RTP sequence number has been received earlier; the packet is considered a duplicate and the string Duplicate Packet is displayed in the Packet Sequence column.

Pkt Jump Out of Limit

In VPA, a RTP sequence tolerance limit of 50 is used as default; any jump of the sequence number leads to a Re-set of the various parameters used for calculating delay, jitter, gap etc. Whenever this happens the Packet Sequence column displays the string Pkt Jump out of limit.

Pkt Jump within Limit

If the Jump is within the preset limit of 50 the display in the Packet Sequence column will be Pkt Jump within limit.

SSRC Collision

Whenever a SSRC Collision occurs, this is displayed in the Packet Sequence column as 'SSRC Collision'.

Session In Probation

Any RTP stream would be considered as valid, only after more than 2 Packets for that session has been received. The first two packets are considered as being in probation, which is suitably reflected in the Packet Sequence column of these packets. The display for these packets is displayed as Session in Probation.

- **Gap (ms)**: Difference in the capture time of the RTP packet from its previous packet calculated in milliseconds is shown as Gap (ms) as shown in the figure below. (Please Refer RFC 1889 for more details)
- **Gap at Sender (ms)**: Difference in the RTP timestamp of this packet and the previous packet calculated in milliseconds. (Please Refer RFC 1889 for more details)
- **Delay (ms)**: Delay is calculated in milliseconds for the packets as shown in the figure below. (Please Refer RFC 1889 for more details)
- **Jitter (ms)**: Jitter calculated in milliseconds for this packet is shown in the figure below. (For more details please Refer RFC 1889)

13.2.1 Functions Invoked By Right Click

The RTP Details tables provide two options, which can be invoked by a right click on either of them.

Sync Scroll

Selecting this option would enable both the tables (left and right) to scroll in a synchronized manner as shown in the figure below. Scrolling up/down in one of the table would do the same for the other. If this option is enabled a Check mark is seen in front of the menu item.

Show Latest

When this option is selected the most recently added frame is brought to view by default as shown in the figure below. If this option is enabled a Check mark appears in front of the menu item.

Pack...	Sequ...	RT...	Payload ...	Payload Len	Packet Sequ...	Gap(ms)	Gap At Sender(ms)	Delay	Jitter	
4491	13425	119...	PCMA/8...	160	In Sequence	19.24	20.00	0	0.97	
4492	13426	119...	PCMA/8...	160	In Sequence	21.14	20.00	1	0.98	
4493	13427	119...	PCMA/8...	160	In Sequence	19.31	20.00	0	0.96	
4494	13428	119...	PCMA/8...	160	In Sequence	21.12	20.00	1	0.97	
4495	13429	119...	PCMA/8...	160	In Sequence	19.16	20.00	0	0.96	
4496	13430	119...	PCMA/8...	160	In Sequence	19.16	20.00	0	0.96	
4497	13431	119...	PCMA/8...	160	In Sequence	21.11	20.00	1	0.96	
4498	13432	119...	PCMA/8...	160	In Sequence	19.29	20.00	0	0.95	
4499	13433	119...	PCMA/8...	160	In Sequence	21.08	20.00	1	0.95	
4500	13434	119...	PCMA/8...	160	In Sequence	19.30	20.00	0	0.94	
4501	13435	119...	PCMA/8...	80	In Sequence	18.62	20.00	-1	0.97	

Figure 207: Show Latest

Column Resizing and Reordering

Columns of the detail view can be resized by dragging the mouse and reordered using drag and drop mouse operation:

Packet #	Sequence #	RTP Timestamp	Payload Type	Payload Len	Packet Sequence	Gap(ms)	Gap At Sender(ms)	Delay	Jitter	
7	35127	1336704049	PCMU/8000	160	Session In Probat...	19.71	20.00	0	0.02	
9	35128	1336704209	PCMU/8000	160	In Sequence	20.46	20.00	0	0.05	
11	35129	1336704369	PCMU/8000	160	In Sequence	19.60	20.00	0	0.07	
12	35130	1336704529	PCMU/8000	160	In Sequence	19.46	20.00	0	0.11	
15	35131	1336704689	PCMU/8000	160	In Sequence	20.55	20.00	0	0.13	
17	35132	1336704849	PCMU/8000	160	In Sequence	19.52	20.00	0	0.16	
19	35133	1336705009	PCMU/8000	160	In Sequence	21.48	20.00	1	0.23	
21	35134	1336705169	PCMU/8000	160	In Sequence	19.59	20.00	0	0.25	
23	35135	1336705329	PCMU/8000	160	In Sequence	20.44	20.00	0	0.26	
25	35136	1336705489	PCMU/8000	160	In Sequence	19.54	20.00	0	0.27	
26	35137	1336705649	PCMU/8000	160	In Sequence	19.51	20.00	0	0.29	

Packet #	Sequenc...	RTP Tim...	Payload Len	Payload Type	Packet Sequence	Gap(ms)	Gap At Sender(ms)	Delay	Jitter	
7	35127	1336704...	160	PCMU/8000	Session In Probat...	19.71	20.00	0	0.02	
9	35128	1336704...	160	PCMU/8000	In Sequence	20.46	20.00	0	0.05	
11	35129	1336704...	160	PCMU/8000	In Sequence	19.60	20.00	0	0.07	
12	35130	1336704...	160	PCMU/8000	In Sequence	19.46	20.00	0	0.11	
15	35131	1336704...	160	PCMU/8000	In Sequence	20.55	20.00	0	0.13	
17	35132	1336704...	160	PCMU/8000	In Sequence	19.52	20.00	0	0.16	
19	35133	1336705...	160	PCMU/8000	In Sequence	21.48	20.00	1	0.23	
21	35134	1336705...	160	PCMU/8000	In Sequence	19.59	20.00	0	0.25	
23	35135	1336705...	160	PCMU/8000	In Sequence	20.44	20.00	0	0.26	
25	35136	1336705...	160	PCMU/8000	In Sequence	19.54	20.00	0	0.27	
26	35137	1336705...	160	PCMU/8000	In Sequence	19.51	20.00	0	0.29	

Figure 208: Column Resizing and Reordering

In the above figure **Sequence #** and **RTP Timestamp** columns are resized. **Payload Type** and **Payload Len** columns are reordered.

13.3 Statistics and Graphs

In the lower pane of the detail view one can get the complete details of a single selected call. A host of graphs and RTCP details are displayed here. Select a tab to move between the various options.

13.3.1 RTP Statistics

Heading	Value	Heading	Value
SSRC	2749889793	SSRC	2800221441
Source IP Address	2001::f01:21fd::fd0d:5606:3df0:2bfb:b056	Source IP Address	21:918:12:1::54
Destination IP Address	21:918:12:1::54	Destination IP Address	2001::f01:21fd::fd0d:5606:3df0:2bfb:b056
Source Port	8002	Source Port	8002
Destination Port	8010	Destination Port	8010
RTP Packets Count	1251	RTP Packets Count	1240
RTCP Packets Count	3	RTCP Packets Count	3
Packets With Marker Bit	1	Packets With Marker Bit	1
Total Audio Bytes	200001	Total Audio Bytes	198400
RTCP Sender's Reports	2	RTCP Sender's Reports	3
RTCP Receiver's Reports	1	RTCP Receiver's Reports	0
Out Of Sequence Packets \ %	0 \ 0.00	Out Of Sequence Packets \ %	0 \ 0.00
Missing Packets \ %	0 \ 0.00	Missing Packets \ %	0 \ 0.00
Duplicate Packets \ %	0 \ 0.00	Duplicate Packets \ %	0 \ 0.00
MOS-CQ \ Conversational R	4.20 \ 93	MOS-CQ \ Conversational R	1.98 \ 31
MOS-LQ \ Listening R	4.20 \ 93	MOS-LQ \ Listening R	1.62 \ 32
G.107 R	92	G.107 R	40
Nominal MOS \ Nominal R	4.20 \ 93	Nominal MOS \ Nominal R	4.20 \ 93
Discarded Packets	0 \ 0.00	Discarded Packets	495 \ 39.92

Figure 209: Call Information

The RTP Statistics displays the following information

- **SSRC:** SSRC (Synchronization Source) identifier associated with this RTP session. In case of RTCP only sessions, this will be the SSRC of the Sender (the side which generates the RTCP packet).
- **Source / Destination IP Address:** Gives the source and destination IP address (in IPv4 or IPv6 format).
- **Source / Destination Port:** Gives the source and destination port number.
- **RTP Packets Count:** Gives the total number of RTP packets.
- **RTCP Packets Count:** Gives the total number of RTCP packets.
- **Packets with Marker Bits:** Gives the total number of packets having marker bits for RTP calls.
- **Total Audio Bytes:** Gives the total number of audio bytes.
- **RTCP Sender's and Receiver's Reports:** Gives the total number of RTCP sender's and receiver's reports.
- **Out of Sequence packets \ %:** Gives the count and percentage of total RTP Packets in this session that has been received out of sequence.
- **Missing Packets \ %:** Gives the total RTP Packets that have not been received by PacketScan™ in this session. Also, displays the percentage of packets not received to the total number of packets received.
- **Duplicate packets \ %:** Gives the count and percentage of total duplicate RTP Packets in this session.
- **MOS-CQ \ Conversational R:** Gives the Mean Opinion Score based on conversational quality that does not consider delay and recency effects.
- **MOS-LQ \ Listening:** Gives the Mean Opinion Score based on listening quality that considers delay and recency effects.
- **G.107 R:** Gives the G.107 R-Factor.
- **Nominal MOS \ Nominal R:** Gives the Nominal (maximum) MOS and R-factor quality for the selected codec.
- **Discarded Packets:** Gives the total count and percentage of discarded packets to the number of received packets.

13.3.2 RTCP Statistics

The display below the RTP Detail View is called the RTCP Details. The different options available in this pane are as shown in the figure below:

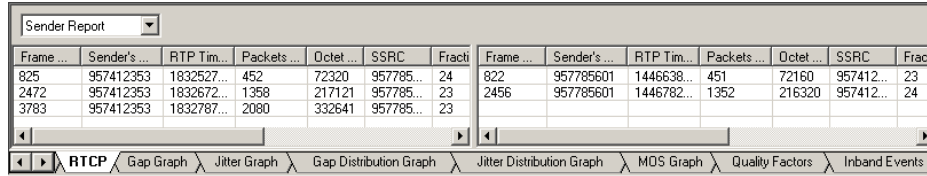


Figure 210: RTCP

Column Details

Sender Report

Frame Number	Sender's SSRC	Rtp Timestamp	Packets Sent	Octet Count	SSRC	Fraction Lost	CFL	EHSNR	Jitter	LSR	DLSR (sec)
284	634786917	0	113	18080	211...	0	0	11102	512	0	0.00
2161	634786917	0	347	55520	211...	0	0	12734	360	0	0.00
2523	634786917	0	679	108640	211...	0	0	12763	360	0	0.00
2886	634786917	0	963	154080	211...	0	0	12841	360	0	0.00
3066	634786917	0	1109	177440	211...	0	0	12874	360	0	0.00
3440	634786917	0	1324	211840	211...	0	0	13032	360	0	0.00
3686	634786917	0	1525	244000	211...	0	0	13076	360	0	0.00
3972	634786917	0	1779	284640	211...	0	0	13107	360	0	0.00
4204	634786917	0	1903	304480	211...	0	0	13214	360	0	0.00
4408	634786917	0	1978	316480	211...	0	0	13342	360	0	0.00

Figure 211: RTCP Details of Sender Report

Receiver Report

Frame Number	Sender's SSRC	SSRC	Fraction Lost	CFL	EHSNR	Jitter	LSR	DLSR (sec)
431	634786917	211993...	0	0	11248	512	0	0.00
739	634786917	211993...	0	0	11555	512	0	0.00
879	634786917	211993...	0	0	11694	512	0	0.00
1026	634786917	211993...	0	0	11840	512	0	0.00
1188	634786917	211993...	0	0	12001	360	0	0.00
1324	634786917	211993...	0	0	12136	360	0	0.00
1510	634786917	211993...	0	0	12321	360	0	0.00
1808	634786917	211993...	0	0	12618	360	0	0.00
1879	634786917	211993...	0	0	12688	360	0	0.00
1880	634786917	0	0	0	0	0	0	0.00

Figure 212: RTCP Details of Receiver Report

The columns of the Sender Report and Receiver Report (Report blocks) table are explained below. (Refer RFC 1889 for more details)

- **Frame Number:** It is the frame number of the RTCP packet as in VPA
- **Sender's SSRC** – It's the source identifier (32-bit numeric SSRC identifier carried in the RTP header which is not dependent upon the network address) from where the packets are getting originated
- **RTP Timestamp (only in Sender Report)**- It is the wall clock time when the packet was sent with the units and offset as in timestamp of RTP data packet
- **Packets Sent (only in Sender Report):** It is the total number of RTP packets that has been sent from the beginning of session till the SR packet is sent
- **Octet Count (only in Sender Report):** It is the total number of payload octets sent (excluding the header length of RTP) since the starting of transmission till the time this SR packet was generated
- **SSRC:** It indicates the source identifier to which information in this reception block is being sent
- **Fraction Lost:** It is the fraction of RTP data packets from the source identifier lost since the previous SR or RR packet was sent
- **CFL (Cumulative Fraction Lost):** The total numbers of RTP data packets that have been lost from source SSRC since the beginning of reception
- **EHSNR (Extended Highest Sequence Number Received):** The least significant 16 bits contain the highest sequence number received in an RTP data packet from source SSRC, and the most

significant 16 bits extend that sequence number with the corresponding count of sequence number cycles

- **Jitter** – This indicates the Inter-Arrival Jitter received in this frame, which is measured in timestamp units and expressed as an unsigned integer
- **Last SR** – (Last SR time stamp) The middle 32 bits out of 64 bits in the NTP(Network Time Protocol) timestamp, received as part of the most recent RTCP sender report (SR) packet from source SSRC
- **DLSR** – (Delay Since Last SR) The delay, expressed in units of 1/65536 seconds, between receiving the last SR packet from source SSRC and sending this reception report block

SDES Item (Source description items)

Frame Number	SSRC/CSRC	SDES Type	Content
907	907	CNAME	GL Communication
2509	2509	CNAME	GL Communication

Figure 213: SDES Item

The columns for SDES table are:

- **Frame Number**-- It is the frame number of the RTCP packet as in VPA
- **SSRC/CSRC** – Identifies the SSRC / CSRC frames whose information is carried in the particular chunk of the SDES packet
- **SDES Type**-- Identifies which SDES item the information pertains to. The following are the SDES types that are identified here:
 - CNAME
 - NAME
 - TOOL
- **Content/SDES Item**-- The string that describes the SDES type is displayed here (like user and domain name, cannon name of source etc).

Bye Packet (Indicates end of participation)

Frame Number	SSRC/CSRC	Reason for Leaving
3927	1410271545	

Figure 214: Bye Packet

The columns for Bye packet are:

- **Frame Number**-- It is the frame number of the RTCP packet as in VPA
- **SSRC**-- Identifies the SSRC / CSRC frames of the sender
- **Reason for leaving** – The Bye packet contains octets representing the text indicating the reason for leaving, e.g., 'camera malfunction' or 'RTP loop detected' and so on

13.4 Graphs

Various graphs related to individual RTP session(s) are displayed in the Call Detail View. Unlike Summary View, users can select both the sessions of the call from the statistics column, and then select the graph by using the tabs at the bottom of the Call Detail View. Plotting both sessions in the same view enables comparison between them. The different graphs provided here are:

13.4.1 Gap Graph

Gap graph plots the Gap (in milliseconds) versus the packet number. If both the sessions of the call have been selected then plotting them in the same view enables comparison between them. A right-click on the graph enables the user to print, save, and to show 2D view. Gap Graph 3D and 2D views are shown in the figures below.

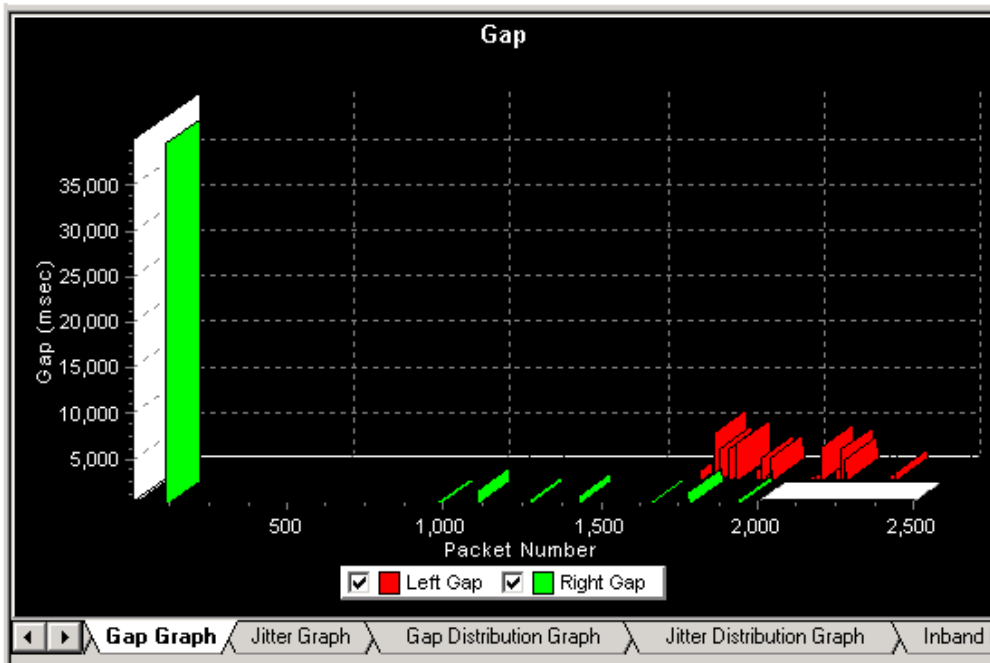


Figure 215: 3D Gap Graph

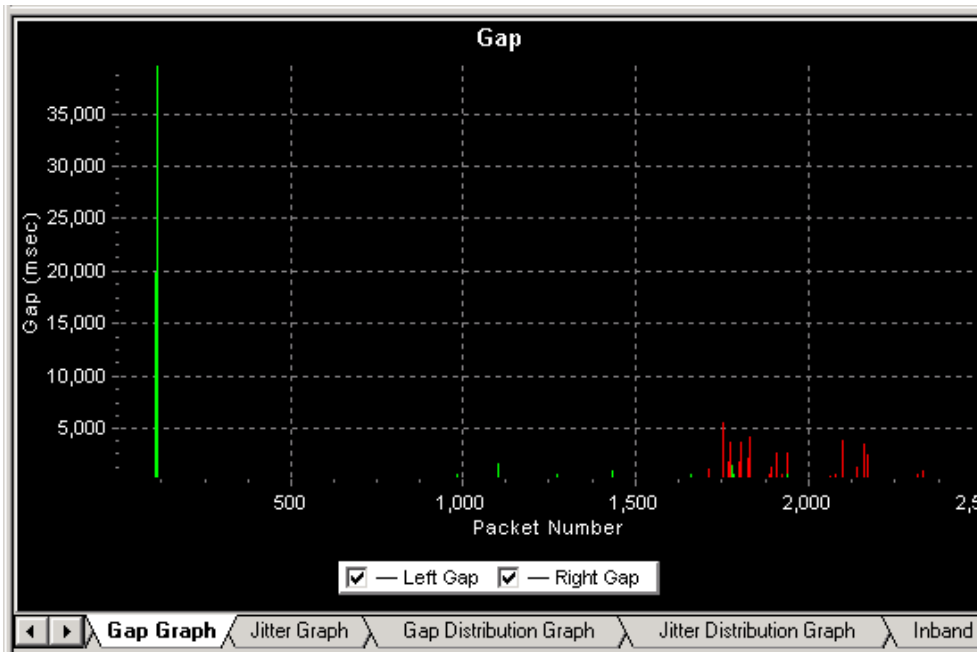


Figure 216: 2D Gap Graph

13.4.2 Jitter Graph

Jitter graph plots the Jitter values versus the packet number similar to gap graph. Like gap graph the jitter values for both the selected sessions are plotted in the same view and thereby enabling comparisons. Jitter graph 3D and 2D views are shown in the figures below.

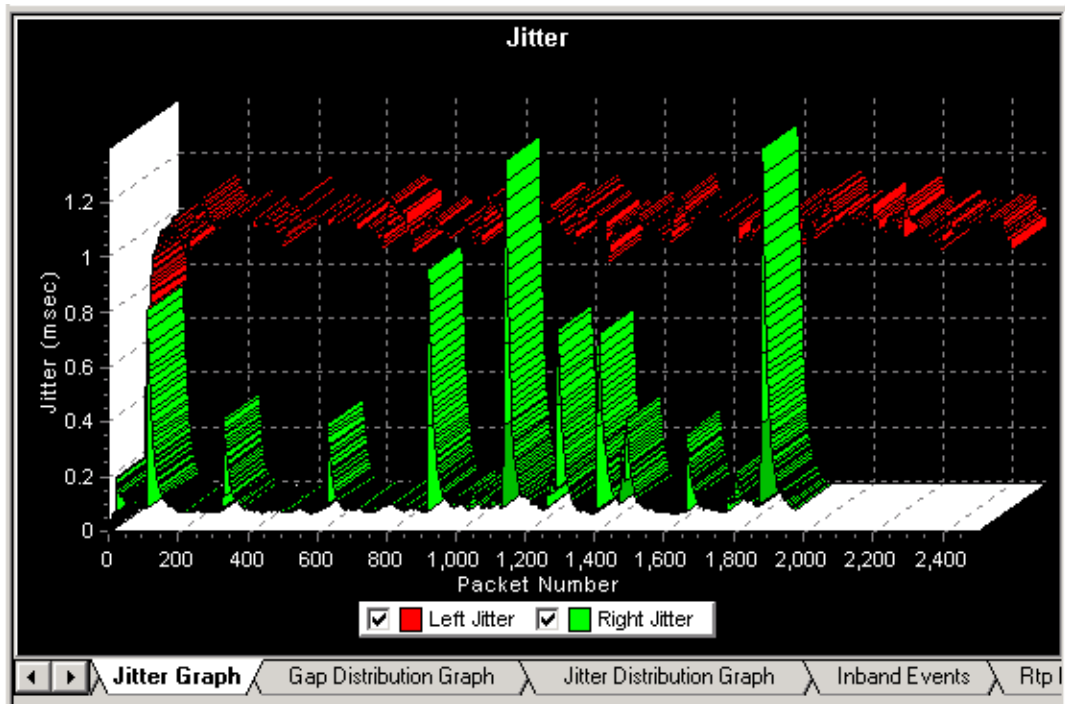


Figure 217: 3D Jitter Graph



Figure 218: 2D Jitter Graph

13.4.3 Gap Distribution Graph

This graph is similar to the 'Average Jitter distribution graph' explained in (section Average Jitter Distribution) in Summary View. Here the number of packets with a particular value of gap is plotted against the (gap) value. Like the above graphs this too plots the two selected sessions simultaneously. Gap Distribution graph 3D and 2D views are shown in the following figures.

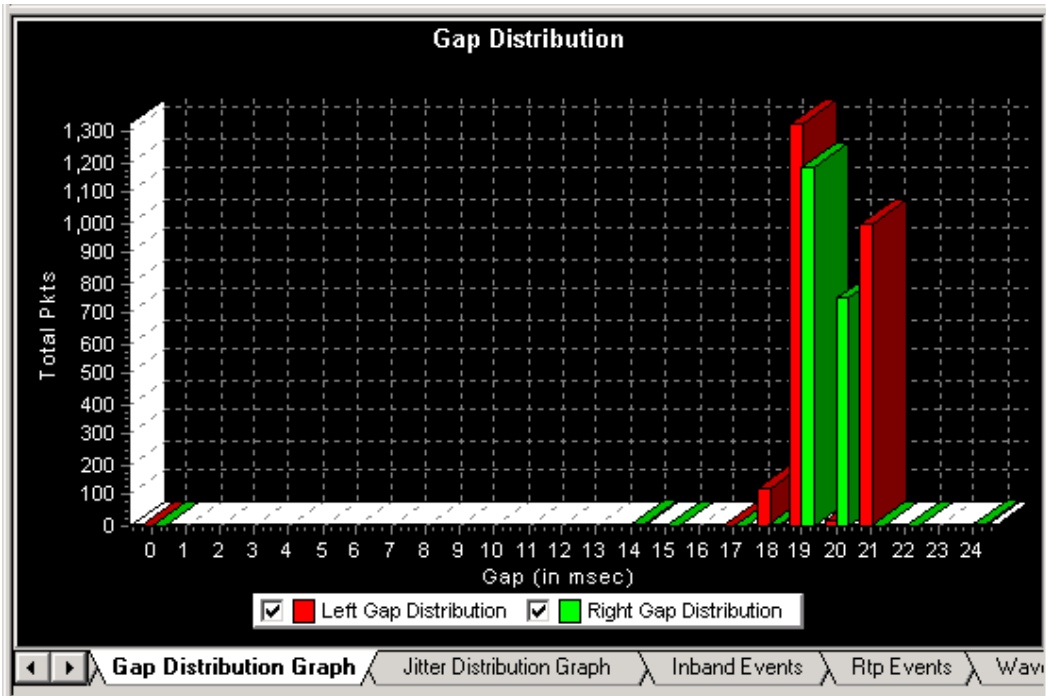


Figure 219: 3D Gap Distribution Graph

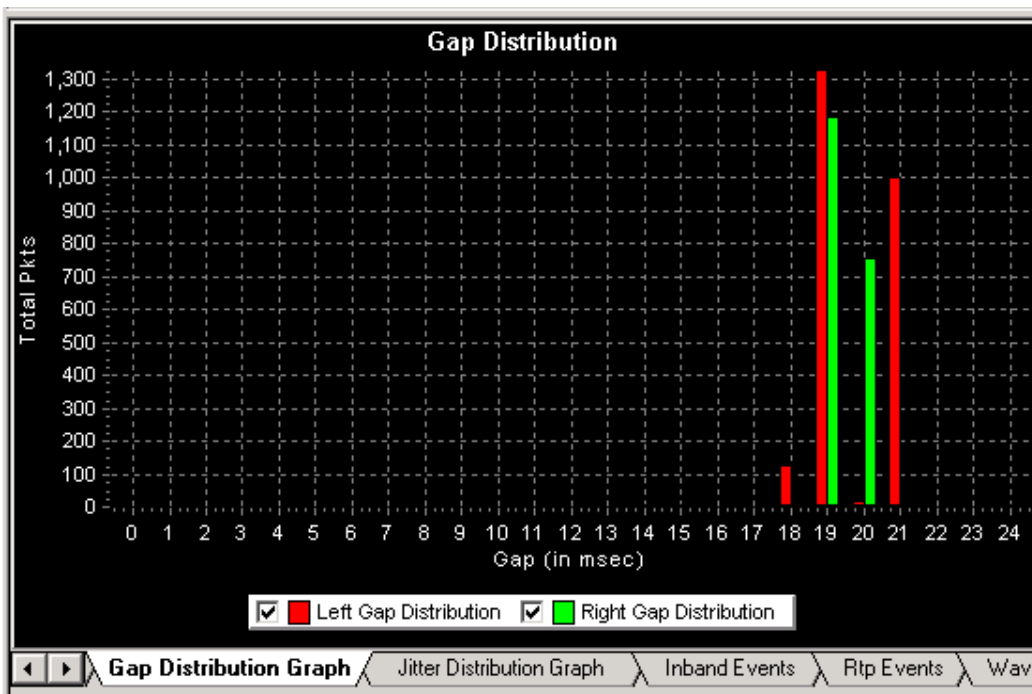


Figure 220: 2D Gap Distribution Graph

13.4.4 Jitter Distribution Graph

Like the 'Gap Distribution Graph', Jitter distribution is plotted in the graph. Here the number of packets with a particular value of jitter is plotted against the jitter value. Options are provided to save and print this graph as well. Jitter Distribution graph 3D and 2D views are shown in the figures below.

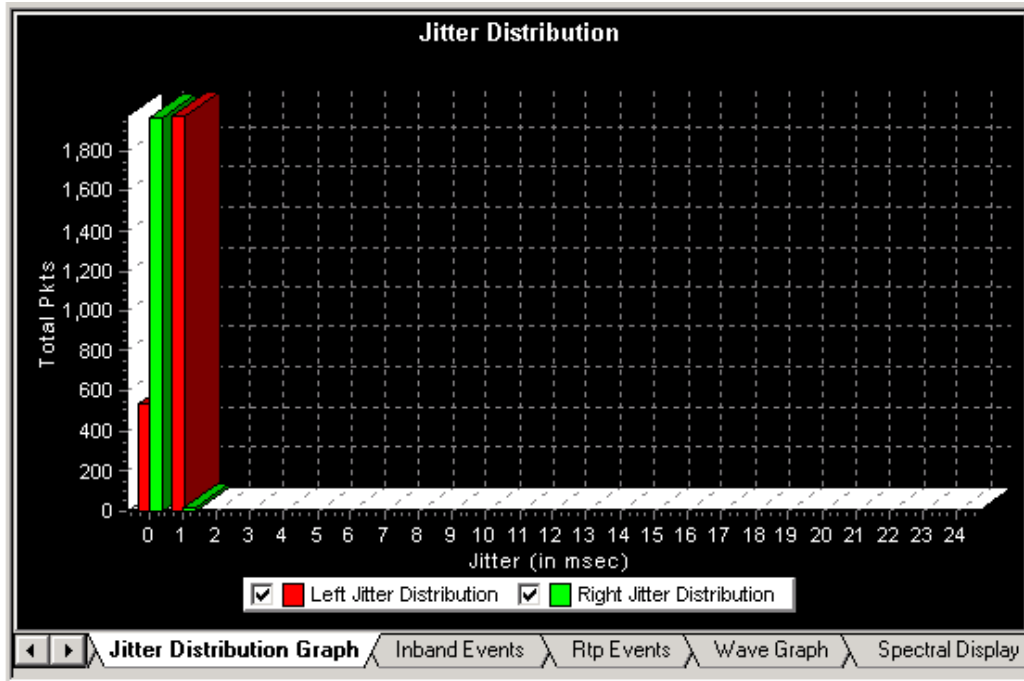


Figure 221: 3D Jitter Distribution Graph

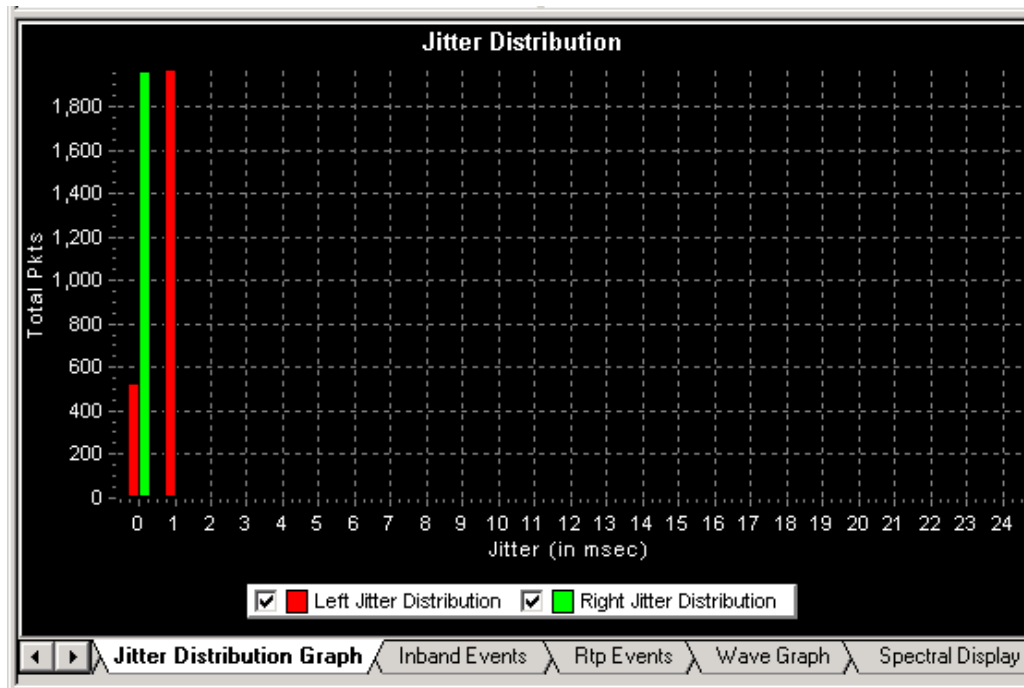


Figure 222: 2D Jitter Distribution Graph

13.4.5 MOS Graph (Mean Opinion Score)

This graph displays MOS over the duration of the individual sessions as shown in the figure below:

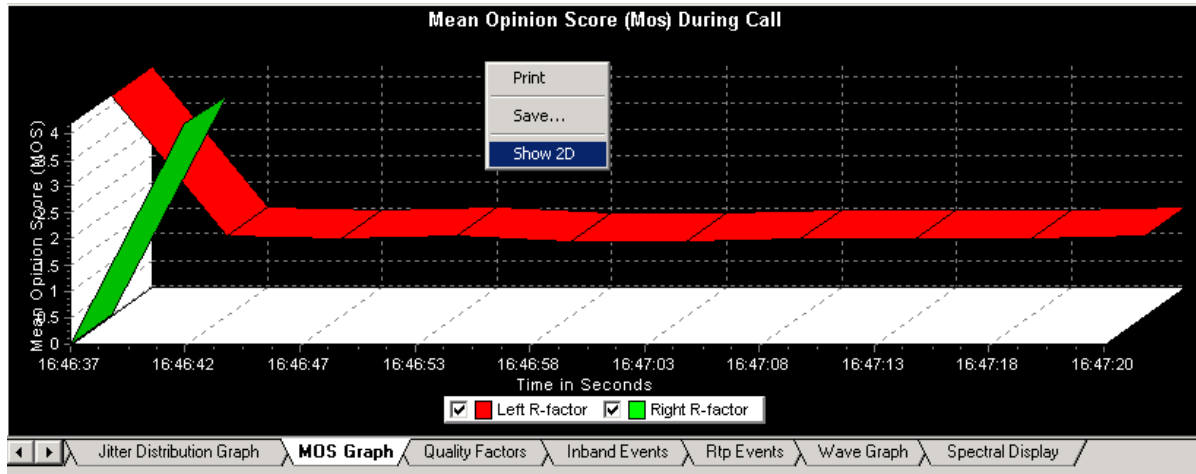


Figure 223: 3D MOS Graph

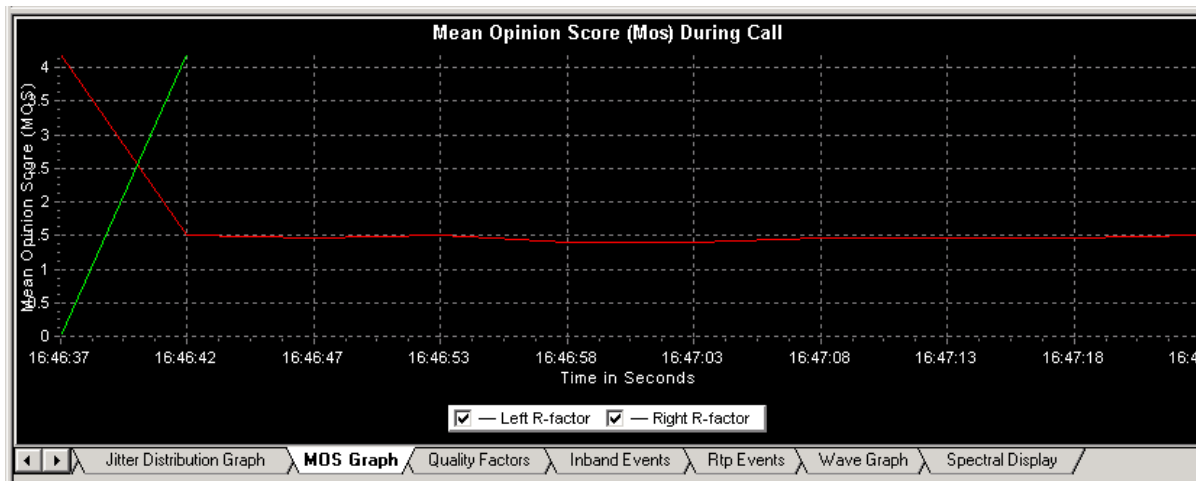


Figure 224: 2D MOS Graph

13.4.6 Inband Events

This displays inband DTMF and MF digits as they are received on selected RTP stream as shown in the figure below.

TimeStamp	Type	Event	On	Power	Freq	TimeStamp	Type	Event	On	Power	Freq
00:00:00.000	IDLE		430	0.00		00:00:00.000	IDLE		54350	0.00	
00:00:00.430	DTMF	1	80	-1.89	69	00:00:54.350	MF	1	80	-1.86	70
00:00:00.510	IDLE		80	0.00		00:00:54.430	IDLE		80	0.00	
00:00:00.590	DTMF	2	80	-1.87	69	00:00:54.510	MF	2	80	-1.89	70
00:00:00.670	IDLE		80	0.00		00:00:54.590	IDLE		80	0.00	
00:00:00.750	DTMF	3	80	-1.85	69	00:00:54.670	MF	3	80	-1.87	90
00:00:00.830	IDLE		80	0.00		00:00:54.750	IDLE		80	0.00	
00:00:00.910	DTMF	4	80	-1.87	77	00:00:54.830	MF	4	80	-1.86	70
00:00:00.990	IDLE		80	0.00		00:00:54.910	IDLE		80	0.00	
00:00:01.070	DTMF	5	80	-1.85	77	00:00:54.990	MF	5	80	-1.87	90
00:00:01.150	IDLE		80	0.00		00:00:55.070	IDLE		80	0.00	
00:00:01.230	DTMF	6	80	-1.87	77	00:00:55.150	MF	6	80	-1.87	11
00:00:01.310	IDLE		80	0.00		00:00:55.230	IDLE		80	0.00	
00:00:01.390	DTMF	7	80	-1.87	85	00:00:55.310	MF	7	80	-1.87	70
00:00:01.470	IDLE		80	0.00		00:00:55.390	IDLE		80	0.00	
00:00:01.550	DTMF	8	80	-1.90	85	00:00:55.470	MF	8	80	-1.88	90
00:00:01.630	IDLE		80	0.00		00:00:55.550	IDLE		80	0.00	
00:00:01.710	DTMF	9	80	-1.88	85	00:00:55.630	MF	9	80	-1.87	11
00:00:01.790	IDLE		80	0.00		00:00:55.710	IDLE		80	0.00	
00:00:01.870	DTMF	0	80	-1.88	94	00:00:55.790	MF	5	80	-1.87	90
00:00:01.950	IDLE		80	0.00		00:00:55.870	IDLE		80	0.00	

Figure 225: Inband Events

- **Timestamp:** Capture Time Stamp
- **Type:** DTMF or MF
- **Event:** Digits
- **On-Time:** Duration of the digit
- **Power:** Total power of the Digit
- **Freq1 / Power1:** Frequency and power of the first Tone
- **Freq2 / Power2:** Frequency and power of the Second Tone

Functions invoked by right click

Digits Only: If this option is selected only DTMF and MF tones are shown. This Digits Only option is effective for the next subsequent data and not for the existing one.

TimeStamp	Type	Event	On	Power	Freq	TimeStamp	Type	Event	On	Power	Freq
00:00:00.430	DTMF	1	80	-1.89	69	00:00:54.350	MF	1	80	-1.86	70
00:00:00.530	DTMF	2	80	-1.87	69	00:00:54.510	MF	2	80	-1.89	70
00:00:00.750	DTMF	3	80	-1.85	69	00:00:54.670	MF	3	80	-1.87	90
00:00:00.910	DTMF	4	80	-1.87	77	00:00:54.830	MF	4	80	-1.86	70
00:00:01.070	DTMF	5	80	-1.85	77	00:00:54.990	MF	5	80	-1.87	90
00:00:01.230	DTMF	6	80	-1.87	77	00:00:55.150	MF	6	80	-1.87	11
00:00:01.390	DTMF	7	80	-1.87	85	00:00:55.310	MF	7	80	-1.87	70
00:00:01.550	DTMF	8	80	-1.90	85	00:00:55.470	MF	8	80	-1.88	90
00:00:01.710	DTMF	9	80	-1.88	85	00:00:55.630	MF	9	80	-1.87	11
00:00:01.870	DTMF	0	80	-1.88	94	00:00:55.790	MF	5	80	-1.87	90
00:00:02.030	DTMF	8	80	-1.90	85	00:00:55.950	MF	2	80	-1.89	70
00:00:02.190	DTMF	5	80	-1.85	77	00:00:56.110	MF	1	80	-1.86	70
00:00:02.350	DTMF	2	80	-1.87	69	00:00:56.270	MF	4	80	-1.86	70
00:00:02.510	DTMF	1	80	-1.89	69	00:00:56.430	MF	5	80	-1.87	90
00:00:02.670	DTMF	4	80	-1.87	77	00:00:56.590	MF	5	80	-1.87	90
00:00:02.830	DTMF	7	80	-1.87	85	00:00:56.750	MF	5	80	-1.87	90
00:00:02.990	DTMF	5	80	-1.85	77	00:00:56.910	MF	5	80	-1.87	90
00:00:03.150	DTMF	5	80	-1.85	77	00:00:57.070	MF	KP	80	-1.86	11
00:00:03.310	DTMF	8	80	-1.90	85	00:00:57.230	MF	7	80	-1.87	70
00:00:03.470	DTMF	3	80	-1.85	69	00:00:57.390	MF	4	80	-1.86	70
00:00:03.630	DTMF	6	80	-1.87	77	00:00:57.550	MF	4	80	-1.86	70

Figure 226: Digits Only

All Events: If this option is checked then all the events are displayed.

TimeStamp	Type	Event	On	Power	Freq
00:00:00.000	IDLE		430	0.00	
00:00:00.430	DTMF	1	80	-1.89	69
00:00:00.510	IDLE		80	0.00	
00:00:00.590	DTMF	2	80	-1.87	69
00:00:00.670	IDLE		80	0.00	
00:00:00.750	DTMF	3	80	-1.85	69
00:00:00.830	IDLE		80	0.00	
00:00:00.910	DTMF	4	80	-1.87	77
00:00:00.990	IDLE		80	0.00	
00:00:01.070	DTMF	5	80	-1.85	77
00:00:01.150	IDLE		80	0.00	
00:00:01.230	DTMF	6	80	-1.87	77
00:00:01.310	IDLE		80	0.00	
00:00:01.390	DTMF	7	80	-1.87	85
00:00:01.470	IDLE		80	0.00	
00:00:01.550	DTMF	8	80	-1.90	85
00:00:01.630	IDLE		80	0.00	
00:00:01.710	DTMF	9	80	-1.88	85
00:00:01.790	IDLE		80	0.00	
00:00:01.870	DTMF	0	80	-1.88	94
00:00:01.950	IDLE		80	0.00	

TimeStamp	Type	Event	On	Power	Freq
00:00:00.000	IDLE		54350	0.00	
00:00:54.350	MF	1	80	-1.86	70
00:00:54.430	IDLE		80	0.00	
00:00:54.510	MF	2	80	-1.89	70
00:00:54.590	IDLE		80	0.00	
00:00:54.670	MF	3	80	-1.87	90
00:00:54.750	IDLE		80	0.00	
00:00:54.830	MF	4	80	-1.86	70
00:00:54.910	IDLE		80	0.00	
00:00:54.990	MF	5	80	-1.87	90
00:00:55.070	IDLE		80	0.00	
00:00:55.150	MF	6	80	-1.87	11
00:00:55.230	IDLE		80	0.00	
00:00:55.310	MF	7	80	-1.87	70
00:00:55.390	IDLE		80	0.00	
00:00:55.470	MF	8	80	-1.88	90
00:00:55.550	IDLE		80	0.00	
00:00:55.630	MF	9	80	-1.87	11
00:00:55.710	IDLE		80	0.00	
00:00:55.790	MF	5	80	-1.87	90
00:00:55.870	IDLE		80	0.00	

Figure 227: All Events

Export to File: If this option is checked, you can export the Inband Events to a text file to the specified location as shown in the figure below:

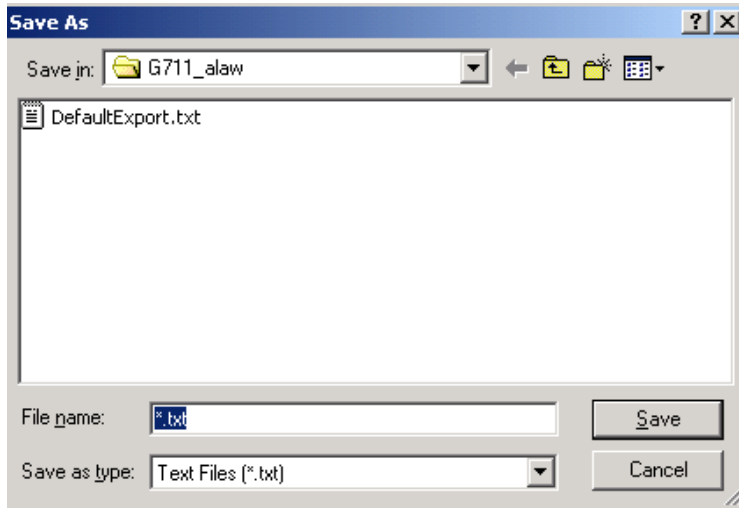


Figure 228: Export to File

Options: If this option is clicked, it opens the Inband Events Options Dialog. For more information please refer to [Inband Options](#).

13.4.7 RTP Events (Outband Events)

RTP Events tab displays all Out band RTP events defined as per RFC 2833 or RFC 4733 as shown in the figure below. By default PacketScan™ displays outband events as per RFC 2833. To set PacketScan™ to detect outband events as per RFC 4733, customize the INI file as explained in this section - [INI Decode Options](#)

- **Timestamp:** Captures time Stamp
- **Event:** Events as per RFC 2833 (i.e. DF, MF, and Line Events)
- **Volume (db):** Power of the event
- **Duration (ms):** Duration of the Event

TimeStamp	Event	Volume [-dB]	Duration (ms)
10:55:10.000888	DTMF 1	10	260
10:55:11.000268	DTMF 2	10	220
10:55:11.000716	DTMF 3	10	240
10:55:12.000267	DTMF 4	10	300
10:55:12.000636	DTMF 5	10	240
10:55:13.000007	DTMF 6	10	260
10:55:13.000707	DTMF 7	10	300
10:55:14.000056	DTMF 8	10	240
10:55:14.000416	DTMF 9	10	240
10:55:14.000953	DTMF 0	10	360

Navigation: MOS Graph | Quality Factors | Inband Events | **RTP Events** | Wave Graph

Figure 229: RTP Events Screen

13.4.8 Wave Graph

The amplitude of the incoming signal in a selected call is displayed in real-time graphic form as a function of time. This application is of use in visually assessing any activity on the traffic such as noise, tone, speech, etc. The data may be displayed in either linear or raw (compressed) format. Time Base in seconds can be set, so that that X axis scale is set according to the selected time base and the user can have a comprehensive view on the wave graph.

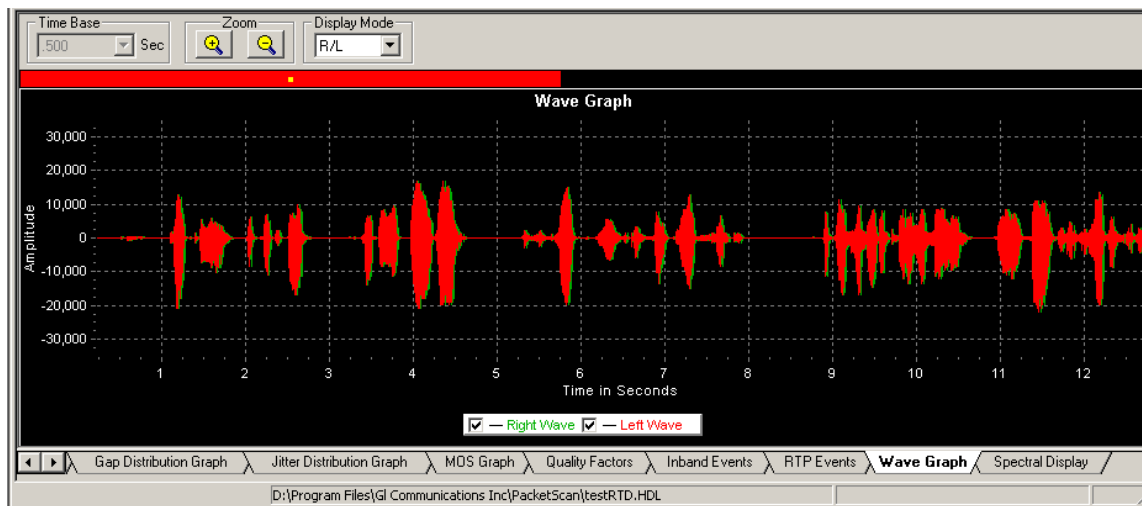


Figure 230: Wave Graph

Wave graph has got three options in display mode:

- **Left\Right (L/R)** – left traffic overlaps right
- **Right\Left (R/L)** – right traffic overlaps left
- **Separate** – left and right traffic are displayed in separate wave graphs

Offline Analysis

The traffic captured pertaining to a call can be analyzed in offline using Offline. When the Call is terminated or a stored file is opened the application starts to build the Wave Graph for Analysis giving the message 'Preparing for Offline Analysis, Please Wait' as shown in the figure below. Once it is finished then we can analyze the traffic captured moving the tab. The graph can be zoomed in and out to look at different Time Base.

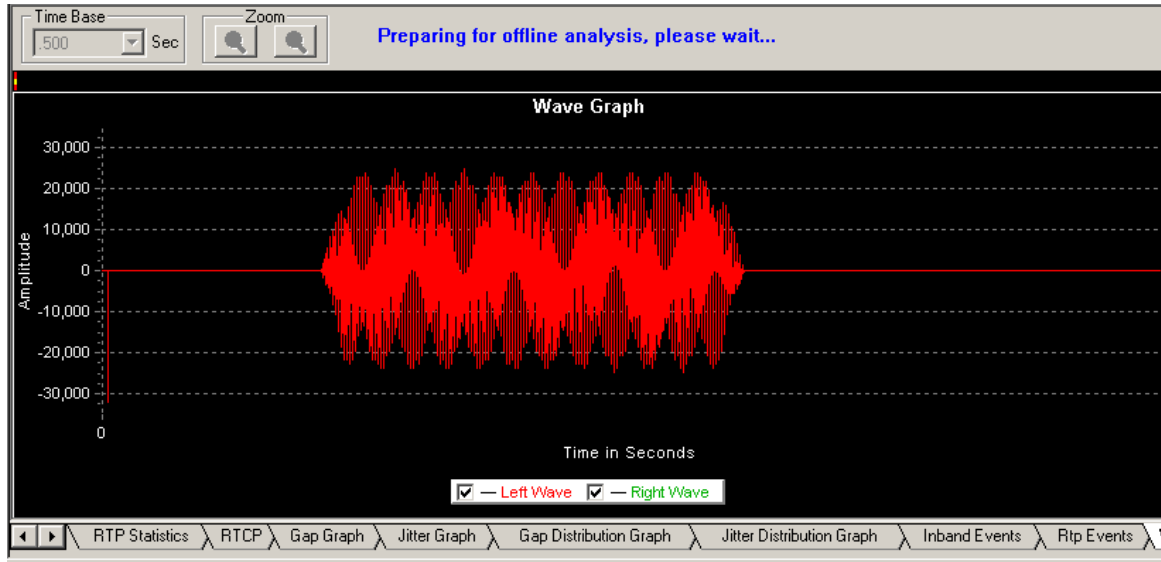


Figure 231: Offline Analysis

13.4.9 Spectral Display

It shows the power of incoming signal while the capturing is going on as a function of frequency. The Power of the Signal can be viewed with different sampling rates and functions. Readings of Power and frequency of data that is flowing in both the directions can be viewed simultaneously in the Spectral display. Also the user has a facility to observe the Spectral graph of data flowing in only one direction.

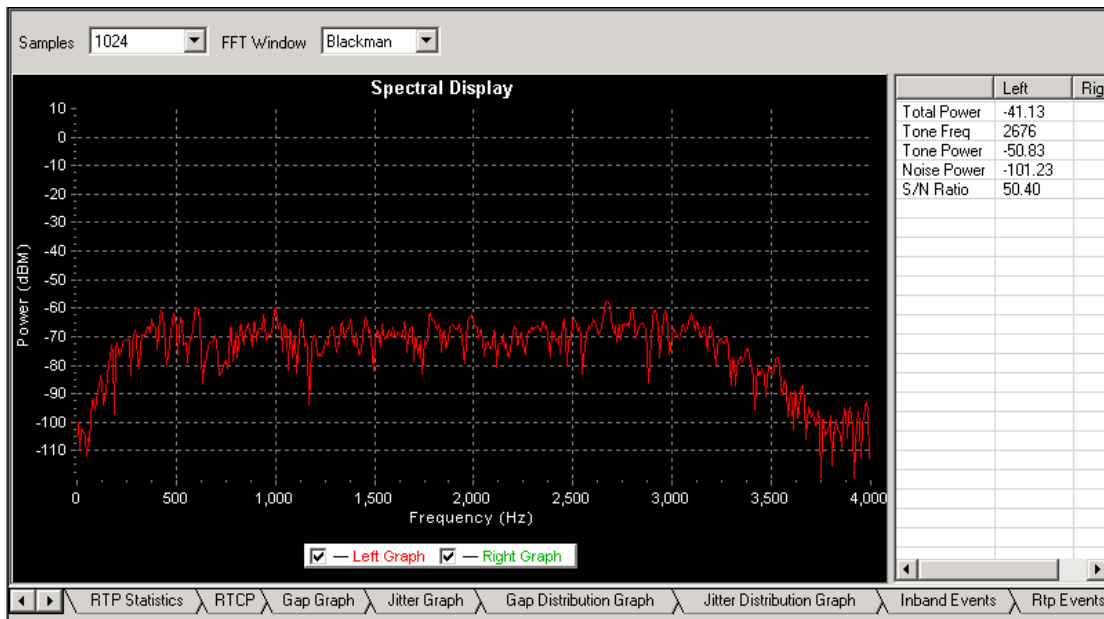


Figure 232: Spectral Display

13.4.10 R-Factor Statistics

This displays the R-Factor statistics for the selected RTP session.

13.4.10.1 Quality Metrics based on E-model

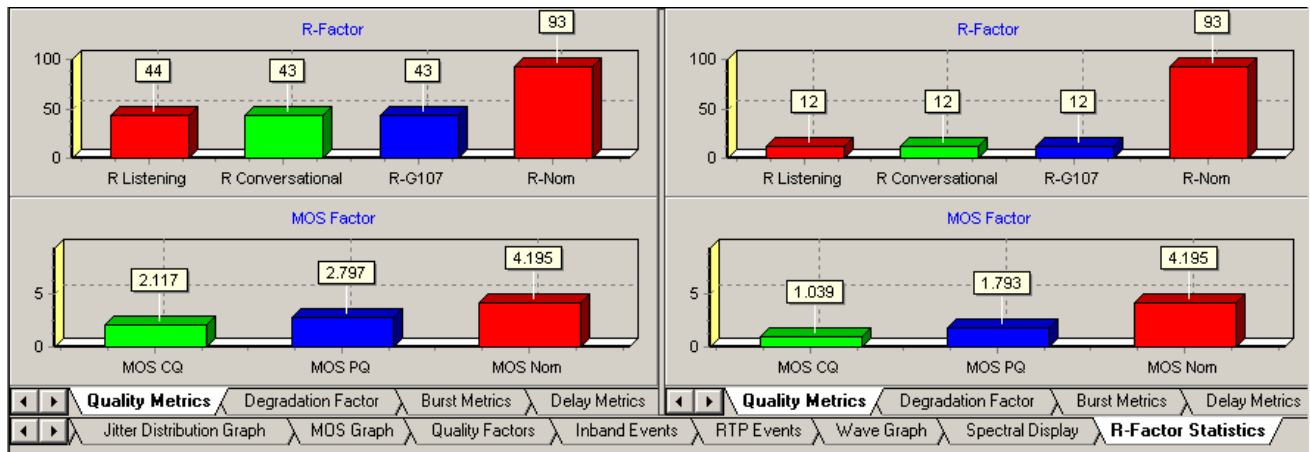


Figure 233: Quality Metrics

This displays two graphs, one for R-Factor and the other for MOS Factor for both the RTP sessions.

- **R-Factor** graph will display statistics such as R Listening, R Conversational, R-G107, and R-Nominal values.
- **MOS Factor** graph will display current statistics such as MOS CQ, MOS PQ, and MOS Nominal values during a call.

Estimating Speech Quality of Packets

The PacketScan™ MOS call quality reporting is based on the Telchemy VQMon/SA application that reports call quality estimates including Listening and Conversational Quality MOS scores - MOS-LQ, MOS-CQ, and Listening and Conversational Quality R factors - R-LQ, R-CQ. Estimates are based on the ITU G.107 E Model which was based on a transmission planning tool developed and using opinion models in ETSI (technical report ETR 250). These models considered the entire Ear-Mouth path and all relevant conditions such as end-to-end level, echo, side tone, and frequency characteristics of the various path segments.

The E Model uses a computational method that includes factors such as noise, signal level, loudness ratings, impairments, delay, codec type, and even network type to derive a quality score. Over time and based on experience with subjective and objective measurements, the E Model's R-Factor score was mapped to an equivalent Mean Opinion Score (Excellent to Bad). Scoring includes consideration for the type of subjective test used for scoring. Passive/listening or active/conversational tests produce slightly different scores.

For IP networks, the score assumes ideal conditions outside the IP cloud and bases the scores on the relevant IP impairments such as packet loss, latency, jitter, and even when these impairments occur over the duration of the call.

Codec Name	MOS-LQ	MOS-CQ	MOS-PQ	R-LQ	R-CQ	VQMon-Nom MOS	VQMon-Nom R factor
G.711 μ-law	4.2	4.18	4.45	93	92	4.2	93
G.711 A-law	4.2	4.18	4.45	93	92	4.2	93
G722	3.91	3.91		96	95	3.91	96
G722.1 (32 K)	4.04	4.01		100	99	4.09	102
G722.1 (24 K)	3.91	3.91		96	95	3.98	98
G.729A/G.729AB	3.91	3.88	3.8	82	81	3.91	82
GSM-FR	3.57	3.53	3.63	73	72	3.57	73

GSM EFR (6.60k)	4.16	4.16	4.16	91	91	4.16	91
GSM HR	3.53	3.53	3.53	72	72	3.53	72
G.726-40k	4.16	4.14	4.13	91	90	4.16	91
G.726-32k	4.04	4.01	3.89	86	85	4.04	86
G.726-24k	3.35	3.3	3.52	68	67	3.35	68
G.726-16k	2.82	2.77	3.2	57	56	2.82	57
G.726-40k with VAD	4.16	4.14	4.13	91	90	4.16	91
G.726-32k with VAD	4.04	4.01	3.89	86	85	4.04	86
G.726-24k with VAD	3.35	3.3	3.52	68	67	3.35	68
G.726-16k with VAD	2.82	2.77	3.2	57	56	2.82	57
AMR NB 7.95k	3.69	3.65	3.7	76	75	3.69	76
AMR WB (23.85k)	4.18	4.18	4.18	107	107	4.18	107
EVRC	3.94	3.94		83	83	3.94	83
EVRCB	3.98	3.98		84	84	3.98	84
SMV	3.61	3.57		74	73	3.88	81
Speex WB	4.14	4.16		106	105	4.16	106
Speex NB	4.14	4.16		91	90	4.16	91
iLBC 13.3k	3.88	3.84	3.79	81	80	3.88	81
iLBC 15.2k	3.95	3.91	3.82	83	82	3.95	83

- **G.711**

PCM has been the standard for digital voice transmission in telephony since 1972. 8 bit compressed pulse code modulation (PCM) samples at 8000 samples/second with 8 bits per sample. (64 kbit/sec) The two algorithms defined in the standard are μ -law (North America & Japan) and A-law (used in Europe and the rest of the world). Both are logarithmic, but A-law was specifically designed to be simpler for a computer to process.

- **G.729**

Annex A and Annex B Voice encoding using CS-ACELP (Conjugate-Structure Algebraic Code Excited Linear Prediction) 8 kbps, is the lowest bit rate ITU-T standard with toll quality. Frame size is 10ms with a 5ms look ahead. Annex A is a low-complexity version of the G.729 standard. Annex B defines VAD/CNG/DTX (Voice Activity Detection/Comfort Noise Generator/Discontinuous Transmission) for G.729 and G.729A.

- **GSM-FR**

GSM-FR is a Full Rate speech coder standardized by the European Telecommunications Standards Institute (ETSI) for compressing toll quality speech (8000 samples / second). and was the first digital speech coding standard used in GSM digital mobile phone systems. The coder has a bit rate of 13 kbps. This coder uses the principle of Regular Pulse Excitation-Long Term Prediction-Linear Predictive coding. The coder works on a frame of 160 speech samples (20 msec), and no look ahead is required. So the algorithmic delay for the coder is 20 msec.

- **GSM EFR**

GSM-EFR (6.60) is an improved and hence the Extended version of GSM-FR(6.10) codec. With sampling frequency of 8000 samples/sec and frame size of 31 bytes/20 msec it achieves the bit rate of 12.2kbps. Codec supports Voice Activity Detection (VAD) to allow saving of bandwidth.

- **GSM HR**

GSM HR 6.20 operates with sampling frequency of 8000 samples/sec. This codec outputs the frames of size 14 Bytes at every 20msec which puts the bit rate of encoder at 5.6kbps. Codec supports Voice Activity Detection (VAD) to allow saving of bandwidth.

- **G.726**

ADPCM (Adaptive Differential Pulse Code Modulation) - Originally a half-rate alternative to ITU-T G.711 and includes both the G.721 and G.723 standards. G.726 compresses by converting between linear, A-law (used in Europe) or μ -law (used in the U.S and Japan) PCM and 40, 32, 24 or 16 kbps.

- **G.726 with VAD**

This is an [ITU-T](#) Adaptive differential pulse code modulation (ADPCM) voice codec, which transmits at bit rates of 16, 24, 32, and 40 kbps. It supports Voice Activity detection and generates SID packets during Silence Period. ADPCM provides the following functionality:

- Voice mail recording and playback, which is a requirement for Internet voice mail.
- Voice transport for cellular, wireless, and cable markets.
- High voice quality voice transport at 32 kbps.

- **AMR NB**

AMR is the 3GPP mandatory standard codec for narrowband speech and multimedia messaging services over GSM and evolved GSM (WCDMA, GPRS and EDGE) networks. It is designed to provide transcoder free connectivity between GSM, US-TDMA and Personal Digital Cellular networks (Japan).

AMR operates at eight bit rates in the range of 4.75 to 12.2 kbps and was specifically designed to improve link robustness.

- **EVRC**

For EVRC codec type three rates are provided (1/8, 1/2 and 1). Default 1/8 and 1 are selected as the minimum rate & maximum rate. Minimum rate should be less than or equal to maximum rate. There is option to select RTP packet format between Header Free Format and Bundled Format. By default Bundled Format is set.

- **EVRCB**

For EVRCB codec type four rates are provided (1/8, 1/4, 1/2, and 1). Minimum rate should be less than or equal to maximum rate. By default 1/8 and 1 are selected as the minimum rate & maximum rate. There is option to select RTP packet format between Header Free Format and Bundled Format. By default Bundled Format is set.

- **SMV**

For SMV codec type, there are four modes supported (Premium mode, Standard mode, Economy mode and Capacity Saving mode).

**Note:**

SMV supports only one stream (session) at a time. Either you can do transmission or reception at a time but not both.

- **Speex WB**

This Codec has a sampling rate of 16000 samples/sec, which makes it a wide band codec. This codec supports different codec options such as Sampling Rate, Variable Bit Rate, Voice Activity Detection and Perceptual Enhancement.

- **Speex NB**

Based on CELP Narrowband (8 kHz), Open source codec targeted for VoIP and file-based applications

- **iLBC Codec**

iLBC (internet Low Bit rate Codec) is a narrow band speech codec that operates at either 13.33 kbit/s with an encoding frame length of 30 ms and 15.20 kbps with an encoding length of 20 ms. Companies that are using iLBC in their commercial products include:

- **Applications/Soft phones:** Skype, Nortel, Webex, Hotsip, Marratech, Gatelinx, K-Phone, XTen
- **IP Phones:** WorldGate, Grandstream, Pingtel
- **Chip:** Audiocodes, TI Telogy, Lead Tek, Mindspeed

The 13.33 kbps rate 30ms frame encodes packets of 399 bits, (50 bytes) and is designated in RTP Toolbox as iLBC_13_33.

The 15.2 kbps 20 ms frame creates packets of 303 bits, (38 bytes). This is labeled iLBC in RTP Toolbox. The basic quality is higher than G.729A.


Note:

R factor statistics now supports more codecs, namely, Mulaw, Alaw, G726 (40 kbps), G726 (32 kbps), G726 (24 kbps), G726 (16 kbps), G726 (40 kbps, 32 kbps, 24 kbps, 16 kbps) with VAD, GSM610, G729, G729B, AMR, iLBC (20 msec), iLBC (30 msec), SPEEX EVRC, EVRCB, and SMV.

MOS and R Factor

Mean Opinion Scores (MOS) are calculated using the ITU-T G.107 E-Model to determine the transmission-rating factor (R-Factor). MOS is based on Absolute Category Rating (ACR) subjective testing. Test results give G.711 PCM an MOS score of 4.1 to 4.4. Those of use who have conducted subjective tests know that some people hate everything i.e. no matter how ideal the circuit otherwise some subjects will score it 'good' instead of 'excellent'. PESQ measurements will give 4.4 -4.5. The R-Factor is based on objective Toll quality circuit parameters and the score ranges from 0 to 93. Companies developing software prefer the MOS method to report as that is the most understandable and accepted around the world.

Some Definitions

R-Factor	Quality score based on various end point and network parameters. Includes codecs, packet loss, and delay.
Conversational R-Factor	The voice quality metric that measures voice quality based on transmission delay, burst packet loss, and burst loss recency.
Listening R-Factor	The voice quality metric based only on burst packet loss and codec selection.
MOS-LQ	Mean Opinion Score based on listening quality. Does not consider recency or delay. ITU-T P.862 Listening Quality implementations.
MOS-CQ	Mean Opinion Score based on conversational quality. Includes recency and delay effects.
MOS-PQ	ITU-T P.862 normalized raw quality score.
MOS-Nom	Nominal quality or maximum score for the codec selected. Similar to the G.107 E-model defaults
Recency	A time factor used to weight scores based on the time from a burst packet loss to the end of the call or next packet loss event.

13.4.10.2 Degradation Factor

The pie chart plots and compares different statistics such as Good Quality, Packets discarded, Echo level, Packet loss, and Regency against total Packets for each individual sessions. All are displayed in terms of percentage as shown in the figure below.

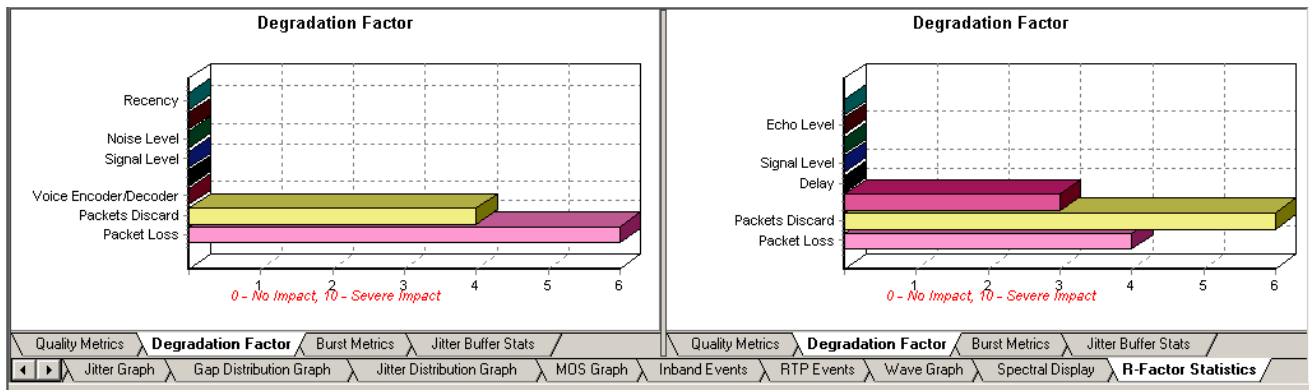


Figure 234: Degradation Factor

13.4.10.3 Burst Metrics

This dialog displays the following statistics.

- Burst R
- Burst Count
- Average Burst Loss Rate
- Average Burst Packet Count
- Average Burst Length
- Gap R
- Average Gap Loss Rate
- Average Gap Packet Count
- Average Gap Length

Burst R	47	Burst R	37
Burst Count	1	Burst Count	44
Burst Loss Rate Proportion	0.33 %	Burst Loss Rate Proportion	0.26 %
Avg Burst Packet Count	12535	Avg Burst Packet Count	88
Avg Burst Length	250700	Avg Burst Length	1783
Gap R	93	Gap R	94
Gap Loss Rate Proportion	0.00 %	Gap Loss Rate Proportion	0.00 %
Avg Gap Packet Count	2	Avg Gap Packet Count	20
Avg Gap Length	40 msec	Avg Gap Length	402 msec

Figure 235: Burst Metrics

13.4.10.4 Jitter Buffer Stats

This dialog will display a pie chart indicating number of packets received, discarded and lost. It also displays the following statistics:

- Total Packets (Received + Discarded + Lost)
- Packets Received
- Packets Discarded
- Packets Lost
- Packet Delay Variation
- Maximum Packet Delay Variation
- Average Mean Packet Delay Variation
- Maximum Average Mean Packet Delay Variation

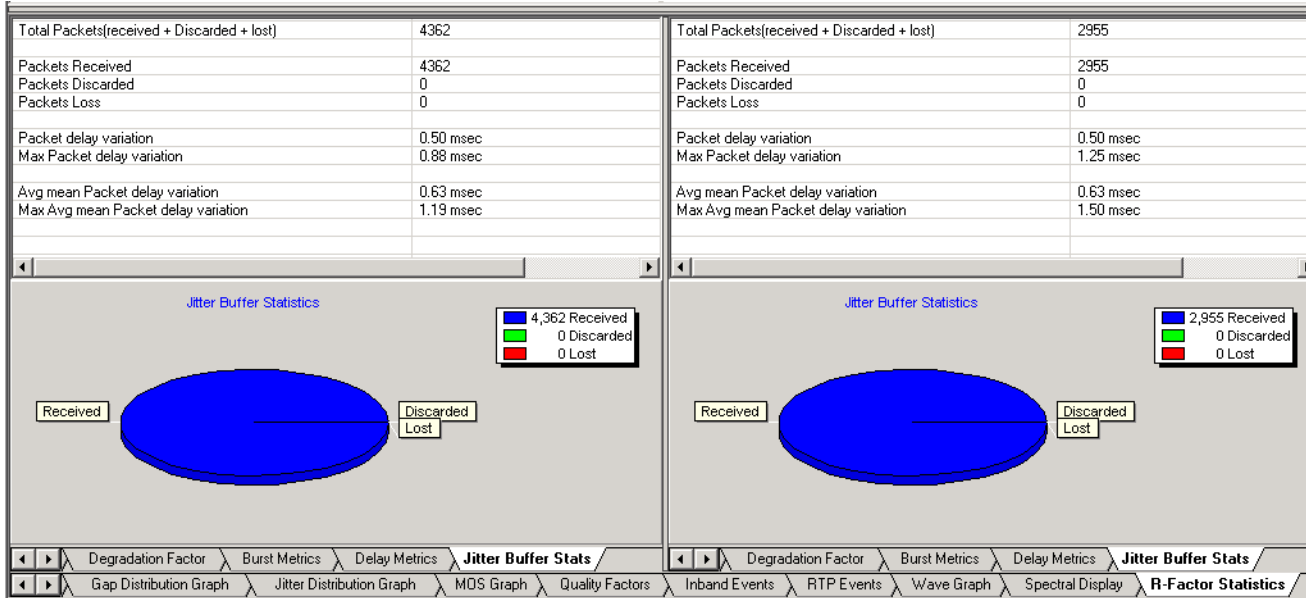



Figure 236: Jitter Buffer Stats

13.5 File Menu Options

13.5.1 Export Displayed Summary

The Export option allows user to save the call records and statistics to a comma-separated (comma-delimited) file. The exported summary can be imported into a database or spreadsheet for post processing.

To open the Export Displayed Summary screen:

- Select **File > Export Displayed Summary** from the main menu as shown in the figure below or
- Click  from the toolbar

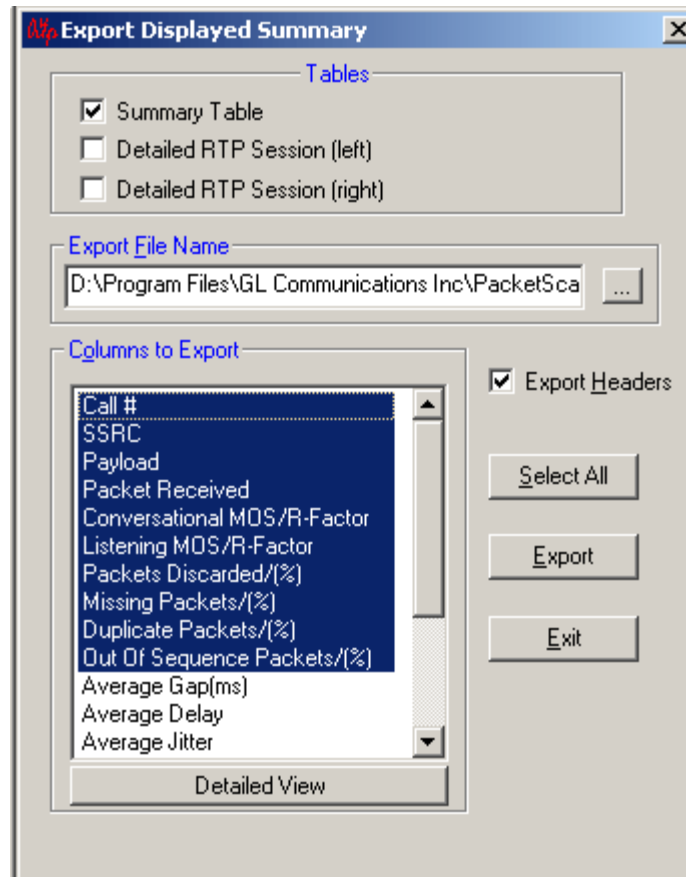


Figure 237: Export Displayed Summary

The Tables option in the Export Displayed Summary screen, allows the user to select values from the three tables.


- Summary Table
- Detail RTP Session (left)
- Detail RTP Session (Right)

Summary Table

The Summary table is selected and exported to a text file which can be viewed in MS Excel

Detail RTP Session (Left)

The Detail RTP session is selected and exported to a text file, which can be viewed in MS Excel

Export File Name option is where the user types in the filename (with full path), where the user wants to save the comma-separated file. Click  to export the file to a particular location in the directory.

The Columns to Export shows the columns that can be exported, corresponding to the table selected. User can select All/Any one/Some columns for exporting.

Selecting (check) **Export Headers**, option selects the names of the headers that are selected by the user. These names will appear once at the top of the comma-separated file.

Select All button is a short cut that selects all the columns with one click.

Clicking the **Export** button starts the actual process of writing the columns to the comma-separated file. A status at the bottom indicating that the application is busy exporting is indicated by the Exporting status message that appears at the bottom.

Click **Exit** to close the screen.

The **Export** option can be invoked both in Online and Offline mode. In online mode, the most recent values collected will be exported. The fact that the comma-separated file can be opened in spreadsheet etc will allow for easier and more powerful search/find techniques to be used on the gathered data.

13.5.2 Export Terminated Calls

This feature is applicable only in **PDA Summary View**. For more details on this, refer to [Export Terminated Calls](#).


13.6 View Menu Options

13.6.1 Find


The Find option is used to search for a particular item from the three tables, One in Summary View and the other two in Detail View. For more details, refer to the section [Find](#) in Summary View.

13.6.2 Call Summary View

In order to go back to Call Summary View

- Select **View > Call Summary View** from the main menu or
- Click  Call Summary/Detail View to switch to Summary View

13.6.3 Go To Analyzer

- Select **View > Go To Analyzer** from the main menu to open the VPA screen or
- Click **GoTo Analyzer**  from the toolbar

13.7 Detail View Menu Options

13.7.1 Save Call

The Save Call feature enables the user to save a particular call either in GL's proprietary *.HDL file format or in Ethereal *.PCAP file format. Call Summary details could also be saved for a particular call and this will be saved as a *.rtf file. This is especially useful to get data from real-time traffic locations to the lab for detail analysis of a flawed call. By using this option, user can save the call that needs to be analyzed as a HDL file and transport it using temporary media to the lab for detail analysis. The whole call with all the SIP and RTP / RTCP packets that are part of the call are saved under the new filename. For more information, refer to section [Save Call](#).

13.7.2 Reports


This option provides the ability to generate PDA detail report of selected or all calls in PDF file format. For more information, refer to section Reports [Generation](#).

13.7.3 Play Audio

The Play Audio plays the selected call to the PC speaker. A host of options are provided to the user before the actual play is started.

Before starting to play the Audio to the Sound Card, user can make a few basic selections. Refer to section [Play Audio](#).

13.7.4 Write To File

Write to file is similar to the 'Play Audio' option the basic difference being that the output is written to a file instead of the Sound Card. Various options are provided so that the user can save the file in a required format, and use the files with voice quality analysis software to investigate more about the quality of voice in the network. Select **Detail View > Write to File > Start** menu item or the corresponding tool button shown  to invoke Write to file dialog.

For a call selected in Summary View, the application allows users to write to a single file if Mix option is selected in Write to File dialog. Two different files for left and right session will be written to a file, if Separate option is selected in Write to file dialog. If user selects either left or right session in a summary view, only single file will be written pertaining to the selected session irrespective of Mix or Separate option selected.

When user selects a Call /Session to be written to a file, a window appears from which user can select the output format, locations, number of files etc. The various options are provided to the user.

For more details, refer to section [Write to File](#) explained in Summary View.

13.7.5 Inband Options

Select this option to open the screen as shown below:

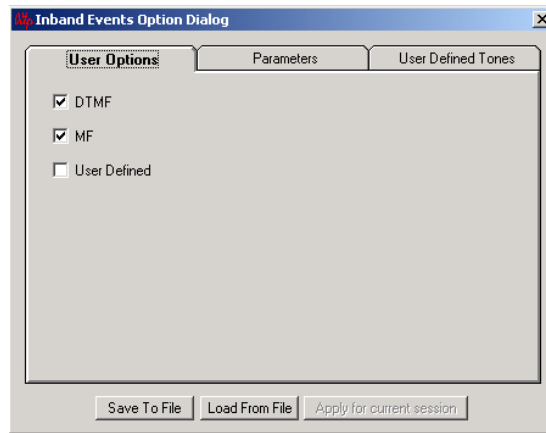


Figure 238: User Options

13.7.5.1 User Options

Select the DTMF and MF check boxes in order to detect the digits. Select User Defined Tones for detecting User-defined Tones.

- Click **Save To File** in order to save the settings to a file in a particular location
- Click **Load From File** to open a saved file

Click **Apply** for current session to save the settings for that particular session only.



Note:

Before selecting the **User Defined Tones** check box, values must be set under **User Defined Tones** tab.

13.7.5.2 Parameters

Select the **Parameters** tab to open the screen as shown in the figure below:

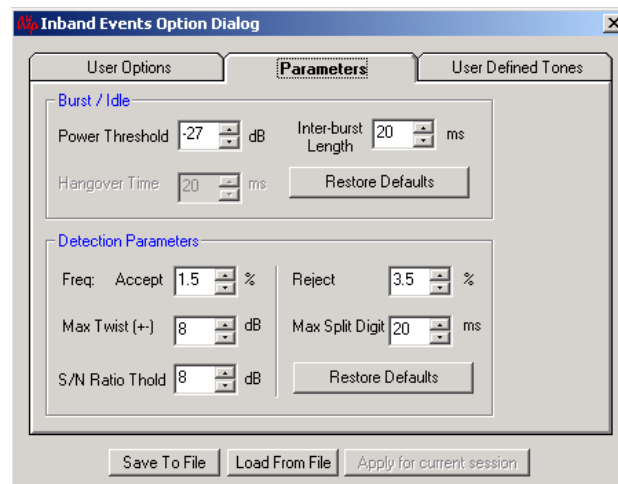


Figure 239: Parameters

Select the Power Threshold and Inter-burst Length values using the spin box as per the requirements. Click Restore Defaults in order to get the default values. Similarly, set the values under the Detection Parameters pane as required else restore the default settings.

Click **Save To File** so that the settings are saved in a particular location.

Click **Load From File** to open a particular setting.

13.7.5.3 User Defined Tones

Select **User Defined Tones** tab to open the screen as shown below:

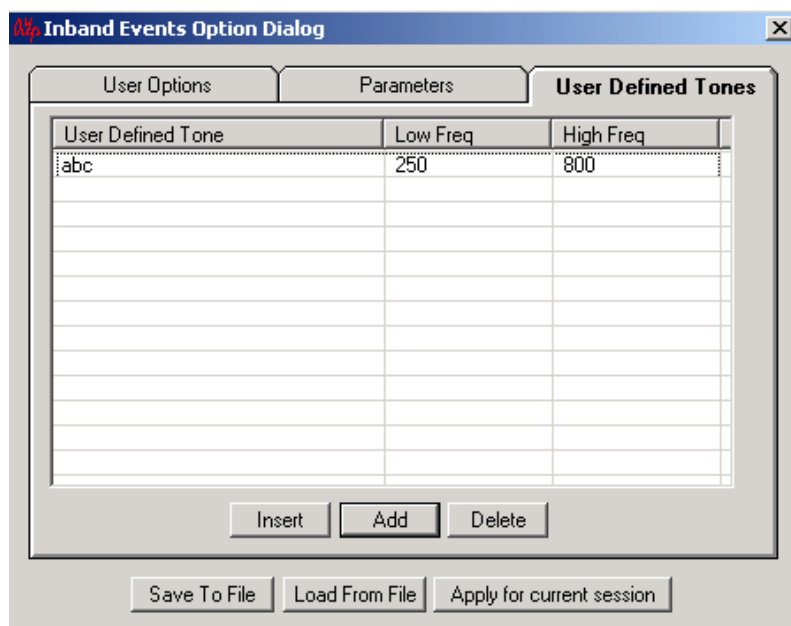


Figure 240: User Defined Tones

User can give the name to a particular frequency using this option. The event will be identified in the Event column by the specified name.

- Click **Add** to define a new tone
- Click **Insert** to insert a row wherever required
- Click **Delete** to remove a particular defined row
- Click **Save To File** in order to save the settings to a file in a particular location
- Click **Load From File** to open a saved file
- Click **Apply for current session** to save the settings for that particular session only

13.8 Additional Settings

This includes E-model parameters, VQMon Jitter Buffer Emulator settings and Dynamic Payload type selection dialogs. For more details on these, refer to [Additional Settings](#) in Summary View.

Section 14.0 Packet Data Analysis – Registration Summary

Note: This feature is applicable only for SIP calls.

14.1 Overview

SIP offers a discovery capability. If a user wants to initiate a session with another user, SIP must discover the current host(s) at which the destination user is reachable.

The proxy servers perform the job of finding out the exact location of the recipient. Every user registers its current location to a REGISTRAR server. The application sends a message called REGISTER informing the server of its present location. The Registrar stores this binding (between the user and its present address) in a location server which is used by other proxies to locate the user.

The registration summary interface displays the SIP registration information in a tabular format which includes user agent, registrar, registered time, status, TTL based, expiry time, remaining time, and RRD (Registration Request Delay) for each user agent. In addition, it displays the registration statistics, active registration graph of the entire registration summary and provides the trace display of each registration.

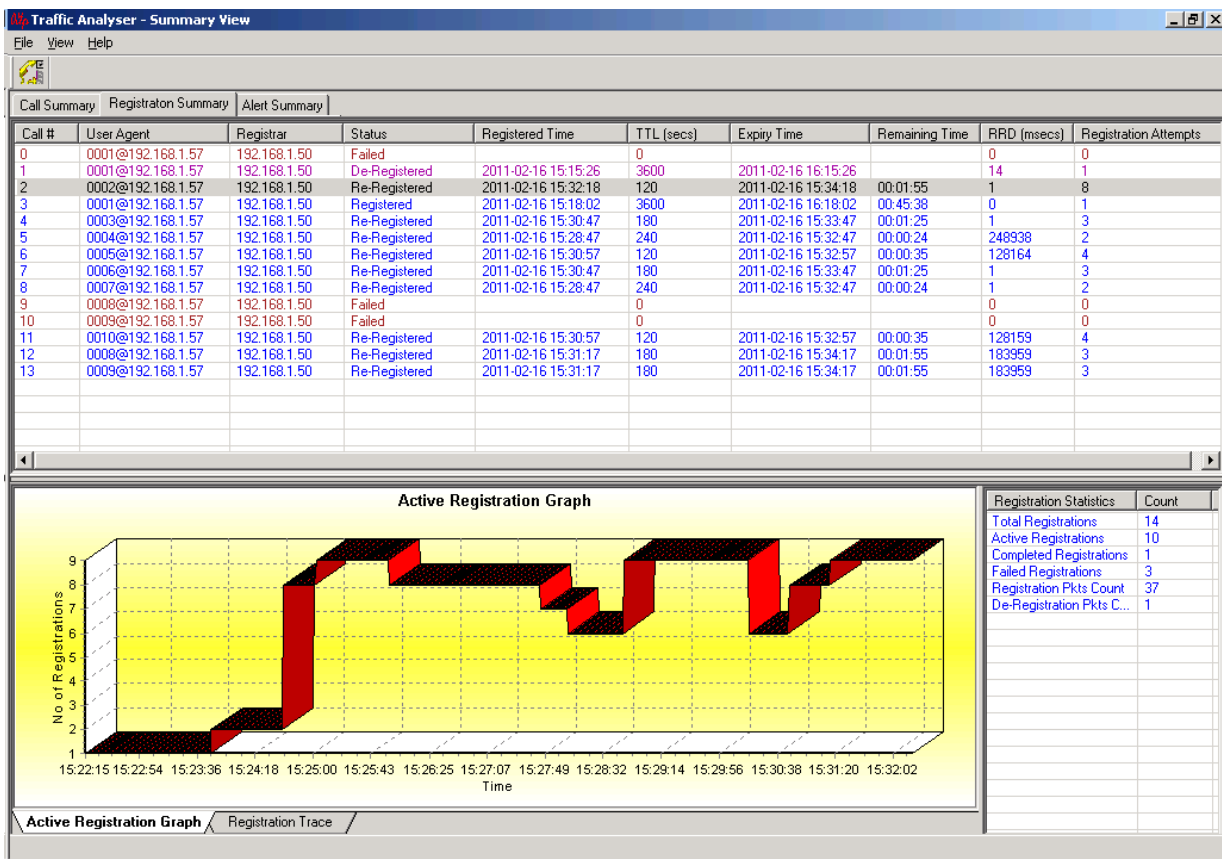


Figure 241: Registration Summary

14.2 Registration Summary

Registration Summary View can be divided into three main parts.

- Registration Summary Information
- Registration Statistics
- Graphs

Registration Summary Information: As the name indicates, it gives a summary of all the registrations that are processed by PacketScan™.

Registration summary displays the following information in tabular format from left to right as shown in the figure below:

Call #: Call # represents the unique call id allocated to this call.

User Agent: Displays the URL of each user agent that request for SIP registration with the registrar. Normally, it would be displayed in the format UserAgent@HostIPAddress.

Registrar: Displays the domain of the location service to which the user agent initiates the SIP registration request.

Status: Displays the status of the SIP registration. The various statuses may include Registered, Expired, De-Registered, Re-Registered, and etc.

Registered Time: Indicates the time at which the SIP registration has occurred.

Time-To-Live (TTL (secs)): Indicates the valid duration of the SIP registration.

Expiry Time: Indicates the time period at which the current registration expires. (It is calculated with reference to the registered time and the TTL).

Remaining Time: Indicates the remaining time of valid SIP registration. This is displayed only during real-time analysis.

RRD (Registration Request Delay – msecs): RRD is a delay measured in response to a UAC REGISTER request. RRD shall be measured and reported only for successful REGISTER requests, The RRD is calculated using the following formula; **RRD = Time of Final Response - Time of REGISTER Request.** Hence, this column displays the calculated RRD value in msecs.

Registration Attempts: this metric is calculated for all Registrations and is displayed in Registration Summary column. For successful registration, the initial Registration Attempt value will be 1. For successful re-registration of the same UA, the value increments and state changes to Re-Registered.

Call #	User Agent	Registrar	Status	Registered Time	TTL (secs)	Expiry Time	Remaining Time	RRD (msecs)	Registration Attempts
0	0001@192.168.1.57	192.168.1.50	Failed		0			0	0
1	0001@192.168.1.57	192.168.1.50	De-Registered	2011-02-16 15:15:26	3600	2011-02-16 16:15:26		14	1
2	0002@192.168.1.57	192.168.1.50	Re-Registered	2011-02-16 15:25:56	120	2011-02-16 15:27:56	00:00:03	1	5
3	0001@192.168.1.57	192.168.1.50	Registered	2011-02-16 15:18:02	3600	2011-02-16 16:18:02	00:50:08	0	1
4	0003@192.168.1.57	192.168.1.50	Re-Registered	2011-02-16 15:27:46	180	2011-02-16 15:30:46	00:02:54	1	2
5	0004@192.168.1.57	192.168.1.50	Registered	2011-02-16 15:24:38	240	2011-02-16 15:28:38	00:00:45	0	1
6	0005@192.168.1.57	192.168.1.50	Re-Registered	2011-02-16 15:26:46	120	2011-02-16 15:28:46	00:00:53	128164	2
7	0006@192.168.1.57	192.168.1.50	Re-Registered	2011-02-16 15:27:46	180	2011-02-16 15:30:46	00:02:54	1	2
8	0007@192.168.1.57	192.168.1.50	Registered	2011-02-16 15:24:38	240	2011-02-16 15:28:38	00:00:45	1	1
9	0008@192.168.1.57	192.168.1.50	Failed		0			0	0
10	0009@192.168.1.57	192.168.1.50	Failed		0			0	0
11	0010@192.168.1.57	192.168.1.50	Re-Registered	2011-02-16 15:26:46	120	2011-02-16 15:28:46	00:00:53	128159	2
12	0008@192.168.1.57	192.168.1.50	Registered	2011-02-16 15:25:03	180	2011-02-16 15:28:03	00:00:09	0	1
13	0009@192.168.1.57	192.168.1.50	Registered	2011-02-16 15:25:03	180	2011-02-16 15:28:03	00:00:09	0	1

Figure 242: Summary Columns

14.3 Registration Filters

This option allows the user to filter the registration summary based on certain criteria as shown below.

Call #	User Agent	Registrar	Status	Registered Time	TTL (secs)	Expiry Time	Remaining Time
0	0001@192.168.1.115	192.168.1.190	Registered				
1	0002@192.168.1.115	192.168.1.190	Re-Registered	2011-01-03 18:35:33	120	2011-01-03 18:37:33	
2	0001@192.168.1.115	192.168.1.190	De-Registered	2011-01-03 18:32:01	120	2011-01-03 18:34:01	
3	0001@192.168.1.115	192.168.1.190	Registered	2011-01-03 18:33:59	120	2011-01-03 18:35:59	

Figure 243: Registrations

- **Show All Registrations:** Displays all the registrations that are traced
- **Show Active Registrations:** Displays only active registrations
- **Show Completed Registrations:** Displays only completed registrations
- **Show Failed Registrations:** Displays only failed and timed-out registrations.
- **Show User Defined Registrations:** Displays only filtered registrations (based on Triggers & Action Settings).

14.4 Registration Statistics

The registration statistics display the count of the registration details as shown in the figure below:

Registration Statistics	Count
Total Registrations	20
Active Registrations	10
Completed Registrations	10
Failed Registrations	0
Registration Pkts Count	20
De-Registration Pkts Count	10

Figure 244: Counter Type

Total Registrations is the total number of SIP registrations requests processed by RRA. It includes all successful and failed SIP registrations.

Active Registrations is a count of total SIP registrations that are presently active.

Completed Registrations is a count of total SIP registrations that are completed.

Failed Registrations is a count of total SIP registrations that have failed and timed-out. This counter is updated for all the failure reasons.

Registration Packets Count is the total number of SIP registration request messages.

De-Registration Packets Count is the total number of De-Registration request messages.

14.5 Graphs

Graphs related to the registration traces selected are displayed at the bottom of the registration summary. The different graphs available in the registration summary are:

- Active Registration Graph
- Registration Trace

14.5.1 Active Registration Graph

The Active Registration Graph is a simple line graph, depicting the Number Of Active Registration Vs Time. A sample (Active registration count) is taken at every 30 seconds.

Functions Invoked By Right Click:

When right-clicked on the graph you get the options to Print the graph, Save the graph, and alternate between 2D/3D views as shown in the figure below:

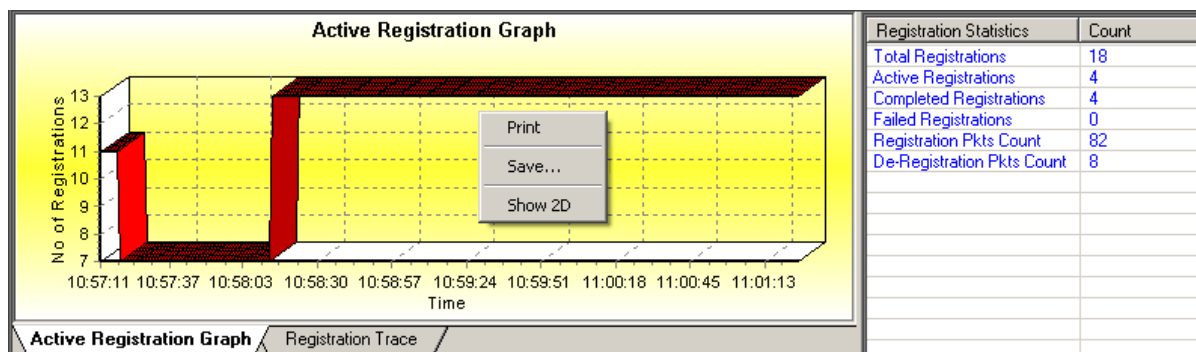


Figure 245: Active Registration Graph

14.5.2 Registration Trace

The Registration Trace displays the message sequence of registered calls. Message sequence pictorially displays the messages exchanged for a particular scenario between a user agent and the registrar. For

example, in the following figure, the registration message between two IP entities shows that, the registration request is placed from User agent (192.168.1.223) to the registrar (192.168.1.231). User can also view the decoded message by selecting a message displayed in the graph.

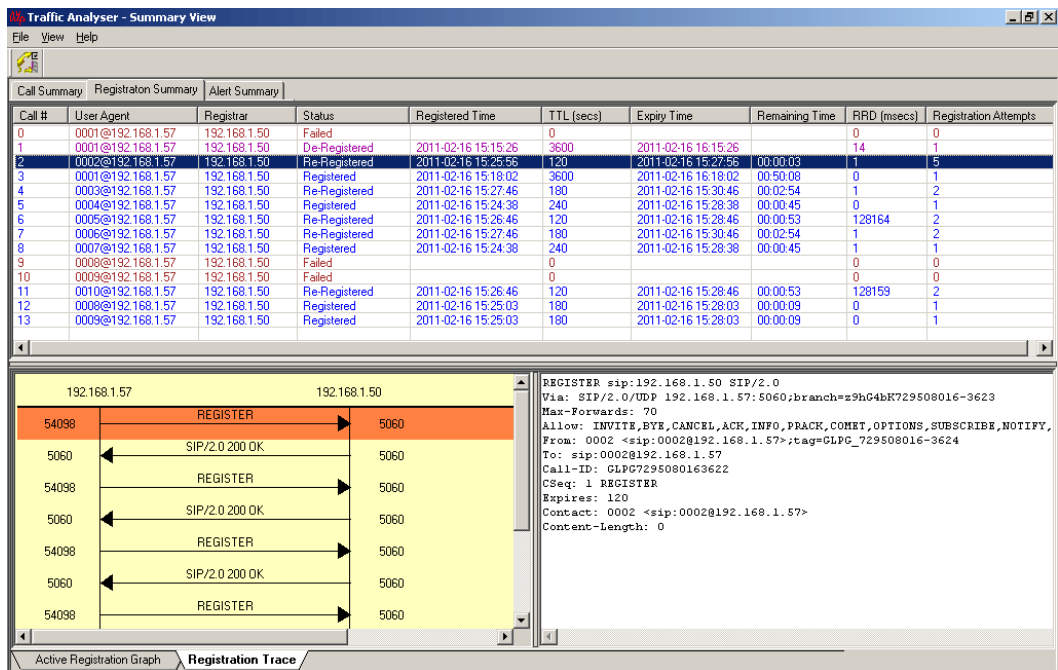


Figure 246: Registration Trace Ladder Diagram

Appendix A: Glossary of Protocol Fields

- **Card number (one relative)** – This field displays the device number on which the data is being captured.
- **Time** – This field displays the time as configured by the user in **View > Time Format**. For more information refer to [Time Display Formats](#).
- **Frame Length(s)** - This field displays the length of each captured frame.
- **Error** – This field displays various error messages during capturing /decoding such as Frame error, Decode error, FCS error, and so on.
- **Error Frames Only** - Select Error Frames Only displays all the error frames.
- **OK Frames Only** - OK Frames Only displays all frames that are error free.
- **Frame Number(s)** - This represents the unique number assigned to each frame in the order it was captured
- **Device Number** - Device Number displays all frames having the specified device number.
- **VLAN ID**- VLAN ID is the identification number of 12 bits that can allow the identification of $(2^{12} - 2)$ VLANs.
- **Ethernet Encoded TPID**- TPID has a defined value of 8100 in hex. When a frame has the Ether type equal to 8100, this frame carries the tag IEEE 802.1Q / 802.
- **Higher Layer Protocol**- Higher Layer Protocol displays all frames in the specified layer such as IP, ARP, etc
- **IP Packet Type** – This field displays the type of packet captured such as SIP, MEGACO, RTP or RTCP etc.
- **PPP Over Ethernet** - PPP over Ethernet (PPPoE) connects a network of hosts (clients) over a simple bridging access device to a Remote Access Concentrator (server), allowing each host to utilize it's own PPP stack.
- **PPPoE Ether Type** - The PPPoE Ether Type is set to either Discovery Stage (0x8863) or PPP Session Stage (0x8864).
- **PPPoE TLV Tag** - The PPPoE contains zero or more TLV (type-length-value) tags. Select all or required TLV Tag to filter out the frames with specific TLV tags as shown in the figure below and click Activate button to apply the settings.
- **IPv4 Source IP Address** - This is the address of a source node that uniquely identifies the source computer while participating in LAN/WAN communication.
- **IPv4 Destination IP Address** - This is the address of a destination node that uniquely identifies the source computer while participating in LAN/WAN communication.
- **IPv6 Source IP Address** - This is the address of a source node that uniquely identifies the source computer while participating in LAN/WAN communication.
- **IPv6 Destination IP Address** - This is the address of a destination node that uniquely identifies the source computer while participating in LAN/WAN communication.
- **Packet Type** - This identifies the type of packet received. Supported packet types over MAC layer are H225, H245, MEGACO, MGCP, RAS, RTCP, RTP, and SIP.
- **NSAP Operation** – This field displays the NSAP messages such as request, response, get nearest server request and get nearest server response. Select the **NSAP Operation Value** to display the frames with specific NSAP type messages.
- **STP Message** – This is the protocol identifier field. Select the protocol type to display the frames for the specific protocols.
- **CLNP Message** – This is the network layer protocol identifier field.
- **RIEP Message** – This field is a type code that displays the ESIS RIEP messages such as End System Hello (ESH), Intermediate System Hello (ISH) and Redirect (RD). The RIEP Message Value displays the specific frames with RIEP messages.
- **COTP Message** – This field is a Transport Protocol Data Unit code that displays the COTP messages like reject, data, connection request, connection confirm and so on. This is a TPDU (Transport Protocol Data Unit) code. The COTP Message Value display specific frames with COTP messages.
- **CLTP Message** - This is a TPDU (Transport Protocol Data Unit) code. The CLTP Message Value display specific frames with CLTP messages.

- **TCP Source Port** – This is a 16-bit unsigned port number assigned to the sending application called TCP source port.
- **TCP Destination Port** – This is a 16-bit unsigned port number assigned to the receiving application called TCP destination port.
- **UDP Source Port** - The source port is the virtual 16-bit port number assigned by the local computer when it transmits data to a remote machine. This is typically a number above 1023.
- **UDP Destination Port** - The destination port is also a 16-bit port number, usually a 'well known port number' such as 69 for trivial file transfer protocol, or 53 for DNS.
- **GRE IP** - The Generic Routing Encapsulation (GRE) is a tunneling protocol that provides a mechanism for encapsulating arbitrary packets within an arbitrary transport protocol. GRE IP uses IP as the payload protocol, where in GRE packets are encapsulated within IP. This field displays the type of GRE IP Packet captured like SIP, MEGACO, RTP or RTCP etc.
- **Source IP Address:** This is the address of a source node that uniquely identifies the source computer while participating in LAN/WAN communication.
- **Destination IP Address-** This is the address of a destination node that uniquely identifies the source computer while participating in LAN/WAN communication.
- **Function Type** – The Function Type Value display specific frames with WiMAX function type.
- **WiMax Function Type** – This field displays WiMAX function type such as Authentication Relay, Context Delivery, Data Path Control and so on.
- **EIGRP (Enhanced Interior Gateway Routing Protocol) Packet Type Opcode** – This field displays the opcode value of the EIGRP packet. The opcode can be Acknowledge, Hello, IPX SAP, Query, Reply, and Update.
- **RSVP Class** - This field displays the RSVP class such as CHALLENGE object, ADSPEC object, EXPLICIT ROUTE object, ERROR SPEC object, etc. RSVP class identifies the object class.
- **RSVP Message Type** - Select all or required RSVP message types to filter out the frames with specific RSVP messages such as Hello Message, Path Message, and more as shown in the figure below.
- **PIM UDP Source Port** - The source port is the virtual 16-bit port number assigned by the local computer when it transmits data to a remote machine. This is typically a number above 1023.
- **PIM UDP Destination Port** - The destination port is also a 16-bit port number, usually a 'well known port number' such as 69 for trivial file transfer protocol, or 53 for DNS. When used with a source port, this allows a remote machine to recognize a data connection.
- **PIM TCP Source Port** – This is a 16-bit unsigned port number assigned to the sending application called TCP source port.
- **PIM TCP Destination Port** – This is a 16-bit unsigned port number assigned to the receiving application called TCP destination port. Select TCP Source Port option and enter the port value (say 4050) to filter the frames through this port of sending application.
- **ICMP Type** - The ICMP Type field is used to identify the type of message.
- **IGMP (Internet Group Management Protocol) Layer** - The IGMP is used by IP hosts to report their host group memberships to any immediately neighboring multicast routers. IGMP is a integral part of IP.
- **IGMP Message Type** - This field displays the message type of IGMP protocol. The message type can be Membership Query, Version1, Version3, Version 4 Membership Report, and Version 2 Leave Group. This identifies the IGMP message types.
- **Message Type** – This gives the Message type of H323, as like Method type in SIP. The messages may be SETUP, CONNECT, ALERTING etc.
- **DNS Layer (Domain Name System)** - DNS is used mostly to translate between domain names and IP addresses, and to control email delivery.
- **DNS Query Name** - This field displays the Query name for DNS operation. It might be any URL of a Website like www.gl.com. Recursive, iterative and reverse are the query types in the DNS.
- **STUN Layer (Simple Traversal of User Datagram Protocol through Network Address Translators)** - STUN is a request-response protocol. There are two requests, Binding Request, and Shared Secret Request. The response to a Binding Request can either be the Binding Response or Binding Error Response. The response to a Shared Secret Request can either be a Shared Secret Response or a Shared Secret Error Response.
- **STUN Message Type** - Select Message Type as shown in the figure below to filter the frames with specific STUN message type. Click Activate button to apply the settings.

- **DHCP (Dynamic Host Configuration Protocol)** - The Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP.
- **DHCP Message Type** - This field displays Dynamic Host Configuration Protocol (DHCP) an Internet protocol for automating the configuration of computers that use TCP/IP. For more details refer RFC 2131.
- **SMTP (Simple Message Transfer Protocol) Layer** - SMTP is mail transfer protocols that transport the mail reliably and efficiently via Internet. When a SMTP client has a message to transmit, it opens a duplex connection with the server and transfers the message using IP/TCP.
- **SMTP From** - This field indicates the reverse path or whom the mail is from. For details refer RFC 821.
- **SMTP Message** - This field indicates the SMTP command like MAIL, RTCP etc. For details refer RFC 821.
- **SMTP To** - This field indicates the forward path or whom the mail is from. For details refer RFC 821.
- **POP3 Message (Post Office Protocol- Version 3) Layer** - Post Office Protocol- Version 3 is the mail retrieving protocol used by the client to retrieve the mails from the server. Initially, the server host starts the POP3 service by listening on TCP port 110. When a client host wishes to make use of the service, it establishes a TCP connection with the server host. When the connection is established, the POP3 server sends a greeting. The client and POP3 server then exchange commands and responses until the connection is closed. This field displays the Post Office protocol messages. For details refer RFC 1939.
- **HTTP Message (Hyper Text Transmission Protocol)** - HTTP (Hyper Text Transmission Protocol) is application protocol for distributed, collaborative, hypermedia information systems and involves MIME like communication between user agent (UA) and origin server identified by URI. Select the HTTP message and enter the value accordingly to filter the frames.
- **FTP Message (File Transfer Protocol)** - It defines a set of commands and replies exchanged between the two users over control connection. A separate full duplex data connection is opened between the two communicating user for actual data transfer.
- **LDP Message Type (Label Distribution Protocol)** - LDP is used to exchange label mapping information between two LSRs (Label Switched Routers) known as LDP peers over an LDP session between them.
- **SIP 3261 Layer** - Session Initiation Protocol is an application layer control protocol that can create, maintain, and tear down multi-media sessions.
- **SIP Method** - This field displays SIP method captured like INVITE, ACK. For details refer RFC 3261.
- **SIP From** - This field displays the URL of User Agent, present in From Header of SIP message.
- **SIP To** - This field displays the URL of User Agent, present in To Header of SIP message.
- **SIP Call ID** - This field displays Call ID of a SIP call, present in Call Id header of SIP message.
- **SIP Cseq** - This field displays Command Sequence of a SIP message, present in Call Id header of SIP message.
- **Called No** - This displays the destination number.
- **Calling No** - This displays the caller related messages.
- **Trans/ConnRedirr#** - This field represents either called party or call forwarded number.
- **ISUP (ISDN User Part) Layer** - ISDN User Part provides call signaling messages required to establish, maintain & release of SS7 call between SS7 nodes.
- **ISUP Message Type** - Defines various network specific messages of the frame. The message type may be one octet or two octets (for network specific messages).
- **ISUP Called Party Number** - This identifies the destination number, type, and numbering plan [inter-national, etc].
- **ISUP Calling Party Number** - This identifies the source number, type and numbering plan [inter-national, etc].
- **ISUP Transf/ConnRedir/Etc**: This identifies the caller-related messages.
- **ISUP (ISDN User Part) Message Type** - This field displays the ISUP message that indicates the establishment/release of SS7 call and maintenance of the call.
- **H225 Q.931 Call Signaling Layer** - Q.931 is ISDN's Connection Control Protocol, similar to TCP in IP stack. Here, H225 carries Q.931 messages.

- **MAP (Mobile Application Part) Package and Component Type** - MAP is a protocol that enables real-time communication between nodes in a mobile cellular network. It encapsulates package and components types of Transaction Capabilities Application Part (TCAP) messages over a common channel network.
- **MAP Operation and MAP Error (Mobile Application Part (Error and operation))**:- This field displays the processes that are required to invoke a MAP operation at remote node and the corresponding errors that are returned by MAP error.
- **CAP Package and Component**: CAP is a protocol that supports the information flows between CAMEL (Customized Application for Mobile network Enhanced Logic) functional elements. It uses basic TCAP Services and is based on various TCAP package like begin, unidirectional, continue and so on. It also includes various TCAP components such as Invoke the operation, Return the results of an operation i.e success /failure etc.
- **CAP Error**: This field displays a failure code for the invoked CAP operation
- **INAP (Intelligent Network Application Part) Package and Component Type**–INAP is a protocol that enables real-time communication between intelligent network elements. It uses basic TCAP services and is based on various TCAP package like Begin, Unidirectional, continue and so on. It also includes various TCAP components such as Invoke the operation, Return the results of an operation i.e success /failure etc.
- **INAP Operation Code and Error Code** - This field displays a list of INAP operations at remote node and the corresponding errors that are returned.
- **RTCP (Real-time Transport Control Protocol)** - RTP (Real time Transport Protocol) combines its data transport with a RTCP (Real time Transport Control Protocol), which makes it possible to monitor data delivery. RTCP enables the receiver to detect if there is any packet loss and to compensate for any delay jitter.
- **SSRC of Sender** – This field displays the SSRC number of sender of RTP packet.
- **RTP (Real-time Transport Protocol) Layer** - The Real time Transport Protocol layer defines a way for applications to manage the real-time transmission of multimedia data. RTP is used for Internet telephony applications. RTP provides the functionality to manage the data as it arrives to best effect.
- **RTP Payload Type** – This field displays the payload type of Content in RTP packet like G711 Ulaw etc.
- **RTP Sequence #** - This field displays the Sequence number of the RTP packet.
- **RTP SSRC ID** – This field displays the SSRC number of the RTP stream. For details refer RFC 1889.
- **RTP Timestamp** – This field displays the Timestamp of RTP packet.
- **Marker bit** – This field shows whether the RTP packet has Marker Bit set.
- **eGTP Messages** – This field displays GPRS Tunneling Protocol (eGTP) defining IP protocol of the GPRS core network.
- **NAS Messages** – The Non-Access Stratum (NAS) signaling, which runs between the MME and the UE, is used for control-purposes such as network attach, authentication, setting up of bearers, and mobility management. All NAS messages are ciphered and integrity protected by the MME and UE. This field displays Non-Access Stratum (NAS) real-time user traffic in a cell.
- **BSSGP Pdu (Base Station System GPRS Protocol)** – This column shows the BSSGP Pdu type corresponding to BssGp Layer.
- **Tunneling of Messages (TOM)** – It is a generic protocol layer used for the exchange of TOM Protocol Envelopes between the MS and the SGSN
- **GMM Message (GPRS Mobility Management)**: This field displays the signaling messages required to handle the mobility of user, who has packet switched connection with the packet switched core network.
- **GPRS Session Mgmt Message** - This displays the Session Mgmt Message Type values like Activate AA PDP context acc, Activate AA PDP context rej, Activate AA PDP context req etc

Megaco 3525 and Megaco 3015

- **Context Id** – This field indicates the MEGACO Context Id. This is assigned by the Media Gateway and is unique within the scope of the Media Gateway.
- **Termination Id** – This field displays the MEGACO Transaction ID. Transactions are identified by a Transaction ID, which is assigned by the sender and is unique within the scope of the sender.
- **Transaction** – This field indicates the Transaction Type of MEGACO. Commands between the Media Gateway Controller and the Media Gateway are grouped into Transactions.

H.323 Protocol Standard

- **CRV (Call Reference Value1 or 2 octets)** – CRV is a unique value assigned at the beginning of a call to identify each call on the user-network interface.
- **Called #** - These numbers identify destination/called parties.
- **Cause Value** – This identifies the reasons for disconnect or incomplete calls.
- **Location** – This provides the information on type of network, for example, International Network, Private Network, Public Network and so on.
- **Call Reference Flag**- Call reference flag is used to identify which end of the user-network interface originated the call.
- **Calling #** - This column displays “Calling Party Number” depending on IE (Information Element) present in the packet.
- **Channel Number** – This identifies type and number of B-Channel(s) requested.
- **Progress Description** – This indicates the status of the outgoing calls.

(Intentional Blank Page)

Appendix B: Call States

Call States: The call states are internal representation of VPA to peg the different stages of a call. Different color codes are allotted to the calls so that it is easier for the user to identify the state of the calls when they are displayed in the Summary View. The call states and the color codes are as follows:

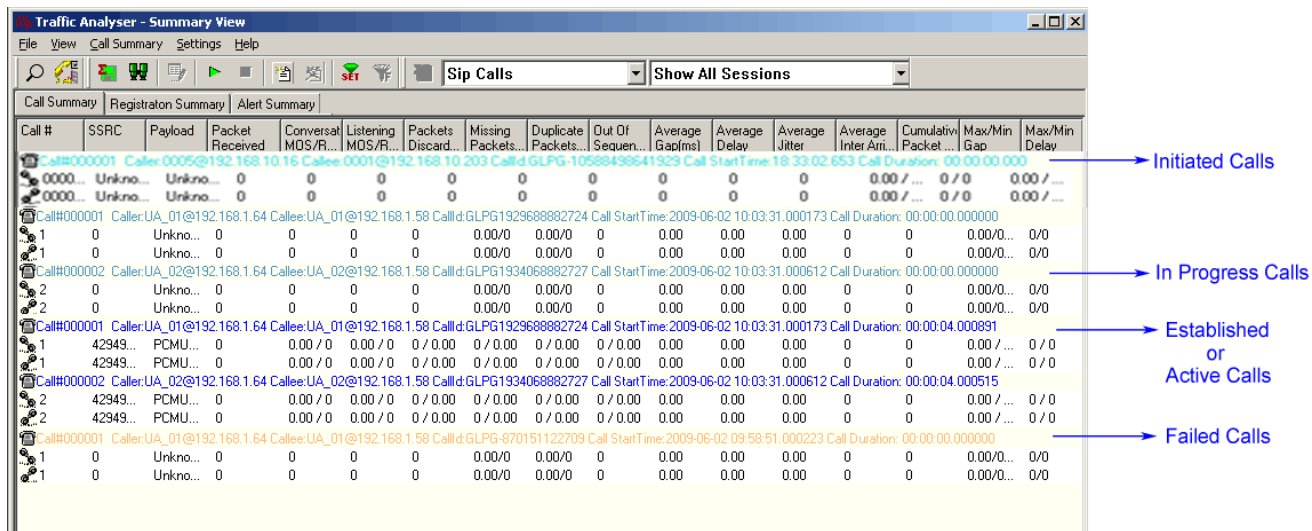


Figure 247: Summary View

Initiated: Once the INVITE message is received, the call is set to 'Call Initiated' state. The display color in this state would be turquoise

In Progress: Once a response to INVITE is received, i.e., 100 TRYING is received the call state changes to 'In Progress'. The display color in this state would be aqua

Established: A call is considered as 'Established', when the '200 OK' message is received by the call originator (as a response to its INVITE message). The display color in this case is blue

Failed: A call is considered as failed if the correct call sequence as prescribed by RFC 3261 (SIP) is not followed at any stage. The display color is gold

Invalid: If a call does not match any of the states described above, it is termed as an invalid state. One example would be that of a 'non SIP supported RTP session'. The display color would be red

Completed: A normal call termination would push the call into a 'Completed' state. This is marked by the 'SIP BYE' message. The display color would be violet.

Call#0000001	1	28555...	PCMU...	2	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0.00	0.00	0	0	0.00 / ...	0 / 0
Call#0000002	2	28626...	PCMU...	3	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0.00	0.00	0	0	0.00 / ...	0 / 0

Active Purged Calls: When the purging starts the color of the active calls is changed to indicating that the calls are getting purged.

Call#0000001	0000...	13782...	G726-40/8000	10097	0	0	0	0	20	0	1	0	0	309.31...	289 / ...	22.70 ...
--------------	---------	----------	--------------	-------	---	---	---	---	----	---	---	---	---	-----------	-----------	-----------

Marker Bit

The 9th bit from the starting of the RTP header is termed as the marker bit. The Marker bit is set to '1', when a RTP stream is resumed after a break in voice traffic. This break/silence could have been inserted deliberately by the sender or because of the Voice Activity Detection software used at the audio – originator. The first RTP packet that indicates the resumption of the RTP packet stream would have its Marker Bit set to '1'. In VPA this is indicated by the alphabet 'M' displayed in the first column of the RTP table in the Detail View

Packet #	Seque...	RTP ...	Payload Ty...	Payl...	Packet Seq...	Gap(ms)	Ga...		Packet #	Seque...	RTP ...	Payload Ty...	Payl...	Packet Seq...	Gap(ms)	Ga...	
M 5	35126	1336...	PCMU/8000	160	Session In ...	0.00	0.00		M 6	41762	1605...	PCMU/8000	160	Session In ...	0.00	0.00	
7	35127	1336...	PCMU/8000	160	Session In ...	19.71	20...		8	41763	1605...	PCMU/8000	160	Session In ...	19.51	20...	
9	35128	1336...	PCMU/8000	160	In Sequence	20.46	20...		10	41764	1605...	PCMU/8000	160	In Sequence	20.50	20...	
11	35129	1336...	PCMU/8000	160	In Sequence	19.60	20...		13	41765	1605...	PCMU/8000	160	In Sequence	20.52	20...	
12	35130	1336...	PCMU/8000	160	In Sequence	19.46	20...		14	41766	1605...	PCMU/8000	160	In Sequence	19.52	20...	
15	35131	1336...	PCMU/8000	160	In Sequence	20.55	20...		16	41767	1605...	PCMU/8000	160	In Sequence	19.53	20...	
17	35132	1336...	PCMU/8000	160	In Sequence	19.52	20...		18	41768	1605...	PCMU/8000	160	In Sequence	20.50	20...	
19	35133	1336...	PCMU/8000	160	In Sequence	21.48	20...		20	41769	1605...	PCMU/8000	160	In Sequence	20.51	20...	
21	35134	1336...	PCMU/8000	160	In Sequence	19.59	20...		22	41770	1605...	PCMU/8000	160	In Sequence	19.55	20...	
23	35135	1336...	PCMU/8000	160	In Sequence	20.44	20...		24	41771	1605...	PCMU/8000	160	In Sequence	19.52	20...	

Figure 248: Marker Bit

Appendix C: SIP Registration States

The registration states are internal representation of PacketScan™ to peg the different stages of a SIP registration. Different color codes are allotted so that it is easier for the user to identify the state of the registration status when they are displayed in the Registration Summary. The registration states and the color codes are as follows:

Call #	User Agent	Registrar	Status	Registered Time	TTL (secs)	Expiry Time	Remaining Time
0	0001@192.168.1.223	192.168.1.231	De-Registered	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
1	0002@192.168.1.223	192.168.1.231	De-Registered	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
2	0003@192.168.1.223	192.168.1.231	De-Registered	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
3	0004@192.168.1.223	192.168.1.231	De-Registered	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
4	0005@192.168.1.223	192.168.1.231	De-Registered	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
5	0006@192.168.1.223	192.168.1.231	Expired	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
6	0007@192.168.1.223	192.168.1.231	Expired	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
7	0008@192.168.1.223	192.168.1.231	Expired	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
8	0009@192.168.1.223	192.168.1.231	Expired	2009-05-19 12:47:22	120	2009-05-19 12:49:22	
9	0010@192.168.1.223	192.168.1.231	Registered	2009-05-19 12:47:22	3600	2009-05-19 13:47:22	00:55:39
10	0011@192.168.1.223	192.168.1.231	Registered	2009-05-19 12:47:22	3600	2009-05-19 13:47:22	00:55:39
11	0012@192.168.1.223	192.168.1.231	Registered	2009-05-19 12:47:22	1800	2009-05-19 13:17:22	00:25:40
12	0013@192.168.1.223	192.168.1.231	Registered	2009-05-19 12:47:22	1800	2009-05-19 13:17:22	00:25:40
13	0014@192.168.1.223	192.168.1.231	Registered	2009-05-19 12:47:22	3600	2009-05-19 13:47:22	00:55:40

Figure 249: Registration Status

Registered: Once the REGISTER message is received, the status is set to Registered state. The display color in this state would be **blue**

De-Registered: The display color in this state would be **violet**.

Expired: A normal registration termination is considered as 'Expired'. The display color in this case is **gold**.

(Intentional Blank Page)

Appendix D: Graphs

□ Summary View Graphs

Summary View graphs are plotted for the entire session. It includes the following –

Active Calls Graph – A line graph, depicting the **Number Of Calls Vs Time**

Average Jitter Distribution - Distribution of the **Average Jitter** values across the **Total Sessions**

E-model - This graph provides R-factor, MOS and packets discarded against number of sessions- all these three graphs show statistics of terminated calls.

- **R-Factor** – A bar Graph that plots **R-Factor** across **No of Sessions**.
- **MOS** – A bar Graph that plots **Mean Opinion Score** across **No. of Sessions**.
- **Packets Discarded** – A bar Graph that plots **Packets Discarded** across **No. of Sessions**.

RTP Packets Graph - Plots and compares out of **ordered packets, missing packets** and **duplicate packets** against **Total Audio Packets**.

T.38 Analysis – Fax (T.38 data) over VoIP monitoring and decoding capability.

Call Graph - displays the message sequence of captured VoIP calls.

□ Detail View Graphs

If both the sessions of the call have been selected then plotting them in the same view enables comparison between them.

Gap graph - Plots the **Gap** (in milliseconds) versus the **packet number**.

Jitter graph - Plots the **Jitter values** versus the **packet number**.

Gap Distribution Graph - Number of packets with a particular value of gap is plotted against the (gap) value.

Jitter Distribution Graph - Number of packets with a particular value of jitter is plotted against the jitter value.

MOS Graph - Plots **Mean Opinion Score** values throughout the duration of the call.

Quality Factor - Plots and compares **Good Quality packets, Packets Discarded**, and **Echo level** against **total Packets** for each individual session.

Wave Graph – Amplitude of the incoming signal in a selected call is displayed in real-time graphic form as a function of time.

Spectral Display - Power of incoming signal while the capturing is going on as a function of frequency.

R-Factor Statistics

Quality Metrics based on E-model - R-Factor and MOS Factor

- **R-Factor** bar graph will display statistics such as R Listening, R Conversational, R-G107, and R-Nominal values.
- **MOS Factor** bar graph will display current values such as MOS CQ, MOS PQ, and MOS Nominal values during a call.

Degradation Factor – A pie chart plots and compares different statistics such as Good Quality, Packets discarded, Echo level, Packet loss, and Regency against total Packets for each individual sessions.

Jitter Buffer Statistics – A pie chart plots and compares packets received, packets discarded and packets lost against total Packets for each individual sessions. Also provides a tabular data on average.

□ Registration Summary Graphs

Active Registration Graph - A line graph, depicting the **Number Of Registrations Vs Time**.

Registration Trace – displays message sequence of registered calls.

(Intentional Blank Page)

Appendix E: Additional Utilities

□ HDL File Conversion Utility

HDL File Conversion Utility converts a file from Ethereal format files (.PCAP, .CAP, and .PCAPNG) to GL proprietary file format (.HDL). The utility can automatically detect the format of the source PCAP file whether it is captured on Linux or Windows® and converts accordingly to HDL file. The HDL files can also be converted to Ethereal formats that is compatible on Windows® and Linux operating systems.

By converting the file to *.HDL format, the users can use the converted *.HDL files in PacketScan™ application to decode and analyze.

Double-click on **HDLFileConversion.exe** from the PacketScan™ installation folder to open the dialog as shown below. To convert Ethernet *PCAP trace files to HDL, configure HDL file conversion utility as shown in the figure below. For more details on the options available in HDL File Conversion Utility, please refer to [HDL File Conversion Utility User's Manual](#).

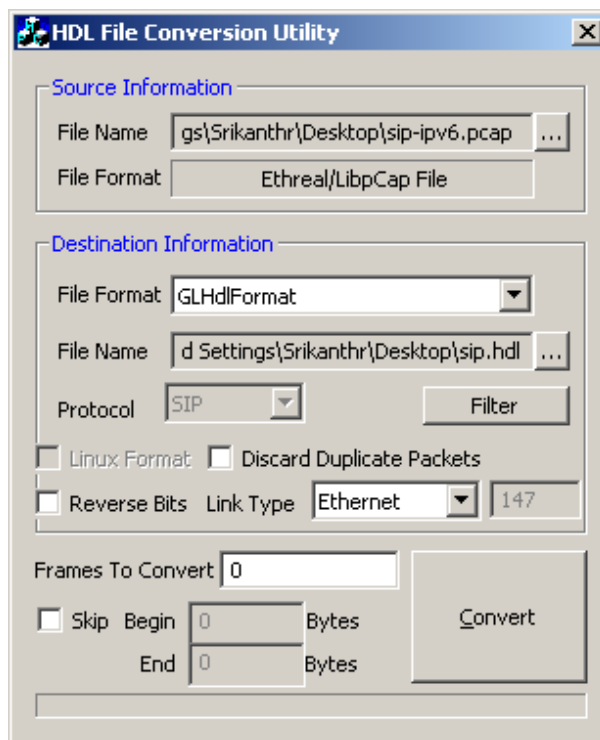


Figure 250: Ethernet PCAP Trace File to HDL

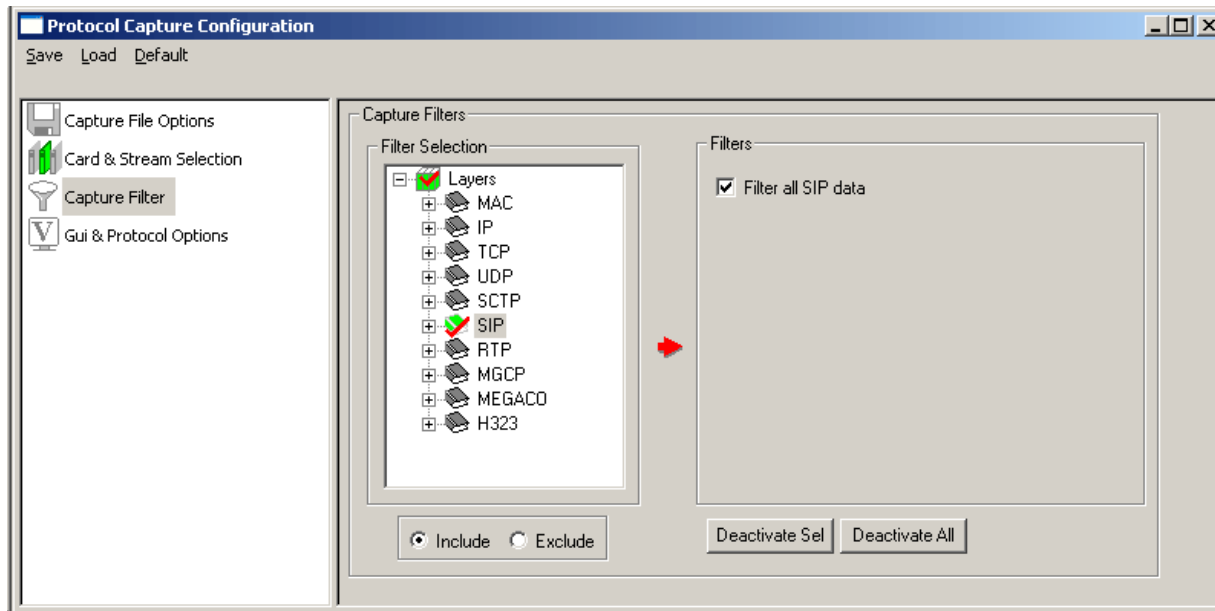
Filtering and Converting the HDL File:

Filter option allows the users to filter the frames of interest while converting from Pcap file to HDL file format.

The user has to set the filter using the Capture Filter option in the PacketScan™ application. Refer to the section Setting Capture Filter to know more on this.

Follow the steps given below to set the filter –

- 1) Open the PacketScan™ application.
- 2) Select the Capture > Capture Filter from the main menu.



- 3) Select the required layer to be filtered. For example, in the above figure SIP layer has been selected.
 - 4) Now, close the Capture Filter dialog and close the PacketScan™ application.
 - 5) Invoke the HDL File Conversion Utility from the installation directory.
 - 6) Now, the filter is applied internally. Select the source file as *.pcap file and destination file as *.hdl file.
 - 7) The destination *.HDL file contains only filtered frames eliminating other frames.
- To remove the applied filter, open PacketScan™ application, uncheck the selected layers, and close the application. Now, invoke the HDL File Conversion Utility and convert from *.PCAP to *.HDL file format. All the frames gets converted to *.HDL without filtering any frames.

Advanced Excel Add-in for Call Detail Record (CDR) Analysis

Using the [Call Detail Record](#) feature, the PacketScan™ can output call details in the form of three Comma Separated Value (CSV) files such as Call Side Record, Call Master Record, and Call Events Record along with the voice file recordings for each direction.

These files are used by GL's [Call Data Records](#) and [Voice Band Application](#) for further processing. CDR application uses the per call data from PacketScan™ and VBA analytics to provide useful call detail records for further analysis using Excel®. The working is depicted in the below picture.

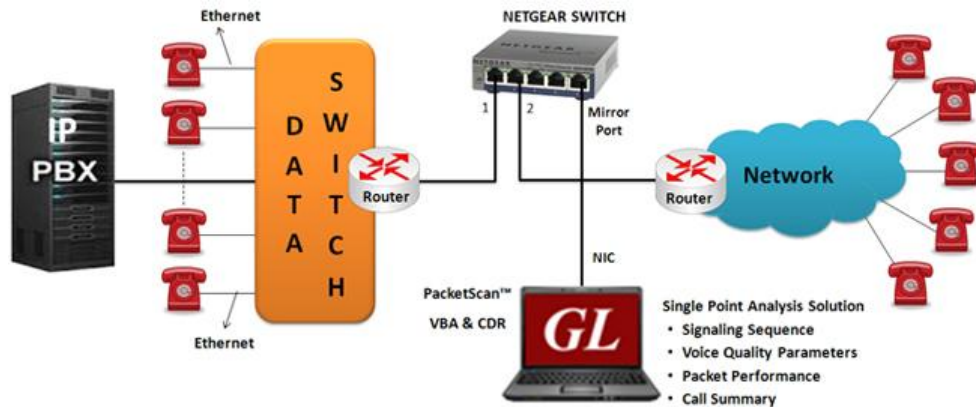


Figure 251: Packet over IP CDR Analysis System

For each call it reports comprehensive information including a complete signaling information for each direction, all alarms and errors, detailed voiceband event information including dual tones (DTMF, MF, MFC-R2), fax tones, modem signals, and more, detailed analysis of the voiceband call including noise level, speech level, speech activity factor, echo measurements, and categorization of the call as voice, fax, modem, or data.

The generated CSV reports from CDR application are analyzed using built in tools included with Excel. The records can be filtered using Advanced Filter in Excel® tool based on signaling, or various measurements to generate reports of "calls of interest". The voice files of these calls can be either downloaded, or played back using Goldwave® or any audio program.

Calls of Interest

Probe ID	Call ID	Side 1	Side 2	Protocol	Start	Released	Durat
VoIPProbe	GLPG-11734837841613	Left	Right	SIP	07-12-2012 15:08:32	07-12-2012 15:08:53	00:00:
VoIPProbe	GLPG-9226557841625	Left	Right	SIP	07-12-2012 15:12:43	07-12-2012 15:13:04	00:00:
VoIPProbe	GLPG-9653117841619	Left	Right	SIP	07-12-2012 15:12:00	07-12-2012 15:12:20	00:00:

Filtered Calls: 3 of 5 Total Calls; Filtering Criteria: Start 07-12-2012 15:08:32 to 07-12-2012 15:12:43

Call Summary Call Side Information Call Events Voiceband Measurements

2

Probe ID: VoIPProbe

Call ID: GLPG-9226557841625

Protocol: SIP

Start Time: 07-12-2012 15:12:43

Release Time: 07-12-2012 15:13:04

Call Duration: 00:00:21

Call Originating Side: Left

Call Terminating Side: Left

Release Code: Normal Call Clearing

Post Dial Delay(PDD): 2

Session Delay(SD): 2

Archive Folder: C:\netpub\ftproot\TestFiles\voicefiles\CSV Files\

Play the Voice Files
(requires the voice file path to have write permissions)

Download and Play the Voice Files

(Enter the folder name only)

Figure 252: SIP CDR Analysis using Excel® Addin

For more information on exporting calls to CSV format and to generate graphs in excel refer to [CDR Excel Quick Start Guide](#).

Advanced Excel Add-in for Reports

PacketScan™ also includes another Excel® addin (**Excel-Dashboard-Tool-IP.xlsm**) to import completed call records (in TXT format) from Packetscan™ into the Microsoft Excel®, workbook. This is available in the PacketScan™ installation directory.

The report files are generated in *.txt (CSV) file format using the [Export Terminated Calls](#) feature in PacketScan™. Imported text files are automatically converted to xls file format, which are then used to generate Pivot table and Pivot charts. Using this Excel® utility, the following graphs can be generated.

- Calls Per Day (CPD)
- Call Duration Per Day (CD)
- Session Disconnect Delay (SDD)
- Post Dial Delay (PDD / SRD)
- Call Failure (CF)
- Minimum Conversational MOS (CMOS)
- Minimum Listening MOS (LMOS)
- Calls Answered/Not
- Avg Packet Loss (PL)
- Avg Delay
- Avg Jitter

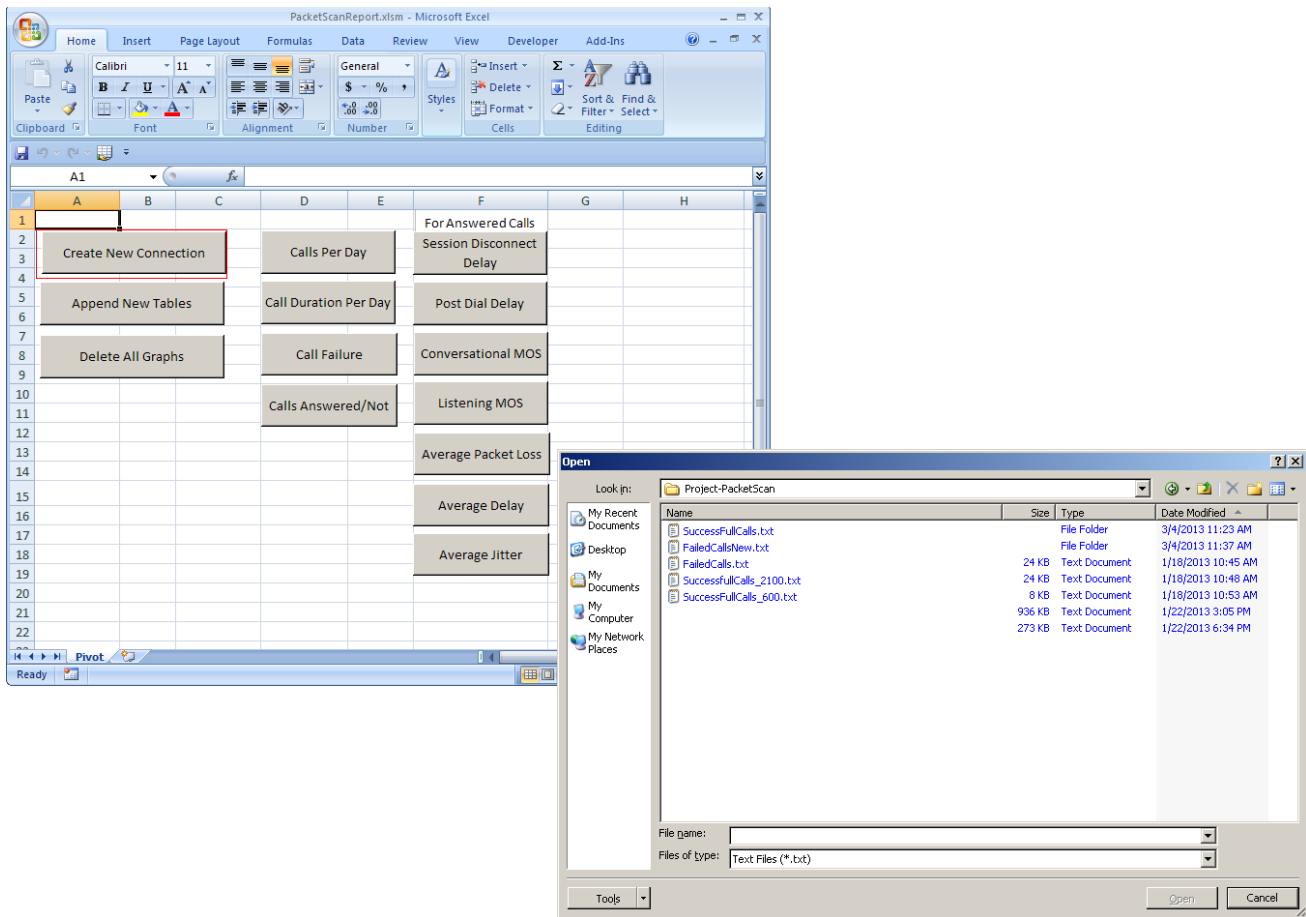


Figure 253: Import PacketScan™ Text (*.txt) Sample Files

- Click on the **Create New Connection** button to import one or more report files (.TXT) into Excel.
- Click on the require graph option from the list to generate the graph
- **For example:** to generate Calls Per Day (CPD) graph click the Calls Per Day option.
- The CPD call details graph is generated and is displayed in CPD tab as seen in the figure below.

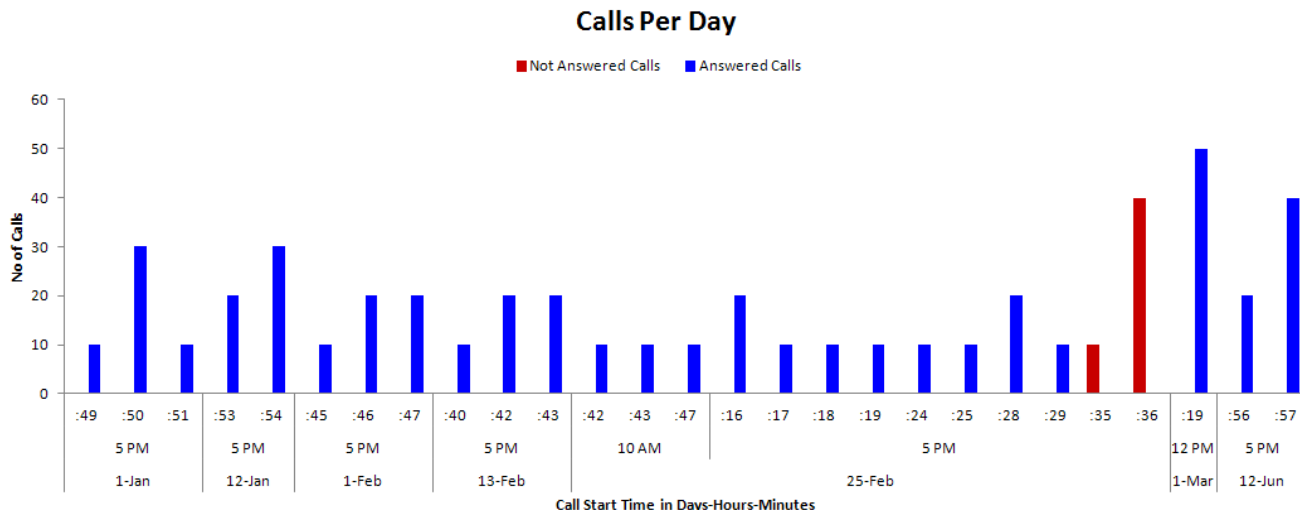


Figure 254: No. of Calls Per Day (CPD) graph

- The Pivot Table for the **No. of Calls Per Day (CPD)** graph is also displayed on to the right- side of the graph.

Call Start Time in			No of Calls		
Days_	Hours_	Minutes_	Not Answered Calls	Answered Calls	Grand Total
1-Jan	5 PM	:49	0	10	10
		:50	0	30	30
		:51	0	10	10
12-Jan	5 PM	:53	0	20	20
		:54	0	30	30
1-Feb	5 PM	:45	0	10	10
		:46	0	20	20
		:47	0	20	20
13-Feb	5 PM	:40	0	10	10
		:42	0	20	20
		:43	0	20	20
25-Feb	10 AM	:42	0	10	10
		:43	0	10	10
		:47	0	10	10
	5 PM	:16	0	20	20
		:17	0	10	10
		:18	0	10	10
		:19	0	10	10
		:24	0	10	10
		:25	0	10	10
		:28	0	20	20
		:29	0	10	10
		:35	10	0	10
		:36	40	0	40
1-Mar	12 PM	:19	0	50	50
12-Jun	5 PM	:56	0	20	20
		:57	0	40	40
Grand Total			50	440	490

Figure 255: Calls per Day Table

For more information on exporting calls to CSV format and to generate graphs in excel refer to [Packetscan Excel Report Quick Start Guide](#).