

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)

Section 1.0 Overview	1
1.1 Introduction	1
1.2 Supported Protocols & Specifications	
1.3 Main Features	
1.4 Pre-requisites	
1.5 VoIP Testing	
Section 2.0 Installation Instructions	
2.1 Installation Procedure	
2.2 Dongle License Installation	
2.3 PacketScan [™] Installation	
2.3.1 WinPcap Installation	
Section 3.0 Getting Started with PacketScan [™]	
Section 4.0 Performing Analysis using PacketScan [™] – an Overview	
4.1 Performing Real-time Analysis	
4.2 Performing Offline Analysis	
4.3 Packet Data Analysis (PDA)	
Section 5.0 File Menu Options	
5.1 Start Real-time	
5.2 Stop (Pause)	
5.3 Open a Trace for Off-line Analysis	
5.4 Close Trace	
5.5 Import	
5.6 Save As and Close	
5.7 Save As	
5.8 Export Details	
5.9 Export Summary Section 6.0 Display Options	
Section by Display Untions	
6.1 Define Views to Display	29
6.1 Define Views to Display 6.2 Summary View	29 30
6.1 Define Views to Display6.2 Summary View6.2.1 Setting a Relative Time	29 30 30
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 	
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 	
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 6.2.6 Define Views 	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 6.2.6 Define Views 6.3 Detail View (Selecting Individual Frame) 	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 6.2.6 Define Views 6.3 Detail View (Selecting Individual Frame)	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 6.2.6 Define Views 6.3 Detail View (Selecting Individual Frame) 6.3.1 Detail View - SIP Capture 6.3.2 Detail View - Megaco Capture 	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 6.2.6 Define Views 6.3 Detail View (Selecting Individual Frame) 6.3.1 Detail View - SIP Capture 6.3.2 Detail View - Megaco Capture 6.3.3 Detail View - H.323 Capture 	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 6.2.6 Define Views 6.3 Detail View (Selecting Individual Frame) 6.3.1 Detail View - SIP Capture 6.3.2 Detail View - Megaco Capture 6.3.3 Detail View - H.323 Capture 6.3.4 Detail View - SS7 SIGTRAN Capture 	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 6.2.6 Define Views 6.3 Detail View (Selecting Individual Frame) 6.3.1 Detail View - SIP Capture 6.3.2 Detail View - Megaco Capture 6.3.3 Detail View - H.323 Capture 6.3.4 Detail View - SS7 SIGTRAN Capture 6.3.5 Detail View - GSM A IP Capture 	29
 6.1 Define Views to Display 6.2 Summary View	29
 6.1 Define Views to Display 6.2 Summary View 6.2.1 Setting a Relative Time 6.2.2 Summary Column Selection 6.2.3 Column Resizing and Reordering 6.2.4 Repositioning Summary View 6.2.5 Summary Colors 6.2.6 Define Views 6.3 Detail View (Selecting Individual Frame) 6.3.1 Detail View - Megaco Capture 6.3.2 Detail View - Megaco Capture 6.3.4 Detail View - H.323 Capture 6.3.5 Detail View - ISDN SIGTRAN Capture 6.3.6 Detail View - GSM A IP Capture 6.3.7 Detail View - UMTS IP Capture 6.3.8 Detail View - LTE Capture 	29 30 30 31 32 32 33 33 33 33 34 35 36 37 36 37 38 39 40 41 41
 6.1 Define Views to Display 6.2 Summary View	29 30 30 31 32 32 33 33 33 34 35 36 37 36 37 38 39 40 40 41 42 43
 6.1 Define Views to Display 6.2 Summary View	29 30 30 31 32 32 33 33 33 34 35 36 36 37 38 39 40 40 41 42 43 44
 6.1 Define Views to Display 6.2 Summary View	29
 6.1 Define Views to Display	29 30 30 31 32 32 33 33 33 34 34 35 36 37 36 37 36 37 38 39 40 41 41 42 43 44 44
 6.1 Define Views to Display	29
 6.1 Define Views to Display 6.2 Summary View	29 30 30 31 32 32 33 33 33 34 34 35 36 37 38 39 40 40 41 42 42 43 44 44 44 44 44
 6.1 Define Views to Display	29

i

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	
6.14 Forward Search and Backward Search	
6.14.1 Searching Towards the End of the Trace (Forward Search)	
6.14.2 Searching Towards the Beginning of the Trace (Backward Search) \dots	
6.15 Display Trace File Name	
6.16 Default Summary Columns	
6.17 Invoke Packet Data Analysis	
Section 7.0 Capture Menu Features	
7.1 Periodic Trace Saving Options	
7.2 Setting Capturing Options	
7.2.1 In Memory for High Traffic Capture Rate	
7.2.2 Circular Capture Buffer	
7.3 Stream / Interface Selection	
7.4 Setting Capture Filter	
7.4.1 MAC Layer	
7.4.2 IP	
7.4.3 TCP	
7.4.4 UDP	
7.4.5 SCTP	
7.4.6 SIP 7.4.7 RTP	
7.4.7 KTP	
7.4.9 MEGACO	
7.4.10 H323	
7.5 GUI and Protocol Options	
Section 8.0 Statistics	
8.1 Steps to Display Statistics	
8.1.1 Selecting Field Names (Step 1)	
8.1.2 Defining Use Type (UT) and Statistics Type (Step 2)	
8.1.3 Update Selected Statistics Information List (Step 3)	
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	
8.3 Loading Statistics	82
8.4 Load and Edit Statistics	82
8.5 Save Statistics	82
8.6 Export Statistics	
Section 9.0 Configuring for Call Detail Records	
9.1 Build Call Detail Record	
9.2 Active Calls Only	
9.3 Open Call Detail Record	
9.3.1 Active and Completed Calls	
9.3.2 Call Duration	
9.3.3 Find CDR	
9.4 Select Call Detail Columns to Display	

9.4.1 Call Detail Records View	
9.5 Display Selected Call Summary	
9.6 Display Entire Summary	
9.7 Closing Call Detail Record	
9.8 Export Call Detail Records	91
Section 10.0 Protocol Analyzer Configuration	93
10.1 Select summary columns to display	
10.2 Menu Checked Options	
10.3 Protocol Standard Selection	
10.4 Network / User Side Selection	
10.5 Time Format	
10.6 Filtering Criteria	
10.7 View Search	
10.8 Connecting to Remote Database	
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
10.13 Define Summary Columns	
•	113
10.14 Capture Options	113 115
10.14 Capture Options	113 115 115
10.14 Capture Options. Section 11.0 Status Indicators 11.1 Capture Rate.	113 115 115 115
10.14 Capture Options Section 11.0 Status Indicators 11.1 Capture Rate 11.2 Trace File Name	113 115 115 115 115
10.14 Capture Options	113 115 115 115 115 115 115
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 115 117
10.14 Capture Options	113 115 115 115 115 115 115 117
10.14 Capture Options	113 115 115 115 115 115 117 117 118
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 115 117 117 118 118
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 117 117 118 118 118 121
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 115 117 117 118 118 121 121
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 117 117 118 118 118 121 121 121
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 117 117 118 118 118 118 121 121 122
10.14 Capture Options Section 11.0 Status Indicators 11.1 Capture Rate 11.2 Trace File Name 11.3 Filtered and Total Frame Count 11.4 Missed Frames Section 12.0 Packet Data Analysis – Traffic Analyzer Summary View 12.1 Overview 12.2 Summary View 12.2.1 Call Summary 12.2.2 Graphs 12.2.2 Average Jitter Distribution 12.2.3 E-Model	113 115 115 115 115 115 117 117 118 118 118 121 121 122 122 124
10.14 Capture Options	113 115 115 115 115 115 115 117 117
10.14 Capture Options Section 11.0 Status Indicators	113 115 115 115 115 115 115 117 117
10.14 Capture Options Section 11.0 Status Indicators	113 115 115 115 115 115 117 117 118 118 118 121 121 122 122 122 124 126 129
10.14 Capture Options Section 11.0 Status Indicators	113 115 115 115 115 115 115 115
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 115 115
10.14 Capture Options Section 11.0 Status Indicators 11.1 Capture Rate. 11.2 Trace File Name. 11.3 Filtered and Total Frame Count. 11.4 Missed Frames. Section 12.0 Packet Data Analysis – Traffic Analyzer Summary View. 12.1 Overview 12.2 Summary View 12.2.2 Graphs. 12.2.2 Graphs. 12.2.2 Average Jitter Distribution 12.2.2.3 E-Model 12.2.2.4 RTP Packets Graph 12.2.2.5 Analysis of Fax over IP (T.38). 12.2.2.6 Call Graph. Call Summary – Signaling, Audio, & Video QoS Parameters. 12.2.2.7 Signaling Parameters. 12.2.2.8 Audio Parameters.	113 115 115 115 115 115 117 117 117 117 118 121 121 122 122 124 124 124 124 124 124 124 124 124 124 120 120 130 130
10.14 Capture Options	113 115 115 115 115 115 115 117 117
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 115 117 117
10.14 Capture Options. Section 11.0 Status Indicators	113 115 115 115 115 115 115 117 117
10.14 Capture Options Section 11.0 Status Indicators	113 115 115 115 115 115 115 115 117 117 118 121 122 122 122 122 124 124 129 130 130 132 133 134 135

12.2.3.6 IuCS1	38
12.3 File Menu Options1	39
12.3.1 Export Displayed Summary1	39
12.3.2 Export Terminated Calls1	40
12.4 View Menu Options1	40
12.4.1 Toolbar/Status Bar1	40
12.4.2 Find1	41
12.4.3 Call Detail View1	.42
12.4.4 Go To Analyzer1	.42
12.5 Call Summary Menu Options1	.42
12.5.1 Protocols1	.42
12.5.2 Filters	.47
12.5.3 Save Call1	.49
12.5.4 Reports	51
12.5.5 Extract Fax Image1	
12.5.6 Play Audio	
12.5.7 Write to File	54
12.5.8 Record Video1	
12.5.8.1 Video Codecs1	
12.5.8.2 Procedure	
12.6 Additional Settings	
12.6.1 E-Model Parameters	
12.6.2 VQMon Settings	
12.6.3 Payload Map Table	
12.6.3.1 Codec Type	
12.6.4 Codec Parameter Settings	
12.6.5 Triggers and Action Settings	
12.6.5.1 Trigger List	
12.6.5.2 Filter Selection	
12.6.5.3 Save Call to File	
12.6.5.4 Audio Recording	
12.6.5.5 User Defined	
12.6.5.6 Send e-mail	
12.6.5.7 Alert Summary	
12.6.5.8 Call Detail Record	
12.6.5.9 Extract Fax Image	
12.6.5.10 File Menu Options	
12.6.5.11 Example – Using Triggers and Action Feature	
12.6.6 PDA Startup Options	
12.0.0 PDA Startup Options	
Section 13.0 Packet Data Analysis Detail View (RTP Diagnostic View)	
13.1 Overview	
13.2 Columns in Detail View	
13.2.1 Functions Invoked By Right Click	
13.3 Statistics and Graphs	
13.3.1 RTP Statistics	
13.3.2 RTCP Statistics	
13.4 Graphs	
13.4.1 Gap Graph	
13.4.1 Gap Graph	
13.4.2 Gap Distribution Graph	
13.4.4 Jitter Distribution Graph1 13.4.5 MOS Graph (Mean Opinion Score)1	
13.4.6 Inband Events	
13.4.7 RTP Events (Outband Events)1	23

13.4.8 Wave Graph	193
13.4.9 Spectral Display	
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
	204
13.7.5.3 User Defined Tones	
13.7.5.3 User Defined Tones 13.8 Additional Settings	
	204
13.8 Additional Settings	204 205
13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary	
13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary Note: This feature is applicable only for SIP calls	
13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary Note: This feature is applicable only for SIP calls. 14.1 Overview	204 205 205 205 205 206
 13.8 Additional Settings	204 205 205 205 206 206
 13.8 Additional Settings	204 205 205 205 206 206 206 206 207
 13.8 Additional Settings	204 205 205 205 206 206 206 207 207
 13.8 Additional Settings	204 205 205 205 206 206 206 207 207 207
 13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary Note: This feature is applicable only for SIP calls. 14.1 Overview 14.2 Registration Summary 14.3 Registration Filters. 14.4 Registration Filters. 14.5 Graphs 14.5.1 Active Registration Graph 	204 205 205 205 206 206 206 207 207 207 207 207
 13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary Note: This feature is applicable only for SIP calls. 14.1 Overview 14.2 Registration Summary. 14.3 Registration Filters. 14.4 Registration Filters. 14.5 Graphs 14.5.1 Active Registration Graph 14.5.2 Registration Trace 	204 205 205 205 206 206 207 207 207 207 207 207 207
 13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary Note: This feature is applicable only for SIP calls. 14.1 Overview	204 205 205 205 206 206 206 207 207 207 207 207 207 207 207 207
 13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary Note: This feature is applicable only for SIP calls. 14.1 Overview 14.2 Registration Summary 14.3 Registration Summary 14.3 Registration Filters. 14.4 Registration Statistics. 14.5 Graphs 14.5.1 Active Registration Graph 14.5.2 Registration Trace Appendix A: Glossary of Protocol Fields.	204 205 205 205 206 206 206 207 207 207 207 207 207 207 207 207 207
 13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary Note: This feature is applicable only for SIP calls. 14.1 Overview. 14.2 Registration Summary. 14.3 Registration Filters. 14.4 Registration Filters. 14.5 Graphs 14.5.1 Active Registration Graph 14.5.2 Registration Trace Appendix A: Glossary of Protocol Fields. Appendix B: Call States.	204 205 205 205 206 206 207 207 207 207 207 207 207 207 207 215 215 219
 13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary Note: This feature is applicable only for SIP calls. 14.1 Overview 14.2 Registration Summary. 14.3 Registration Filters. 14.4 Registration Filters. 14.5 Graphs 14.5.1 Active Registration Graph 14.5.2 Registration Trace Appendix A: Glossary of Protocol Fields. Appendix B: Call States. Appendix C: SIP Registration States Appendix D: Graphs	204 205 205 205 206 206 207 207 207 207 207 207 207 207 207 207
 13.8 Additional Settings. Section 14.0 Packet Data Analysis – Registration Summary	204 205 205 205 206 206 207 207 207 207 207 207 207 207 207 207
 13.8 Additional Settings Section 14.0 Packet Data Analysis – Registration Summary	204 205 205 205 206 206 207 207 207 207 207 207 207 207
 13.8 Additional Settings Section 14.0 Packet Data Analysis - Registration Summary	204 205 205 205 206 206 207 207 207 207 207 207 207 207 219 219 219 219 219
 13.8 Additional Settings Section 14.0 Packet Data Analysis - Registration Summary	204 205 205 205 206 206 207 207 207 207 207 207 207 207

(Intentional Blank Page)

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

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

Figure 129: Call Summary	
Figure 130: RTD Calculation	
Figure 131: Active Calls Graph	121
Figure 132: Average Jitter Distribution	
Figure 133: R-Factor	
Figure 134: Mean Opinion Score	123
Figure 135: Packets Discarded	
Figure 136: RTP Packets Graph	
Figure 137: Fax analysis over IP (T.38) Ladder Diagram	124
Figure 138: Decode PacketScan™ Captured Fax files in GLInsight™	
Figure 139: Call Flow Ladder Diagram for SIP Call	
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	
Figure 144: Signaling, Audio and Video Parameters	
Figure 145: Video QoS Statistics	
Figure 146: Counter Type	
Figure 147: SIP Counters	
Figure 148: H.323 Counters	
Figure 149: MEGACO Counters	
Figure 150: RTP Counters	
Figure 151: GSMA Counters	
Figure 152: IuCS Counters	138
Figure 153: Export Displayed Summary	139
Figure 154: Export Summary Calls Summary	
Figure 155: Play Sound Toolbar	
Figure 156: Find Dialog	
Figure 157: Protocols	
Figure 158: SIP Calls	
Figure 159: H.323 Calls	
Figure 160: Auto Detected RTP Calls	
Figure 161: MeGaCo Calls	
Figure 162: GSM A Calls	
Figure 163: IuCS Calls	
Figure 164: Sessions	148
Figure 165: Save Call	149
Figure 166: Call Summary File	
Figure 167: PCAP Option Selected	
Figure 168: Selection of RTP Headers	
Figure 169: Packetscan Call Summary Report in PDF Format	152
Figure 170: Extract Fax Image from Call	152
Figure 171: Play Jitter Options	
Figure 172: Write to File	
Figure 173: Write to File with Separate Option Selected	
Figure 174: Invoke Adobe Audition after Write	
Figure 175: Summary View Displaying Video Calls	
Figure 176: Record	
Figure 177: Record Video	160
Figure 178: E-model Parameters	
Figure 179: VQMon Settings	
Figure 180: Dynamic Payload Mapping Table	162
Figure 181: G726 Codec Type	
Figure 182: AMR Codec Type	
Figure 183: EVRC Codec Type	
Figure 184: G722.1 Codec Type	
Figure 185: AMR_WB Codec Type	
Figure 186: EVRCB Codec Type	
Figure 187: EVRC_C Codec Type	
Figure 188: G726_VAD Codec Type	
Figure 189: Triggers and Action Settings	
Figure 190: Save Call Options	
Figure 191: Audio Recording	
Figure 192: Send e-mail	
Figure 192: Alert Message	
······································	_, 0

Figure 194: Call Detail Record	
Figure 195: Call Side Record171	
Figure 196: Call Master Record172	
Figure 197: Call Event Record173	
Figure 198: Extract Fax Image174	
Figure 199: File Menu	
Figure 200: Enable Triggers	
Figure 201: Enabling Startup Options	,
Figure 202: Loading tgr Profile File	
Figure 203: Trigger and Action Profile Path in sipProt.ini	,
Figure 204: Alert Summary	
Figure 205: Detail View	
Figure 206: Detail View Columns	
Figure 207: Show Latest	
Figure 207: Show Latest	
Figure 209: Call Information	
Figure 210: RTCP	
Figure 211: RTCP Details of Sender Report	
Figure 212: RTCP Details of Receiver Report	
Figure 213: SDES Item185	
Figure 214: Bye Packet	
Figure 215: 3D Gap Graph	
Figure 216: 2D Gap Graph	
Figure 217: 3D Jitter Graph	
Figure 218: 2D Jitter Graph	
Figure 219: 3D Gap Distribution Graph	
Figure 220: 2D Gap Distribution Graph	
Figure 221: 3D Jitter Distribution Graph	
Figure 222: 2D Jitter Distribution Graph	
Figure 223: 3D MOS Graph	
Figure 224: 2D MOS Graph	
Figure 225: Inband Events	
Figure 226: Digits Only	
Figure 227: All Events	
Figure 228: Export to File	
Figure 229: RTP Events Screen	
Figure 230: Wave Graph193	
Figure 231: Offline Analysis194	
Figure 232: Spectral Display194	
Figure 233: Quality Metrics	
Figure 234: Degradation Factor	
Figure 235: Burst Metrics	
Figure 236: Jitter Buffer Stats	ļ
Figure 237: Export Displayed Summary	
Figure 238: User Options	
Figure 239: Parameters	
Figure 240: User Defined Tones	
Figure 241: Registration Summary	
Figure 242: Summary Columns	
Figure 242: Summary Columns	
Figure 244: Counter Type	
Figure 245: Active Registration Graph	
Figure 246: Registration Trace Ladder Diagram	
Figure 247: Summary View	
Figure 248: Marker Bit	
Figure 249: Registration Status	
Figure 250: Ethernet PCAP Trace File to HDL	
Figure 251: Packet over IP CDR Analysis System	
Figure 252: SIP CDR Analysis using Excel® Addin223	
Figure 253: Import PacketScan [™] Text (*.txt) Sample Files	
Figure 254: No. of Calls Per Day (CPD) graph225	
Figure 255: Calls per Day Table	

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.

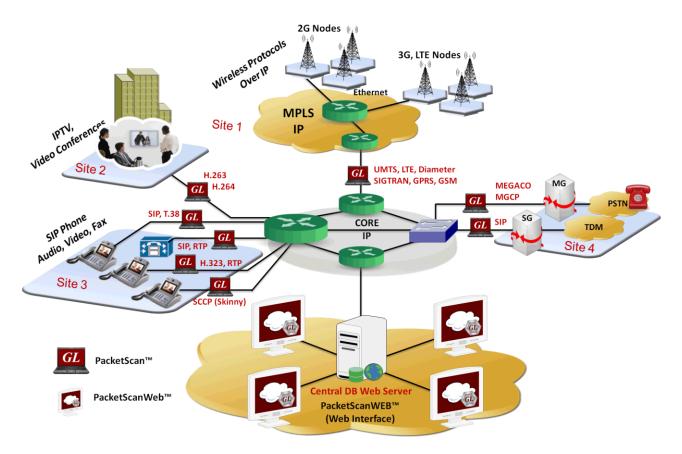


Figure 1: PacketScan™ Main Image

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.

 $\mathsf{PacketScan}^{\mathsf{M}}$ 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 <u>PacketScanWEB[™]</u>, 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^M 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 GSMA over IP (BSSAP, CC, MM, RR, GCC, BCC, and more)

• GPRS over IP

Decodes GPRS-GB interface (BSSGP, LLC, SNDCP, 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 Pro	tocols	Standards / Specifications Used
SIP-3261	МАС	IEEE 802.3
Megaco3525	IP	RFC 791
Megaco3015	ТСР	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
	НТТР	RFC 2616
	FTP	RFC 959
	SNMP	RFC 1157,1155,1902,3416,2863,2578,3418,2011,2012 etc
	Т38	ITU-T T.38
	ARP	RFC 826
	RARP	RFC 903
	RIP	RFC 2453
	SCTP	RFC 2960
	СОТР	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
	·

	DIMONDIA	
	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
		KSVF . KIC-2205, KIC-2210 KSVF-1L . KIC-5205
	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 IUA	ANSI - T1.113.1 to T1.113.4 RFC 4233 / RFC 5133
	IUA	BICC pl-080r1, T-REC-Q.1902.2-07/2001, T-REC-
	BICC	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
<u> </u>	M3UA ANSI	RFC 3332
 	MTP2- ITU	ITU-T Q.703
	MTP3 ITU MTP3 ANSI	ITU-Y Q.701-Q.705 / ITU-T Q.782 T1.111.4-1996
<u> </u>	MTP3 ANSI MTP2, MTP3 ANSI	T1.111.4-1996 T1.111.4-1996
<u> </u>	ICMP	RFC 792
<u> </u>	MAP R99	3GPP TS 09.02 V7.14.0 (2003-09)
<u> </u>		
1		
 	MAP R4 TCAP ITU	3GPP TS 29.002 V4.18.0 ITU-T Q.771 - Q.775

	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
	SNDCP	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	3GGP TS 29214-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	3GGP TS 29.328 & TS 29.329
	Rf/RO	3GGP TS 32.225, 3GPP TS 32.299 3GPP TS 29.061
	Wg/Wm/Wa/Wd/Pr	3GPP TS 29.234

1.3 Main Features

Capacity	 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	SIP RFC 3261- MAC, IP, IPv6, UDP, TCP, SMPP
<u></u>	 SIP-I, SIP-T
	 Megaco- RFC 3525, RFC 3015
	 MGCP - RFC 3991
	H 222 // 225
	 H.323/H.225 RTP - RFC 3550, RTCP, T.38, Video, and more.
	 SS7 SIGTRAN - SS7 over IP (ISUP, MAP, CAP, TCAP, INAP, CNAM,
	• SS7 SIGTRAN - SS7 OVELTP (ISOP, 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, SNDCP, 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	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.
<u>As a Single Point</u> <u>Analysis System</u>	PacketScan [™] has been enhanced to work with GL's <u>VoiceBand Analyzer (VBA)</u> and <u>Call Data Records (CDR)</u> applications to provide useful call detail records for further analysis <u>using built-in tool in Excel®</u> .
Packet Data Analysis	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	 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	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	 Segregation of IP traffic, VoIP, and Fax calls Extracts fax images in TIFF format for Fax calls <u>Audio capture/playback - Listen and Record RTP (Audio) streams</u> <u>Record Video and Video QoS Statistics</u>
SIP Registration Details	Registration statistics and trace messages depicted graphically.
Utilities	 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/H323, 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.

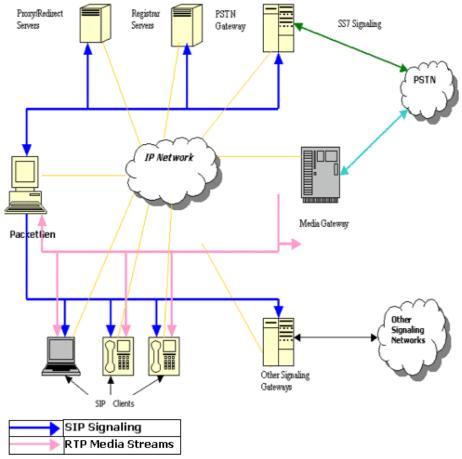


Figure 2: Testing networks components with PacketScan™

(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:

Setup			×
Information Please read the following text.			1
Text			
The following applications will be enabled: Part#, Application Name, Serial# PKS100, PacketVision, 0180BDD5 PKS101, PacketSim SIP Core, 0180BDD5 PKS102, PacketSim Soft RTP Core, 0180BDD5 PKS110, H323 Call Generator, 0180BDD5			<u>^</u>
InstaliShield			<u>۔</u> اع
	< <u>B</u> ack	Next >	Cancel

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.

InstallShield Wizard	×
	Welcome to the InstallShield Wizard for PacketScan
	The InstallShield® Wizard will install PacketScan on your computer. To continue, click Next.
	< Back Next > Cancel

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:

InstallShield Wizard
Choose Destination Location
Select folder where Setup will install files.
Setup will install PacketScan in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
E:\\GL Communications Inc.\PacketScan Browse
InstallShield
< <u>B</u> ack <u>Next></u> Cancel

Figure 5: Choose Destination Location

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

InstallShield Wizard	×
Setup Status	
PacketScan Setup is performing the requested operations.	
Installing:	
E:\\missing-out of seq-duplicate packets_single completed session.HDL	
50 <mark>%</mark>	
InstallShield	Cancel

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:

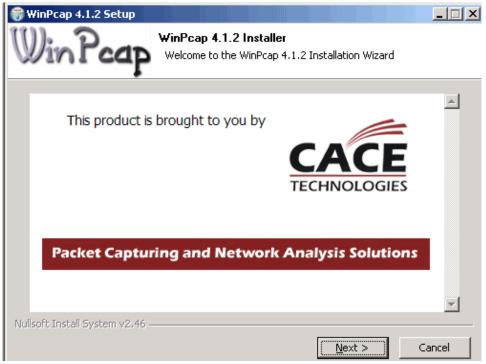


Figure 7: WinPcap Installation Wizard



Figure 8: WinPcap Welcome Screen

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

😽 WinPcap 4.1.2 Setup			
License Agreement Please review the license terms before installing WinPcap 4.1	.2.		
Press Page Down to see the rest of the agreement.			
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy). Copyright (c) 2005 - 2010 CACE Technologies, Davis (California). All rights reserved.	-		
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:			
 Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials 			
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.2.			
Nullsoft Install System v2,46			
< <u>B</u> ack I <u>Ag</u> ree Cance	¥		

Figure 9: WinPcap License Agreement Screen

 Select 'Automatically start the Winpcap driver at boot time' option and click 'Install' to install the software.

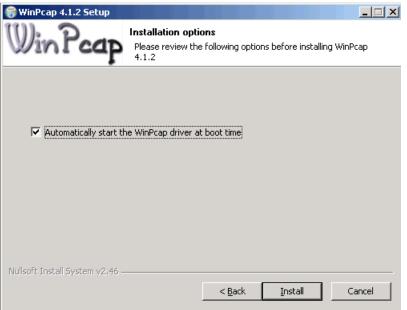


Figure 10: WinPcap Installation Wizard -Screen4

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

🗑 WinPcap 4.1.2 Setup		- 🗆 🗵
	istalling Please wait while WinPcap 4.1.2 is being installed.	
Output folder: E:\Program File	s\WinPcap	
Nullsoft Install System v2,46 ——	< Back Next >	Cancel
WinPcap 4.1.2 Setup	Completing the WinPcap 4.1.2 Setup Wizard WinPcap 4.1.2 has been installed on your computer Click Finish to close this wizard.	_ _ ×
	< Back	Cancel

Figure 11: WinPCap Installation Completion Wizard

5) Microsoft Visual C++ 2005 Redistributable installation status

InstallShie	d Wizard		×
Setup St	atus		
Packe	Microsoft Visual C++ 2005 Redistributable		1
	12		
		Cancel	
InstallShield		C	ancel

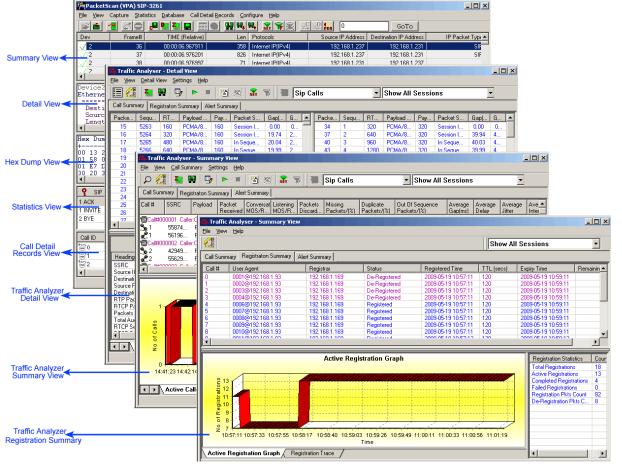
Figure 12: Microsoft Visual C++ 2005 Redistributable

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

InstallShield Wizard	
InstallShield Wizard	InstallShield Wizard Complete Setup has finished installing PacketScan on your computer.
	< <u>B</u> ack Finish Cancel

Figure 13: PacketScan[™] Installation Complete

тм



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

 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 <u>Protocol Standard Selection</u>.

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 <u>Setting Capturing Options</u>.
- 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 <u>Stream / Interface Selection</u>.
- 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 <u>Periodic Trace Saving Options</u>.
- 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 <u>Setting Capture Filter</u>.
- 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 <u>View Filtering Criteria</u>.

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 <u>Start Real-time</u> and <u>Stop (Pause)</u>.
- 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 <u>Save As and Close</u> and <u>Save As</u>.
- 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 <u>Export Details</u> and <u>Export Summary</u>.

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 <u>Open a Trace for Off-line Analysis</u>.

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 <u>Packet Data Analysis – Traffic Analyzer Summary View</u>, <u>Packet Data Analysis – Traffic Analyzer Detail View</u>, and <u>Packet Data Analysis – Registration Summary</u>.

(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.

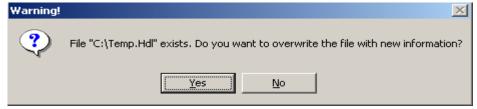


Figure 16: Saving the trace file

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

Open		? ×
Look jn: 🔁	G.711 💌 🗲 🖻 💣 🎟 🕇	
Auto detec	t RTP_G.711-alaw_ATA to Router_VAD OFF.HDL	
Auto detec	t RTP_G.711-mulaw_ATA to Router_VAD OFF.HDL	
File <u>n</u> ame:	<u></u> per	n
Files of <u>type</u> :	HDLC Files (*.*)	el
	Dpen as read-only	

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:

🛃 HDL File Conversion Utility 🛛 🗙									
Source Information									
File Name gs\Srikanthr\Desktop\sip-ipv6.pcap									
File Format Ethreal/LibpCap File									
Destination Information									
File Format									
File Name d Settings\Srikanthr\Desktop\sip.hdl									
Protocol SIP Filter									
🗖 Linux Format 🔲 Discard Duplicate Packets									
Reverse Bits Link Type Ethernet 💽 147									
Frames To Convert 0									
Skip Begin 0 Bytes Convert									
End 0 Bytes									

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 <u>HDL File Conversion Utility</u>

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

Save As		? ×
Save jn: 🔂	G.711 🔽 🗧 🖆 🎟	•
Auto detect	RTP_G.711-alaw_ATA to Router_VAD OFF.HDL	
📄 Auto detect	RTP_G.711-mulaw_ATA to Router_VAD OFF.HDL	
I		
File <u>n</u> ame:	<u>S</u> a	ve
Save as <u>type</u> :	HDLC Frame Output Files (*.HDL)	ncel

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

Save As						x
Source Frame / P	Displayed	C From	0	to	0	
Output File	Success			×		
unications Inc\	File writing) has complet	ted succe	essfully.	ignaling	
Overwrite		ОК				
OK	Cancel					

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 I from the tool bar

Save As			? ×
Save in: 🔂	G.711	- + 🗈	
Auto_Deta	ect_G.711.TXT		
File <u>n</u> ame:	Auto_Detaect_G.711.TXT		<u>S</u> ave
Save as <u>t</u> ype:	ASCII Export Files (*.TXT)	•	Cancel

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.

Export Summary	×	Save As					? ×
Export File Name		Save jn: 🔁	G.711	• +	£ (• 🎫 🎽	
		Auto_Deta	ect_G.711.TXT				
Columns to Export Device Frame# Time Length (Bytes) Error Source IP Address Destination IP Address Packet Type TCP Source Port TCP Source Port	Export Headers Select All Export Cancel						
TCP Destination Port		File <u>n</u> ame:	Auto_Detaect_G.711.TXT			<u>S</u> ave	;
		Save as <u>type</u> :	ASCII Export Files (*.TXT)		•	Cano	el

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.

Define Views to Display
Summary Detail Hex Dump Statistics Call Trace
OK Cancel

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.

Packe	tScan (VP	A) 5IP-3261							_	
File View Capture Statistics Database Call Detail Records Configure Help										
Dev	Frame#	TIME (Relative)	Protocols	Len	Error	Source IP Addr	ess	Destination IP Addre	IP Packet Type	T(🔺
$\sqrt{1}$	0	-00:00:00.039	Internet IP(74		192.168.20.1	01	192.168.20.231	RTP	
$\sqrt{1}$	1	-00:00:00.020	Internet IP(74		192.168.20.1	01	192.168.20.231	RTP	
$\sqrt{1}$	2	00:00:00.000	Internet IP(Set	: Relative	Time	[1	192.168.20.231	RTP	
$\sqrt{1}$	3	00:00:00.009	Internet IP(lumn Selection	11	192.168.20.101	RTP	
$\sqrt{1}$	4	00:00:00.020	Internet IP(Columns	11	192.168.20.231	RTP	
$\sqrt{1}$	5	00:00:00.020	Internet IP(nmary Co		11	192.168.20.101	RTP	
$\sqrt{1}$	6	00:00:00.039	Internet IP(fine Views		11	192.168.20.231	RTP	
$\sqrt{1}$	7	00:00:00.040	Internet IP(17	1110 11011	102.100.20.2		192.168.20.101	RTP	
./1	8	00:00:00 059	Internet IPí	74		192 168 20 1	01	192 168 20 231	BTP	

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.

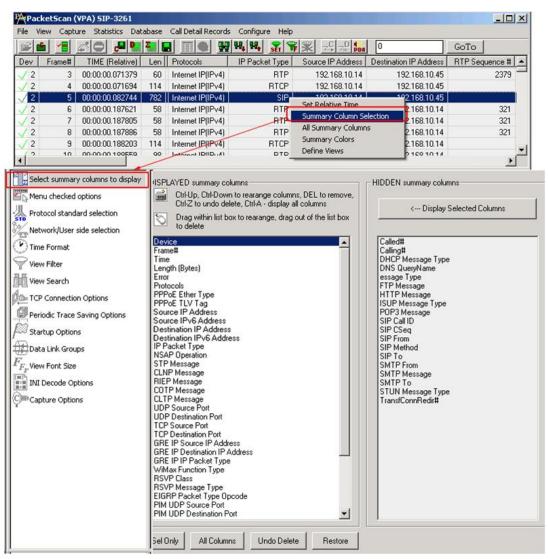


Figure 25: Select Columns to Display

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 <u>Select Columns to Display</u> 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.

PacketSca	n (VPA) SIP	-3261					_ 0	×		
<u>File View</u> Ca	pture <u>S</u> tati	stics <u>D</u> atabase	Call Detail <u>R</u> ed	ords <u>C</u> onfigur	e <u>H</u> elp					
🖆 🖆	2 0	da 🔤 🔤		₩ ₩, ₩,	🚮 🎀 🛒 🚅		GoTo			
Dev	Frame#	TIME (Relative	Protocols	Len	Source IP Address	Destination IP Addre	, IP Packet Type			
$\sqrt{1}$	0	-00:00:00.039	Internet IP[74	192.168.20.101	192.168.20.23	RTP			
√ 1	1	-00:00:00.020	Internet IP(74	192.168.20.101	192.168.20,231	RTP			
$\sqrt{1}$	2	00:00:00.000	Internet IP(74	192.168.20.101	192.168/20.231	RTP			
$\sqrt{1}$	3	00:00:00.009	Internet IP(74	192.168.20.231	192.168.20.101	RTP			
√1	4	00:00:00.020	Internet IP(74	192.168.20.101	192.168.20.231	RTP			
√1	5	00:00:00.020	Internet IP(74	192.168.20.231	192.168.20.101	RTP			
<u>√</u> 1	6	00:00:00.039	Internet IP(74	192.168.20.101	192.168.20.231	RTP	<u> </u>		
•					/	/	Select summary	columns	to display	DISPLAYED summary columns
		\					Menu checked o	ptions		Ctrl-Up, Ctrl-Down to rearange columns, DEL to remove
PacketScar	n (YPA) SIP	-3261								Ctrl-Z to undo delete, Ctrl-A - display all columns
<u>File View</u> Ca	pture <u>S</u> tati	stic <mark>s <u>D</u>atabase</mark>	Call Detail <u>R</u> ed	ords <u>C</u> onfigur	e <u>H</u> elp	5	Protocol standar	u seleu	.1011	Drag within list box to rearange, drag out of the list box
🚅 🖆 📲		e 🔤 🔤		👯 W, W,	** **		Network/User sid	de selec	tion	to delete
Dev	TIME (Rel	Frame#	Protocols	Len Error	Packet Type 9	Source IP Address D	Yime Format			Device A
$\sqrt{1}$	-00:00:00.	0	nternet IP(74	RTP	192.168.20.101	View Filter			Time
√1	-00:00:00.	1	nternet IP(74	RTP	192.168.20.101	E.,			Protocols Length (Bytes)
$\sqrt{1}$	00:00:00.0	l 2	nternet IP(74	BTP	192.168.20.101	View Search			Error
$\sqrt{1}$	00:00:00.0	1 3	nternet IP(74	RTP	192.168.20.231	= TCP Connection	Options	;	Source IP Address
$\sqrt{1}$	00:00:00.0	l 4	nternet IP(74	RTP	192.168.20.101	Periodic Trace Sa	uina O	ntions	Destination IP Address IP Packet Type
√1	00:00:00.0	l 5	nternet IP(74	RTP	192.168.20.231			paons	TCP Destination Port
<u>√</u> 1	00:00:00.0	1 6	nternet IP(74	RTP	192.168.20.101	Startup Options			TCP Source Port
4							•			

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:

PacketScan (VPA) SIP-3261										
<u>File V</u> iew	Capture <u>S</u> tal	istics <u>D</u> ataba	se Call Del	tail <u>R</u> ecords 🛛 🖸	onfigure <u>H</u> elp					
Dev	TIME (Date)	Protocols	Frame#	Len	Source IP Address	Destination IP Addre	IP Packet Type	CP Source P 🔺		
√1	2004-03-2	Internet IP(4	74	192.168.20.101	192.168.20.231	RTP			
$\sqrt{1}$	2004-03-2	Internet IP(5	74	192.168.20.231	192.168.20.101	RTP			
$\sqrt{1}$	2004-03-2	Internet IP(6	74	192.168.20.101	192.168.20.231	RTP			
$\sqrt{1}$	2004-03-2	Internet IP(7	74	192.168.20.231	192.168.20.101	RTP			
$\sqrt{1}$	2004-03-2	Internet IP(8	74	192.168.20.101	192.168.20.231	RTP			
$\sqrt{1}$	2004-03-2	Internet IP(9	74	192.168.20.231	192.168.20.101	RTP			
$\sqrt{1}$	2004-03-2	Internet IP(10	74	192.168.20.101	192.168.20.231	RTP			
11	2004/02/2	Internet IPI	11	74	100 100 00 001	100 100 00 101	DTD			
•										
			-24 11:	30:50.400	464 OK Len=74					
	et Frame Da									
	===== MAC nation Add					32008BE8	Click G			
	e Address	iress				L8007C6C	Press	Enter		
	h/Protocol	Tune				Internet IP(IP	σA.)			
	===== IP			==	=	10001000 11(11				
Versi		20.902			= 0100.	(4)				
Inter	net Header	Length (In 32 b	it words)						
	of Service			,	=			_		
. Door	odonoo			-1	- 101	רסדידר /ערס		_		
•										

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.

Taci	ketScan (VPA) 5IP-3261								
ile Vi	ew Captu	ure Statistics Dat	tabase	Call Detail Records	Configure Help					
2	à 📲	alo 📕 🔛	2		¥, ¥, 💦 🖷	꽃모ᄱ	0	GoTo		
)ev	Frame#	TIME (Relative)	Len	Protocols	IP Packet Type	Source IP Address	Destination IP Address	RTP S	iequence # 🔺	
/ 2	3	00:00:00.071379	60	Internet IP(IPv4)	BTP	192.168.10.14	192.168.10.45		2379	
/ 2	4	00:00:00.071694	114	Internet IP(IPv4)	RTCP	192.168.10.14	192.168.10.45			
/ 2	5	00:00:00.082744	782	Internet IP(IPv4)	Set Relative	Time 4	192.168.10.45	11-		
/ 2	6	00:00:00.187621	58	Internet IP(IPv4)		5	192.168.10.14		Summary Colors	
/ 2	7	00:00:00.187805	58	Internet IP(IPv4)	All Summary Co	lumn Selection 5	192.168.10.14		Dev	
/ 2	8	00:00:00.187886	58	Internet IP(IPv4)	Summary Co	5	192.168.10.14		Frame#	
2	9	00:00:00.188203	114	Internet IP(IPv4)	Define Views		192.168.10.14		TIME (Relative)	
12	10	00-00-00 100550	00	Internet ID(ID(d)	Denne views	, k	102 100 10 14		Error	
									Protocols	
									PPPoE Ether Type PPPoE TLV Tag	
Pac	ketScan (VPA) 5IP-3261							Source IP Address	
•		(VPA) SIP-3261 ure <u>S</u> tatistics <u>D</u> ai	tabase	Call Detail <u>R</u> ecords	; <u>C</u> onfigure <u>H</u> elp				Source IP Address Destination IP Address	s
ile ⊻	jew Capti	ure <u>S</u> tatistics <u>D</u> a						60	Source IP Address Destination IP Address IP Packet Type	s
jle V P	jew Capti	ure <u>S</u> tatistics <u>D</u> a	2		W, W, <u>st</u> ¶			Goʻ	Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message	s
ile ⊻ 22 1 Dev	iew Capti	ure Statistics Da Contractions Da TIME (Relative)	Len	Protocols	IP Packet Type	Source IP Address	Destination IP Address		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message	s
ile <u>V</u> Pev	jew Captr Frame#	ure Statistics Da IIME (Relative) 00:00:00.071379	Len 60	Protocols Internet IP(IPv4)	IP Packet Type RTP	Source IP Address 192.168.10.14	Destination IP Address 192.168.10.45		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message RIEP Message	\$
ile ⊻	jew Captr Frame# 3 4	ure Statistics Da TIME (Relative) 00:00:00.071379 00:00:00.071694	Len 60 114	Protocols Internet IP(IPv4) Internet IP(IPv4)	IP Packet Type RTP RTCP	Source IP Address 192.168.10.14 192.168.10.14	Destination IP Address 192.168.10.45 192.168.10.45		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message RIEP Message COTP Message CLTP Message	s
ile <u>V</u> Dev / 2 / 2 / 2	iew Captr Frame# 3 4 5	ure Statistics Da TIME (Relative) 00:00:00.071373 00:00:00.071694 00:00:00.082744	Len 60 114 782	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	IP Packet Type BTP RTCP SIP	Source IP Address 192.168.10.14 192.168.10.14 192.168.10.14	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message RIEP Message CLTP Message CLTP Message UDP Source Port	S
ile <u>V</u> Dev / 2 / 2 / 2 / 2	jew Capti Frame# 3 4 5 6	ure Statistics Da TIME (Relative) 00:00:00:071379 00:00:00:071694 00:00:00:082744 00:00:00:187621	Len 60 114 782 58	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	HU Packet Type RTP RTCP SIP RTP RTP	Source IP Address 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.45	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.14		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message RIEP Message COTP Message CLTP Message	\$
ile ⊻ Dev / 2 / 2 / 2 / 2 / 2	jew Captr	ure Statistics Da TIME (Relative) 00:00:00.071379 00:00:00.071594 00:00:00.082744 00:00:00.187621 00:00:00.187805	Len 60 114 782 58 58	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	HU Packet Type RTP RTCP SIP RTP RTP RTP	Source IP Address 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.45 192.168.10.45	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.14 192.168.10.14		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message RIEP Message CLTP Message CLTP Message UDP Source Port	\$
ile <u>V</u> Dev / 2 / 2 / 2 / 2 / 2 / 2 / 2	iew Captr Frame# Frame# 3 4 5 6 7 8	ure Statistics Da TIME (Relative) 00:00:00.071379 00:00:00.0082744 00:00:00.187621 00:00:00.187805 00:00:00.187886	Len 60 114 782 58 58 58	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	IP Packet Type RTCP SIP RTCP RTP RTP RTP RTP	Source IP Address 192.158.10.14 192.168.10.14 192.168.10.14 192.168.10.45 192.168.10.45 192.168.10.45	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.14 192.168.10.14 192.168.10.14		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message COTP Message COTP Message UDP Source Port UDP Destination Port	
le <u>V</u> Dev 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	iew Captr Frame# Frame# 3 4 5 6 7 8 9	ure Statistics Da TIME (Relative) 00:00:00.071373 00:00:00.002744 00:00:00.187825 00:00:00.187826 00:00:00.187886 00:00:00.188203	Len 60 114 782 58 58 58 58 114	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	IP Packet Type RTCP SIP RTCP RTP RTP RTP RTP RTP RTCP	Source IP Address 192.158.10.14 192.168.10.14 192.168.10.14 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message RIEP Message CLTP Message CLTP Message UDP Source Port	s Cancel
ile <u>V</u> Dev 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	iew Captr Frame# 3 4 5 6 7 8 9 10	ure Statistics Da TIME (Relative) 00:00:00.071379 00:00:00.082744 00:00:00.187621 00:00:00.187686 00:00:00.187686 00:00:00.188559	Len 60 114 782 58 58 58 58 114 98	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	IP Packet Type IP Packet Type RTCP SIP RTP RTP RTP RTP RTP RTP RTP RT	Source IP Address 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message COTP Message COTP Message UDP Source Port UDP Destination Port	
le <u>V</u> Dev 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	iew Captr Frame# 3 4 5 6 7 8 9 10 11	ure Statistics Da TIME (Relative) 0:00:00.0071373 0:00:00.0071373 0:00:00.00187821 00:00:00.187805 00:00:00188203 00:00:00188259 00:00:00.188559 00:00:00.188459	Len 60 114 782 58 58 58 58 58 114 98 98	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	IP Packet Type IP Packet Type RTCP SIP RTP RTP RTP RTP RTP RTP RTP RT	Source IP Address 192.168.10.14 192.168.10.14 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message CLPP Message CLTP Message UDP Source Port UDP Source Port UDP Destination Port	
le <u>V</u> Dev / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2	iew Capt Frame# 3 4 5 6 7 8 9 10 11 12	ure Statistics Da TIME (Relative) 00:00:00.071694 00:00:00.00187621 00:00:00.187865 00:00:00188559 00:00:001988559 00:00:001988559 00:00:00198407 00:00:00.231749	Len 60 114 782 58 58 58 58 58 114 98 98 214	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	IP Packet Type RTCP SIP RTCP SIP RTP RTP RTP RTP RTCP RTCP RTCP RTCP RTP RTCP RTP	Source IP Address 192.168.10.14 192.168.10.14 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLTP Message COTP Message CLTP Message UDP Source Port UDP Source Port UDP Destination Port	
ile ⊻ Dev 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2	iew Captr Frame# 3 4 5 6 7 8 9 10 11	ure Statistics Da TIME (Relative) 0:00:00.0071373 0:00:00.0071373 0:00:00.00187821 00:00:00.187805 00:00:00188203 00:00:00188259 00:00:00.188559 00:00:00.188459	Len 60 114 782 58 58 58 58 114 98 98 214 214	Protocols Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4) Internet IP(IPv4)	IP Packet Type IP Packet Type RTCP SIP RTP RTP RTP RTP RTP RTP RTP RT	Source IP Address 192.168.10.14 192.168.10.14 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.45	Destination IP Address 192.168.10.45 192.168.10.45 192.168.10.45 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14 192.168.10.14		Source IP Address Destination IP Address IP Packet Type NSAP Operation STP Message CLNP Message CLPP Message CLTP Message UDP Source Port UDP Source Port UDP Destination Port	

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**.

PacketScan	n (VPA)	SIP	-3261						<u> </u>
<u>F</u> ile ⊻iew Cap	pture 🔅	<u>S</u> tatis	tics <u>D</u> atabase	Call Detail <u>R</u> e	cords 🤇	<u>C</u> onfigure <u>H</u> elp			
🖻 🖆 📲		0	🚚 🎦 🎦 🛛		W 4	4 🕰 🚮 🌾 🛒			GoTo
Dev	Fram	ne#	TIME (Date)	Protocols	Len	Source IP Address	Destination IP Addre	IP Packet Type	TCP S 🔺
$\sqrt{1}$		4	2004-03-24	Internet IP(74	192.168.20.101	192.168.20.231	RTP	
$\sqrt{1}$		5	2004-03-24	Internet IP(74	192.168.20.231	192.168.20.101	RTP	
√ 1		6	2004-03-24	Internet IP(74	192.168.20.101	192.168.20.231	RTP	
√ 1		7	2004-03-24	Internet IP(74	192.168.20.231	192.168.20.101	RTP	
√ 1		8	2004-03-24	Internet IP(74	192.168.20.101	192.168.20.231	RTP	
√ 1		9	2004-03-24	Internet IP(74	192.168.20.231	192.168.20.101	RTP	
√ 1		10	2004-03-24	Internet IP(74	192.168.20.101	192.168.20.231	RTP	
4	1	11	2004.02.24	Internet IDf	74	100 100 00 001	102 100 20 101	DTD	
Device1 Fro Ethernet r				24 11:30:5	50.400)467 OK Len=74			
			Layer ===:			=			
Destinat			ess				18007C6C		
Source A			T				82008BE8		
Length/P:			aver ====:			= X0800	Internet IP(IP	∀4)	
Version	1		ayor			= 0100.	(4)		
Internet	Head	ler	Length (In	n 32 bit v	vords)				
Type of S		ice				=			-
- Procedor	<u> </u>					- 001	Pnioni++		

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 Laver	-
Destination Address	= x001CC0A3F414
Source Address	= x0013208E1369
Length/Protocol Type	= x86DD IPv6
======== IPv6 Laver =========	
Protocol Version	= 0110 (6)
Traffic Class	= 0 (0000 0000)
Flow Label	= 0 (0000 0000000 0000000)
Pavload 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=z9hG4
HDR	= From: sip:0001@[2001:ff01:21fd:fd0d:5606:3df0:2bfb:b056];tag=FromTag_4137862
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, UK
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
1	

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

🙀 Packet Scan (VPA) Megaco 3525							_ 8 ×
File View Capture Statistics Database Call	Detail <u>R</u> ecords <u>C</u> onfigure <u>H</u> el	p					
🖻 🖆 📲 🖾 🗢 🖉 🖳 🎴	= • ₩ ₩ ₩ ~ *	🎀 🛒 🚅 🚚 🚺 🛛		GoTo			
Dev Frame# T	IME (Relative)	Len	Error	Protocols	Source IP Address	Destination IP Address	IP Packet 🔺
/ 1 7 00:	:00:25.447443	84		Internet IP(IPv4	192.168.1.167	192.168.1.105	MEGACO 🗸
•							
	7443 OV Ten=84						
Ethernet Frame Data	440 OK LEH-04						
========= MAC Laver ======							
Destination Address		0050BAC1A951					
Source Address		0090BB15C66C					
Length/Protocol Type		(0800 Internet IP(I)	Der 4 A				
=========== IP Laver =======		.0000 inceined in(i)					
Version		0100 (4)					
Internet Header Length (In 32		$\dots 0101 (5)$					
Type of Service	. Dit words)	0101 (3)					
Precedence	- 1	10 Internetwo:	nle Const	mol			
Delay		0 Normal Dela		.101			
Throughput		0 Normal Thr					
Reliability		0Normal Rel:					
Reserved for Future Use		00. Normai Rei.	labiii	, y			
Total Length		70 (x0046)					
Identification		LO (x00048)					
Reserved) (0)					
DF		.0 May Fragme:					
MF							
Fragment Offset		0 Last Fragmu) (00000 0000000					
Time To Live		L28 (x80))				
Protocol							
		00010001 User Datag: xB57C	ram				
Header Check Sum							
Source IP Address		L92.168.1.167 (xCOA					
Destination IP Address		L92.168.1.105 (xCOA	20123)				
UDP Layer							
Source Port		2944 (x0B80)					
Destination Port		2944 (x0B80)					
Length (Header + Data)		50 (x0032)					
Checksum		51839 (xF18F)					
========== Megaco Layer ====							
MEGACO	= M	MEGACO/1 [192.168.1	.167]:2	944 Pendin	g=2U{}		

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	
<u>File View</u> Capture <u>Statistics</u> <u>Database</u> Call Detail <u>Records</u> <u>C</u>	onfigure <u>H</u> elp
# 4 # 4 4	1 👯 🛒 🛒 🚽 🚛 🚺 0 Goto 1
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 Ţ
· · · · · · · · · · · · · · · · · · ·	
Urgent Pointer	= x0000
========= TPKT Header Layer ========	
TPKT Hdr	-
Version	= 3 (x03)
Reserved	= 00000000 (0)
Length	= 326 (x0146)
======================================	
Protocol Discriminator	= 00001000 Q931/I.451 user-network call control
Call Reference Length	=0010 (2)
Call Reference Value Call Reference Flag	= 30357 (.1110110 10010101) = 1 TO side that originated callref
Message Type	= 1 10 side that originated callrer = 00000001 ALERTING
IEI Display	= 00101000 Display IE Identifier
IEI DISPIRY IE Length	= 9 (x09)
Display Information	= x4E61676172616A7300
IEI User User	= 0111110 User User IE Identifier
IE User User Length	= 303 (x012F)
Protocol Discriminator(H323)	= 000001011 X.680 and X.690 coded user information
======================================	=
H323-UserInformation	= SEOUENCE
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	
protocolIdentifier	= OBJECTIDENTIFIER
Length Determinant	
Contents	= 0.0.8.2250.0.4 - CEOURCE
destinationInfo Extensibility Marker	= SEQUENCE = 0
Extensibility Marker Preamble	= 0 = 010001
vendor	= SEQUENCE
Extensibility Marker	
Preamble	= 11
vendor	= SEQUENCE
L, Vender	

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

PacketScan (All-in-One)				_	
e <u>V</u> iew Capture <u>S</u> tatistics <u>D</u> atabase Call Detail <u>R</u> ecords <u>C</u> on	figure <u>H</u> elp				
= • · · · · · · · · · · · · · · · · · ·	▙▓▓▓ヹヹヹ	Da O	GoTo		
ev Frame# TIME (Relative)		Error Protocols	IP Packet Type	NSAP Operation	
4 00:00:04.244418	90	Internet IP(IPv4)			_
					Þ
)18 Header Check Sum	= xAA46				_
)1A Source IP Address	= 192.168.1.85	(xCOA80155)			
)1E Destination IP Address	= 192.168.1.20	1 (xCOA801C9)			
SCTP Layer	=				
22 Source Port Number	= 2905 (x0B59)				
24 Destination Port Number	= 2905 (x0B59)				
)26 Verification Tag	= 1992927916 (1	x76C9AAAC)			
)2A Checksum	= 1513447696 ()				
)2E Chunk Type	= 00000000 DAT				
)2F U bit	=0 Orde	ered DATA chunk			
)2F Beginning/Ending bits	=11 Rese	erved			
)30 Length	= 44 (x002C)				
132 TSN	= 1 (x00000001))			
136 Stream Identifier	= 1 (x0001)	,			
38 Stream Seguence Number	= 1 (x0001)				
13A Payload Protocol Identifier		P3 Hser adaptat:	ion Layer(M3UA)		
========== MTP3 User Adaptation Layer			,,,		
)3E Version	= 00000001 Rele	ease 1.0			
)40 Message Class	= 00000001 Tra				
)41 Transfer Message Type	= 00000001 Pav				
)42 Message Length	= 28 (x0000001				
Protocol Data	=	-,			
)46 Tag	= 528 (x0210)				
)48 Length	= 20 (x0014)				
Originating Point Code	=				
)4C Point Code	= 0.32.2(000)	001 00000010)			
Destination Point Code	- 0.32.2(000)	001 00000010)			
150 Point Code		001 00000001			
150 Foint Code 152 Service Indicator	= 0.32.1(000) =0101 ISD				
152 Service Indicator 153 Network Indicator	=10 Nat:				
153 Metwork Indicator 154 Message Priority	=00 Pric				
154 Message Friority 155 Signalling Link Selection	=0001 (1)	pricy code 0			
========== ISUP Laver =========					
J56 Circuit Identification Code		0000 (1)			
58 Message Type	= 00000001 = 00001001 Anst				
Mandatory Fixed Parameters	- 00001001 Ans	MCT.			
59 Pointer to optional parameters	= = x00 (0)				
	= x00 (0) = None				
Mandatory Variable Length Parameters	= None = None				
Optional Variable Length Parameters	- Mone				
					►
f-line Viewing E:\1	New Folder (3)\Isup Sigtran\AN	SI'Isun, Sic 62 Erames			

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

PacketScan (All-in-One)				_
le <u>Vi</u> ew Capture <u>S</u> tatistics <u>D</u> atabase Call Detail <u>R</u> ecords <u>C</u> onfig				
	▶ <u>\$</u> ₹₩₩ <u></u> <u></u> <u></u>	0	GoTo	
Dev Frame# TIME (Relative)		Protocols	IP Packet Type	NSAP Operation
/ 1 1 00:00:00.002111	102	Internet IP(IPv4)		
030 Length	= 55 (x0037)			
D32 TSN	= 8 (x00000008)			
D36 Stream Identifier	= 1 (x0001)			
038 - Stream Sequence Number	= 8 (x0008)			
D3A Pavload Protocol Identifier	= x00000001 ISDN U	ser Adaptatio	n Laver(IUA)	
=========== ISDN Q.921-User Adaptation L	ayer Layer ========	'		
D3E Version	= 00000001 Release			
D40 Message Class	= 00000101 Q.921/Q	.931 Boundary	Primitives Transpor	t (QPTM) Messages
041 QPTM Message Type	= 00000010 Data In	dication Mess	age	
042 Message Length	= 39 (x00000027)			
D46 Tag	= 1 (x0001)			
D48 Length	= 8 (x0008)			
D4A Interface Identifier (integer)	= 0 (x0000000)			
D4E Tag	= 5 (x0005)			
D50 Length	= 8 (x0008)			
D52 SAPI(Service Access Point Identifier)	= 000000 (0)			
D53 TEI(Terminal Endpoint Identifier)	= 0000001. (1)			
Protocol Data	=			
D56 Tag	= 14 (x000E)			
D58 Length	= 15 (x000F)			
Higher Layer Data	= x08028004021804E	1808381		
======== Q.93x Layer 3 Layer =======				
D5A Protocol Discriminator	= 00001000 Q931∕I.	451 user-netw	ork call control	
D5B Call Reference Length	=0010 (2)			
D5C Call Reference Value	= 4 (.0000000 0000			
D5C Call Reference Flag	= 1 TO side		ted callref	
D5E Message Type	= 00000010 CALL PR			
D5F IEI Channel Identification	= 00011000 Channel	Identificati	on IE Identifier	
D60 IE Channel Identification Length	= 4 (x04)			
D61 Info Channel Selection	=01 B1 chan:			
D61 D-channel Indicator			ed is not the D-chan	inel
D61 Preferred/Exclusive	=0 Indicat			
061 Interface Type	=1 Primary			
D61 Interface Identifier Present		ce explicitly	identified in one c	or more octets
D62 Interface Identifier	= .0000000 (0)			
063 Channel type∕Map elem type	=0011 B-channe			
D63 Number/Map			by the number in th	e following octet
D63 Coding Standard	= .00 ITU_T (CCITT) standa	rdized coding	
D64 Channel number	= .0000001 (1)			

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

APacketScan (All-in-One)		
<u>File Vi</u> ew Capture <u>S</u> tatistics <u>D</u> atabase Call Detail <u>R</u> ecords <u>C</u> onfigu	jure <u>H</u> elp	
🖻 🖆 💋 🚚 🛄 🔜 🔛 💘 🛰 🛰	🖌 🔐 🎇 🛫 🖓 🕹 0 🖉 GoTo	
Dev Frame# TIME (Relative)	Len Error Protocols IP Packet Type NSAP Operation	_
/1 55 00:00:22.887650	114 Internet IP(IPv4)	
· · · · · · · · · · · · · · · · · · ·		F
J054 Message Priority	=00 Priority Code 0	
0055 Signalling Link Selection	=0001 (1)	
SCCP Laver		
056 Message Type	= 00000110 DT1 data form 1	
Mandatory Fixed Parameters	=	
Destination Local Reference Parameter	=	
0057 Destination Local Reference	= 3 (x000003)	
Segmenting Reassembling Parameter		
005A More Data Indicator	=0 No more data	
05B Pointer to Mandatory Parameter	= Parm0 offset x01 (1)	
Mandatory Variable Length Parameters	=	
Data	= mandatory parameter	
105C Parameter length	= 20	
105D SCCP user data	= x01001103011C03A0B0D07E0400A0B0D07F02A0B0	
Optional Variable Length Parameters	= None	
=========== GSM Phase2+ Layer =========	== =	
005D Discrimination bit D	=1 DTAP	
DOSE SAPI	=000 Signalling	
005E Control channel identification	= 00 Not Specified	
)05F Message Length	= 17 (x11)	
DTAP Info	= x03011C03A0B0D07E0400A0B0D07F02A0B0	
========= CC Layer =========	=	
CALL ESTABLISHMENT MESSAGE	=	
0060 Protocol Discriminator	=0011 Call control	
0060 Transaction identifier	= 0000 (0)	
)061 Message Type	=000001 ÅLERTING	
Facility	=	
0062 IE Identifier(F)	= 00011100 Facility	
063 Length of Facility	= 3 (x03)	
0064 Facility information	= xAÓBODÓ	
User-user	=	
067 Information Element ID	= 01111110 User-To-User	
068 Length	= 4 (x04)	
1069 Protocol Discriminator	= 00000000 User Specific Protocol	
User-to-User Information	= xA0B0D0	
SS version	=	
06D IE Identifier(SSVI)	= 01111111 SS Version Indicator	
006E IE SS Version Indicator Length	= 2 (x02)	
106F SS version information	= xA0B0	

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 ٠
- MTP3 Layer ٠
- SCCP Layer •
- **RANAP** Layer •
- MM Layer •
- CC Layer •

PacketScan (All-in-One)

(PacketScan (All-in-One) le View Capture Statistics Database Call Detail Records Coi	nfigure Help		<u></u> [
		GoTo	
ev Frame# TIME (Relative)	Len Error Protocols	IP Packet Type	NSAP Operation
			NSAF Operation
1 6 00:00:00.220611	114 Internet IP(IPv4)		
RANAP Layer	=		
RANAP PDU	= CHOICE		
Extensibility Marker	= 0		
Choice Index	= 0		
InitiatingMessage	= SEQUENCE		
ProcedureCode	= INTEGER		
Contents	= 20 id-DirectTransfer		
Criticality	= ENUMERATOR		
Contents	= 1 ignore(1)		
Value	= Open Type		
Length	= 16		
DirectTransfer	= SEQUENCE		
Extensibility Marker	= 0		
Preamble	= 0		
ProtocolIE-Container	= SEQUENCE OF		
Iteration Count	= 2		
ProtocolIE-Container	= Instance O		
ProtocolIE-Field	= SEQUENCE		
ProtocolIE-ID	= INTEGER		
Contents	= 16 id-NAS-PDU		
Criticality	= ENUMERATOR		
Contents	= 1 ignore(1)		
Value	= Open Type		
Length	= 4		
NAS-PDU	= SEQUENCE		
NAS-PDU	= OCTET STRING		
Length Determinant	= 3		
Contents	= x051801		
ProtocolIE-Container	= Instance 1		
ProtocolIE-Field	= SEQUENCE		
ProtocolIE-ID	= INTEGER		
Contents	= 59 id-SAPI		
Criticality	= ENUMERATOR		
Contents	= 1 ignore(1)		
Value	= Open Type		
Length	= 1		
SAPI	= ENUMERATOR		
Extensibility Marker	= 0		
Contents	= 0 sapi-0(0)		
MM Layer	=		
SECURITY MESSAGE	=		
69 Protocol Discriminator	=0101 Mobility management	;	
69 Skip Indicator	= 0000 Valid MM Message		
06A Message Type	=011000 IDENTITY REQUEST		
Identity type	=		
6B Type of identity	=001 IMSI		

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

PacketScan (All-in-One)					
ile <u>V</u> iew Capture <u>S</u> tatistics <u>D</u> atabase Call Detail <u>R</u> ecords <u>C</u> onfig	gure <u>H</u> elp				
= <u>-</u>	🖌 🚮 🎬 💥 🖵 🖓 📴 🛛	GoTo			
Dev Frame# TIME (Relative) Len Erro	r Protocols IP Packet Type		NSAP Operation	STP Message	CLNP
/ 1 4 00:00:00.004942 81	Internet IP(IPv4)				, i i i i i i i i i i i i i i i i i i i
					Þ
00F Delay	=0 Normal Delay				
00F Throughput	=0 Normal Delay				
00F Reliability	= 0 Normal Reliability				
00F Reserved for Future Use	=00 (0)				
D10 Total Length	= 67 (x0043)				
012 Identification	= 35445 (x8A75)				
014 Reserved	= 0				
14 DF	= .0 May Fragment				
014 MF	=O Last Fragment				
014 Fragment Offset	= 0 (00000 00000000)				
D16 Time To Live	= 128 (x80)				
D17 Protocol	= 00010001 User Datagram				
018 Header Check Sum	= x2BEB				
01A Source IP Address	= 192.168.1.84 (xC0A80154)				
01E Destination IP Address	= 192.168.1.165 (xCOA801A5)				
========= UDP Layer =========	=				
022 Source Port	= 2124 (x084C)				
024 Destination Port	= 2123 (x084B)				
026 Length (Header + Data)	= 47 (x002F)				
028 Checksum	= 9289 (x2449)				
eGTP R8 Layer	=				
02A TEID	=1 TEID Present				
02A Piggybacking (P)	=0 No piggybacked mess	sage			
02A Version	= 010 GTP-C				
02B Message Type	= 01000000 Modify Bearer Comma	and			
D2C Length	= 35 (x0023)				
D2E Tunnel Endpoint Identifier	= 1 (x00000001)				
032 Sequence Number	= 0 (x0000)				
APN-Aggregate Maximum Bit Rate (APN-AMBR					
036 Information Element Id	= 01001000 Aggregate Maximum H	Bit Rate	(AMBR)		
037 Length	= 8 (x0008)				
039 Instance	=0000 (0)				
039 Comprehension Required (CR)	= 000 (0)				
Aggregate Maximum Bit Rate-Down Link	= 0 (x00)				
Aggregate Maximum Bit Rate-Up Link	= 0 (x00)				
Aggregate Maximum Bit Rate-Down Link (E					
Aggregate Maximum Bit Rate-Up Link (Ext					
Aggregate Maximum Bit Rate-Down Link (E					
Aggregate Maximum Bit Rate-Up Link (Ext					
AMBR-Specific Data	= x0000				

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

PacketScan (All-in-One)					_0	×
Eile View Capture Statistics Database Call Detail Records Configure	Help					
	r 🐨 	25 z# 歸	0	GoTo		
Dev Frame# Application Identifiers	L	en Er	ror Protocols	Source IP Address	Destination IP Address	
1 10 Application-ID of the S6a/S6d interface application	on 1	78	Internet IP(IPv4)	192.168.1.201	192.168.1.85	
√1 11		62	Internet IP(IPv4)	192.168.1.85	192.168.1.201	
1 12 Application-ID of the S6a/S6d interface application	on 2	62	Internet IP(IPv4)	192.168.1.201	192.168.1.85	-
					•	
SCTP Layer	-					
0022 Source Port Number	= 3868 (x					-
	= 3868 (x					
0026 Verification Tag	= 3888896					
002A Checksum	= 3313050					
002E Chunk Type 002F U bit	= 0000000		unk DATA chunk			
002F 0 bit 002F Beginning/Ending bits	=1					
0030 Length	= 132 (x0		: П			
0032 TSN	= 102 (x0)					
0036 Stream Identifier	= 0 (x000					
0038 Stream Sequence Number	= 1 (x000)					
003A Payload Protocol Identifier	= x000000	2É Undefi	ned			
Diameter Protocol Layer						
003E Version			r Version 1			
003F Length	= 116 (x0	00074)				_
Command Flags:	=					
0042 Request (R)			is Request			
0042 Proxiable (P)			Locally Proc			
0042 Error (E)				ain Protocol Error		
0042 Potentially Retransmitted Message (T) 0043 Command Code				ue to Link Failure ation Request/Answe		
				ation Request/Answe he S6a/S6d interfac		
0048 Application Identifiers	= 0 (x000)		ation-ip of t.	ne stavstu interiac	e application	
004E End To End Identifier	= 0 (x000)					
User-Name	=	,				
AVP Code	= x000000	01 User-N	ame			
AVP Flags	=					
Vendor Specific Bit (V)			ID Field Not 1			
Mandatory Bit (M)			Of AVP Not R	equired		
Encryption For End To End Security (P)	=0		ded			
Reserved (r)	=0000					-
[◄]					•	
Off-line Viewing C:\Program File	esi Gl Communica	tions Inc\P. 26	Frames			
Crimic noming Criterogramming	sayar communice	adono in lutro jeu	ri rumos	J	ļ	_///

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

🕂 Pac	cketScan ((All-in-One)							<
<u>F</u> ile ⊻i	jew Captur	re <u>S</u> tatistics <u>D</u> ata	base (Call Detail <u>R</u> ecords	<u>C</u> onfigure <u>H</u> elp				
	6 18 /		횥 🗖		14 14 set 🚏	💥 🚅 📰 🖸)	GoTo	
Dev	Frame#	TIME (Relative)	Len	Protocols	Source IP Address	Destination IP Address	TCP Source Port	TCP Destination Port (^
$\sqrt{0}$	32	00:00:38,995845	82	Internet IP(IPv4)	192.168.20.75	192.168.1.167	2000	51918	_
V 0	33	00:00:38.996066	78	Internet IP(IPv4)	192.168.20.75	192.168.1.167	2000	51918	
V 0	34	00:00:38,996295	78	Internet IP(IPv4)	192.168.20.75	192.168.1.167	2000	51918	
V 0	35	00:00:38,996508	70	Internet IP(IPv4)	192.168.20.75	192.168.1.167	2000	51918	
V 0	36	00:00:38.996692	66	Internet IP(IPv4)	192.168.20.75	192.168.1.167	2000	51918	~
<								>	
			Clien	t Control H	rotocol Layer			1	^
	Cisco S				=				
						(x14000000)			
003A 003E	Header Messag	Version				(x11000000) CM7 ! (x10010000) Se		ovo Mosoogo	
0032		e lype nstance				x00000000)	SIECT SOLT N	eys nessage	
0046		Identifier				x000000000)			
004A		ey Set Descr:	iptic	n		x00000000) On H	look		
004E	Soft K		-			1 Show			
004E	Soft K					1. Show			
004E	Soft K					1. Show			
004E 004E	Soft K Soft K					.1 Show 1 Show			
004E	Soft K					Show			
004E	Soft K					Don't sho	w		
004E	Soft K				= 1	Show			
004F	Soft K					1 Show			
004F	Soft K					1. Show			
004F	Soft K					1. Show			
004F 004F	Soft K Soft K					.1 Show 1 Show			
004F	Soft K					Show			
004F	Soft K					Show			
004F	Soft K				= 1	Show			¥
<								>	
Off-line	Viewing			E:\packetsc	an\Skinny_Test.hdl	161 Frames			//
						,,			11

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

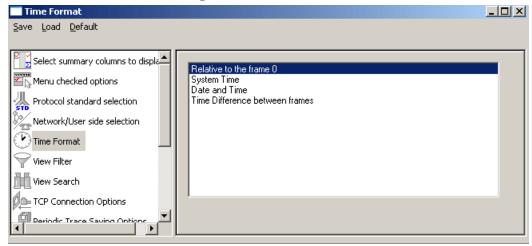


Figure 40: Time Format

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 0:00:0000000. 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 offline 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.

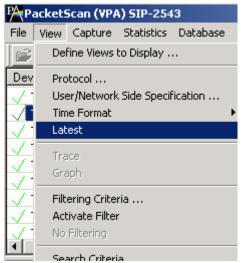


Figure 41: Auto Screen Refresh during Real-time Analysis

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 **Filtering Criteria** icon from the toolbar. The Filter selection dialog is displayed as shown in the figure below:

Filter Selection SIP-2543 SIP-2543 Frame Length OK Frames D Frame Numbe Device Numbe MAC ARP RARP NetWare Internet Logical Link Cont	Dnly nly er Packet E	Frame Length N or Range Min-Max						
All Selected	F 11							
Layer	Field	Filter Value						
Data Link	Frame Length(s)	20						
•								
Conditions for all selections C AND O OR OR C Include C Exclude Deactivate Sel Deactivate All								

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

Pa	cketScan (VPA) SIP-3261					_	
File	View Capture Statistics Database C	all Detail Records	Configure Help				
	Define Views to Display		H, H, 🚮 👬 🙀		Goʻ	Го	
Dev	Protocol	Protocols	IP Packet Type	Source IP Address	Destination IP Address	RTCP Packet Type	
14	User/Network Side Specification	Internet IP(IPv4)	RTCP	192.168.10.45	192.168.10.14	Sender Report SR	
12	Time Format	Internet IP(IPv4)	RTCP	192.168.10.45	192.168.10.14	Sender Report SR	
	Latest	Internet IP(IPv4)	RTCP	192.168.10.14	192.168.10.45	Sender Report SR	
14	Trace	Internet IP(IPy4)	RTCP	192.168.10.14	192.168.10.45	Sender Report SR	
12	Graph	Internet IP(IPv4)	RTCP	192.168.10.45	192.168.10.14	Sender Report SR	
1.	Graph	Internet IP(IPv4)	RTCP	192.168.10.45	192.168.10.14	Sender Report SR	
$\sqrt{1}$	Filtering Criteria	Internet IP(IPv4)	RTCP	192.168.10.14	192.168.10.45	Sender Report SR	
1	Activate Filter	Internet (D((Dud))	סחדם	1021001014	100 100 10 AE	Condor Doport CD	Ľ.
	No Filtering						<u> </u>
Dev - Eth	Search Criteria	17097 OK Len	.=94				-
==	Next		=				
D	Prev		= x000	55D41B6D5			
S.	FIGY			244234B40			
L	Display Trace File Name		= x080	0 Internet IP()	[Pv4)		
	Default Summary Columns		= 0100	(4)			
I I	Invoke Packet Data Analysis	2 bit words		0101 (5)			
Ty	po or opratoo .	1	=				-1
I ∎ [®]	recedence		- 000	Doutino			
Hex	Dump of the Frame Data		<u> </u>				
+	+++++	+	\+	+++			
00 0		4B 40 08 00]A¶Õ D#K@ E			
00 5 0A 2		CO A8 OA OE 81 C8 00 0C	COA8 🖪 7692 -	[+ IæÀ¨ À¨ ≆ <Æî∎È v´			
		00 00 DD 40		ÈIN -OB: Ý@			_
				ant all			<u> </u>
A shine i	- Cilca	DulDur		Thu 10 -6 4020 f			
Activat	e Hiter	D:\Program	h Filesi,GL Communicati	ons Fltr 12 of 4228 fran	nes		

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.

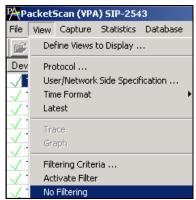


Figure 44: Deactivating Filter

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.

Filter Selection			- ''Y'' fo	r Errored frames only	
🛛 🥰 SIP-3261			Y		
📄 💓 Data Link			P		
🚽 💮 💮 Frame Length	n(s)				
Error Frames Only					
- OK Frames Only					
🔰 💮 💮 Frame Numbe	er(s)				
Device Numb	ber	•			
📄 🖳 MAC					
ARP					
RARP					
NetWare Internet					
📃 🖳 🍉 Logical Link Cont	rol 🔽				
			<i>F</i>	Activate	Deactivate
All Selected					
Layer	Field			Filter Value	
Data Link	Error Frames O	nly		Y	
•					F
Conditions for all selections	s		_		
C AND C OR C	Include C Exc	lude		Deactivate Sel	Deactivate All

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 ¹¹ View Search</sup> button from **Configure > Protocol and GUI Options** Or
- Click I from the toolbar to open search criteria window as shown in the figure below

Save Load Default	
Menu checked options SIP-3261 Protocol standard selection Strame Length(s)	
 Time Format View Filter View Search TCP Connection Options Periodic Trace Saving Options Startup Options All Selected 	ons selection selection selection Selection OK Frames Only Frame Number(s) Device Number Device Number MAC ARP NetWare Internet Packet E Solicial Link Control
Image: Provide state Layer Field Search Value Data Link Frame Length(s) 60	
INI Decode Options	s Conditions for all selections

Figure 46: Setting Search Criteria

6.14 Forward Search and Backward Search

File	View	Capture	Statistics	Database	C
2	Del	fine Views I	o Display		
Dev	Use	otocol er/Network ne Format	Side Specif	ication	•
1:	Lat	est			
× :	Tra Gra	ice aph			
$\overline{\mathbf{v}}$		ering Criter tivate Filter			
$\overline{\langle}$	No	Filtering			
1		arch Criteri	a		
	Ne: Pre				
• Dev			File Name . ary Column		
	Inv	voke Packel	: Data Analy	sis	

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 ¹¹ 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.

Trace File Name	×
C:\Program Files\Gl Communications Inc\PacketScan\Examples\Auto Detect RTP only tests_NO SIP\G.711\Auto detect RTP_G.711-alaw_ATA Router_VAD OFF.HDL	to
OK]	

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:

File	View	Capture	Statistics	Database	C ₁				
	Del	fine Views I	to Display						
Dev		Protocol							
	User/Network Side Specification								
\sqrt{i}		Time Format 🕨 🕨							
\checkmark :	Lat	:est							
\checkmark	Tra	ice							
	Gra	aph							
$ \cdot $					-				
$ \cdot $		ering Crite							
\sim		tivate Filter	r						
	No	Filtering							
$ \cdot\rangle$	Sea	arch Criteri	a						
\leq	Ne:	×t							
	Pre	ev .							
Ľ.	Dis	play Trace	File Name .		-				
Dev	Del	fault Summ	ary Column	s					
	Inv	voke Packe	t Data Anal	/sis					

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

ρ	🅼 📲 🖇	8 🦻	▶ ■	🗎 🖄	SET 🕈	ř 🔳	Sip Calls		Show All 3	Sessions	;	-				
all Su	immary Reg	straton Su	mmary Aler	t Summary												
all #	SSRC	Payload	Packet Received	Conversat MOS/B			Missing Packets/(%)	Duplicate Packets/(%)	Out Of Sequence Packets/(%)	Average Gap(ms)	Average Delav	Average Jitter	Average Inter Arri	Cumulativ Packet		Max/M Delav
Call#	:000001 Calle	r:0001@1:							artTime:2009-05-18 1				-		laab	D oldy
1	55874	PCMU	1355	3.44 /	3.53 /	22 / 1	0 / 0.00	0 / 0.00	0 / 0.00	29.65	0.00	0.00	0	0	3144.4	327-
1	56196	PCMU	6	0.00 / 0	0.00 / 0	070.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	2	0	0.007	0/0
	000002 Calle	r:0001@1	92.168.1.22	3 Callee:000	2@192.16	8.1.48 Call	d:GLPG395630	0962546 Call 9	tartTime:2009-05-18 1	4:35:13.000)581 Call Du	ration: 00:0	00:01.00054	6		
2	42949	PCMU	0	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0
2	55629				0.00 / 0		0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0
				3 Callee:000	12@192.16	8.1.48 Calli	d:GLPG408927		tartTime:2009-05-18 1				00:25.00001	1		
3	55999	PCMU	1084	4147	4.16 /	8/074	0 / 0.00	0 / 0.00	0/0.00	20.03	0.00	0.00	Ω	0	35.46	57.5
10	55550	T ON O	1004	4.147	1.101	070.14	070.00	01 0.00	070.00	20.03	0.00	0.00	0	U	33.40	375
Ľ		1 0010	1004	4.147		070.14	07 0.00	01 0.00	070.00	20.03	0.00	0.00		0	55.40	
	33330	10110	1004	T. I T 7		Active		010.00		20.00	0.00	Counter		0	Counte]
									070.00	20.03	0.00	Counter		0]
			1004							20.03		Counter Total Par Total Cal	Type cket Count Is		Counte 23331 15]
	1											Counter Total Par Total Cal Active Ca	Type cket Count Is alls		Counte 23331 15 0]
	1											Counter Total Par Total Cal Active Ca Complete	Type cket Count lls alls ed Calls		Counte 23331 15 0 13	J
	1											Counter Total Par Total Cal Active Ca Complete Purged C	Type cket Count ls alls ed Calls Calls(Comple		Counte 23331 15 0 13 0	
Calls	1											Counter Total Par Total Cal Active Ca Complete	Type cket Count ls alls ed Calls Calls(Comple		Counte 23331 15 0 13	J
of Calls	1											Counter Total Par Total Cal Active Ca Complete Purged C	Type cket Count ls alls ed Calls Calls(Comple alls	ted)	Counte 23331 15 0 13 0	J
Calls	1											Counter Total Par Total Cal Active Ca Complete Purged C Failed Ca Counter	Type cket Count ls alls ed Calls Calls(Comple alls	ted)	Counter 23331 15 0 13 0 2 Counters	J
of Calls	1											Counter Total Par Total Cal Active Ca Complete Purged C Failed Ca Counter	Type cket Count ls alls ed Calls Calls(Comple alls Yppe Packets	ted)	Counte 23331 15 0 13 0 2	J
No of Calls			ſ			Active	Calls					Counter Total Par Total Cal Active Ca Complete Purged C Failed Ca Failed Ca Counter Total SIP SIP Calls SIP Activ	Type cket Count ls alls cd Calls Calls(Comple alls Type P Packets re Calls	ted)	Counter 23331 15 0 13 0 2 2 Counters 123 15 0	J
Calls	1											Counter Total Par Total Cal Active Ca Complete Purged C	Type cket Count ls alls ed Calls Calls(Comple		Co 23 15 0 13 0	ounte 3331 5
of Calls	1											Counter Total Par Total Cal Active C Complete Purged C Failed Ca Counter Total SIF SIP Calls	Type cket Count ls alls ed Calls Calls(Comple alls Type P Packets	ted)	Counter 23331 15 0 13 0 2 2 Counters 123 15	
of Calls	1											Counter Total Par Total Cal Active C Complete Purged C Failed Ca Counter Total SIF SIP Calls	Type cket Count ls alls ed Calls Calls(Comple alls Type P Packets	ted)	Counter 23331 15 0 13 0 2 2 Counters 123 15	
No of Calls			ſ			Active	Calls		14:49:09 14:49:56 1			Counter Total Par Total Cal Active Ca Complete Purged C Failed Ca Failed Ca Counter Total SIP SIP Calls SIP Activ	Type cket Count ls alls ad Calls calls(Comple alls Type P Packets re Calls pleted Calls	ted)	Counter 23331 15 0 13 0 2 2 Counters 123 15	

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.

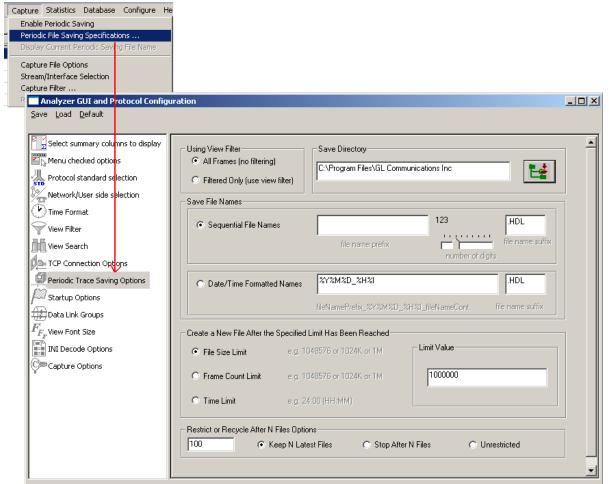


Figure 51: Periodic File Saving Specifications

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.

Capture Menu Features

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

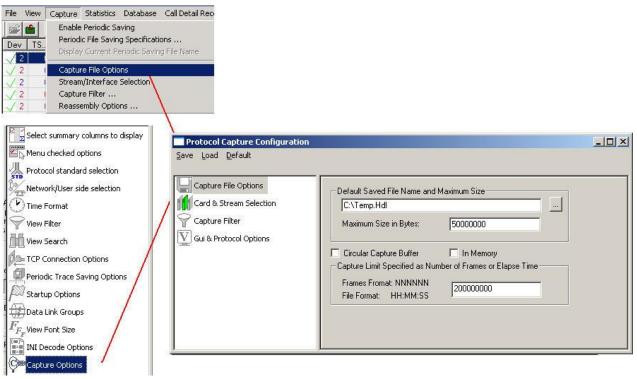


Figure 52: Capturing Options

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 in 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** Trom the toolbar.

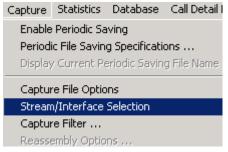


Figure 53: Setting the Capturing option

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.

Card & Stream Selection		
<u>S</u> ave <u>L</u> oad <u>D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Capture Filter	Stream / Interface Selection Ethernet Boards Generic dialup adapter NDIS 5.0 driver 192.168.10.21	

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.

🔠 Capture Filter		
<u>S</u> ave Load <u>D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Capture Filter Capture Filter	Capture Filters Filter Selection Filter Selection MAC MAC MAC MAC MAC MAC SIP STP STP MGCP MGCP MGCP MGCP MGCACO MGCA	Filters

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.

👯 Capture Filter		
<u>Save Load D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Gui & Protocol Options	Capture Filters Filter Selection MAC MAC <	
		1
	4	

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.

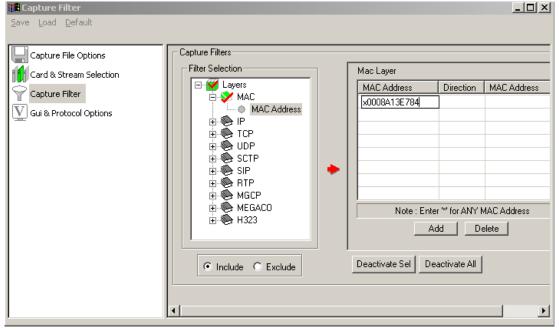


Figure 57: MAC Address

7.4.2 IP

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

Capture Filter			<u>- 0 ×</u>
<u>Save Load D</u> efault			
Capture File Options Card & Stream Selection Capture Filter Capture Filter Gui & Protocol Options	Capture Filters Filter Selection Filter Selection Avers MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection Filter Selection MAC Filter Selection Filter Sel	Filters Filter all IP data Reassemble IP Datagrams Deactivate Sel	
	4		•

Figure 58: IP Layer

If the machine where **PacketScanTM** 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.

Capture Filter					
Save Load Default					
Save Load Default	Capture Filters Filter Selection Cayers Cayers Cayers Cayers Capture Filters Capture Filters Filter Selection Capture Filters Filter Selection Filter Selection Filt	IP Layer IP Address 2001:FF01::FD0D:5606:3DF0:2BF8:8052 ↓ 192:168:1.56 ↓ Note : Ente Add	Direction > r ^{**} for ANY I dDel	IP Address 2001:FF01::FD0D:5606:3DF0:2BF8:8056 192.168.1.78 P Address ete	
	Include C Exclude	Deactivate Sel Deactivate All			-
•	•				

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.

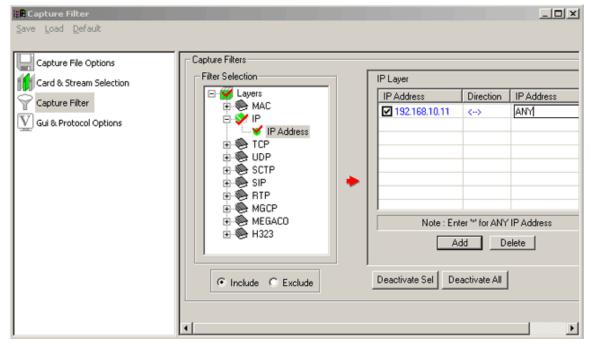


Figure 60: ANY IP Address

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.

📲 Capture Filter		
Save Load Default		
Capture File Options Card & Stream Selection Capture Filter	Capture Filters Filter Selection Filter Selection Filter Selection MAC How MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection Filter Selection	Filters ↓ Filter all TCP data
	C Include C Exclude	Deactivate Sel Deactivate All
	•	

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.

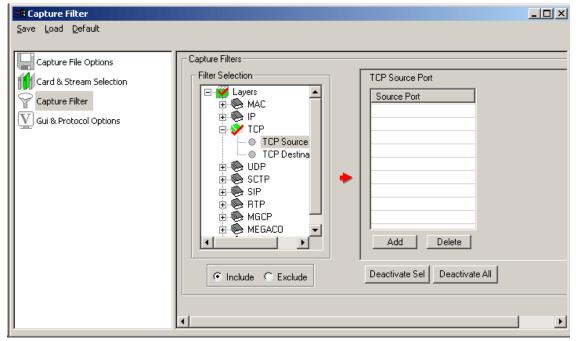


Figure 62: TCP Source and Destination Port

7.4.4 UDP

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

👯 Capture Filter		<u>_0 ×</u>
Save Load Default		
Capture File Options Card & Stream Selection Capture Filter Capture Filter Capture Filter	Capture Filters Filter Selection Cayers Cayers Cayers Cayers MAC Cayers MAC Cayers MAC Cayers MAC Cayers MAC Cayers MAC Cayers MAC Cayers MAC Cayers MAC Cayers MAC Cayers MAC Cayers SIP Cayers SIP Cayers SIP Cayers MGCP Cayers MGCC Cayers MAC Cayers Caye	Filters
		Deactivate Sel Deactivate All

Figure 63: UDP Layer

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

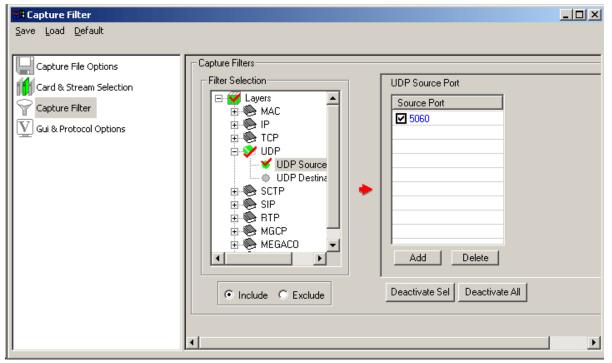


Figure 64: UDP Source and Destination Port

7.4.5 SCTP

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

Capture Filter		
<u>Save Load D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Sui & Protocol Options	Capture Filters Filter Selection Filter Selection MAC Filter Selection Filter S	Filters ☐ Filter all SCTP data
	● Include C Exclude	Deactivate Sel Deactivate All
	[•]	

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.

Capture Filter		<u>_ D ×</u>
<u>S</u> ave Load Default		
Capture File Options Card & Stream Selection Capture Filter	Capture Filters Filter Selection Layers MAC MAC Source Port Source Port Source Port Source Port Source Port Source Port Add Delete Deactivate Sel Deactivate All	

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.

Capture Filter Save Load Default		
Capture File Options Card & Stream Selection Capture Filter Capture Filter Capture Filter	Capture Filters Filter Selection Image: Selection	

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.

Capture Filter		_ D ×
<u>Save Load Default</u>		
Capture File Options Card & Stream Selection Capture Filter Capture Filter Capture Filter	Capture Filters Filter Selection MAC MAC MAC TCP UDP SIP MGCP MEGACO H323 Add Deactivate Sel Deactivate All	

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.

Capture Filter		
<u>S</u> ave Load <u>D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Capture Filter Cau & Protocol Options	Capture Filters Filter Selection Filter Selection MAC MAC TCP TCP TOP SCTP SSIP MGCP MGCP MGCP MEGACO H323 Include Exclude Deactivate Sel Deactivate All	

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 <u>PacketGen[™]</u> (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.

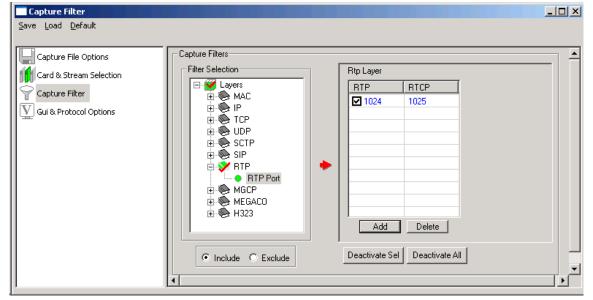


Figure 70: RTP Port

7.4.8 MGCP

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

Capture Filter		
<u>Save Load D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Capture Filter Capture Filter	Capture Filters Filter Selection Image: Selection <	

Figure 71: MGCP Layer

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

Capture Filter	_ 🗆 ×
Save Load Default	
Capture File Options Card & Stream Selection Capture Filter Capture Filter Capture Filter Capture Filter Capture Filter Capture Filters Filter Selection Capture Filters Filter Selection Capture Filters Filter Selection Capture Filters Filter Selection Capture Filters MAC C C C C C C C C C C C C C	

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.

Capture Filter		<u>- 0 ×</u>
<u>Save Load D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Capture Filter Gui & Protocol Options	Capture Filters Filter Selection Image: Selection <	

Figure 73: MEGACO Layer

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

Capture Filter		
<u>S</u> ave <u>L</u> oad <u>D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Gui & Protocol Options	Capture Filters Filter Selection Filter Selection MAC MAC Filter Selection Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection MAC Filter Selection Filter Selecti	MEGACO Binary Binary Diagonal

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.

Capture Filter		_ 🗆 🗡
<u>S</u> ave Load <u>D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Capture Filter Cau & Protocol Options	Capture Filters Filter Selection Image: Selection <	

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:

Capture Filter		<u>_ × - ×</u>
Capture Filer Save Load Default	Capture Filters Filter Selection IP IP <	
	BAS Port Include C Exclude Deactivate Sel Deactivate All	

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:

2 3 00.000.00.002632 691 Internet IP(IPv4) 192.168.1.233 192.168.1.235 SIP 54098 2 4 00:00:00.003282 389 Internet IP(IPv4) 192.168.1.235 192.168.1.233 SIP 54098 2 5 00:00:00.002242 214 Internet IP(IPv4) 192.168.1.235 192.168.1.233 RTP 1024 2 6 00:00:00.002397 214 Internet IP(IPv4) 192.168.1.233 192.168.1.235 RTP 1024 2 8 00:00:00.002397 214 Internet IP(IPv4) 192.168.1.233 192.168.1.235 RTP 1024 2 8 00:00:00.002632 OK Len=691 192.168.1.235 RTP 1024 Evoloce Frame=3 at 00:00:00:00.002632 OK Len=691 Chayer = Destination Address = x001320E21520 Source Address = > UPU of the Frame Data = Internet PI(Pv4) = <td cols<="" th=""><th>Packet</th><th>tScan (VP</th><th>A) 5IP-2543</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>_ []</th></td>	<th>Packet</th> <th>tScan (VP</th> <th>A) 5IP-2543</th> <th></th> <th>_ []</th>	Packet	tScan (VP	A) 5IP-2543														_ []
Dev Frame# TIME (Relative) Len Error Protocols Source (P Address Destination (P Address IP Packet Type UDP Source 12 3 0000000002652 651 Internet (P(Pv4) 1921681.233 1921681.233 SIP 54098 2 4 000000002322 389 Internet (P(Pv4) 1921681.235 1921681.233 SIP 54098 2 6 000000002327 214 Internet (P(Pv4) 1921681.235 1921681.235 RTP 1024 2 7 000000003397 214 Internet (P(Pv4) 1921681.235 1921681.235 RTP 1024 2 7 000000003403 214 Internet (P(Pv4) 1921681.235 1921681.235 RTP 1024 2 7 00000003403 214 Internet (P(Pv4) 1921681.235 RTP 1024 2 7 00000003403 214 Internet (P(Pv4) 1921681.235 RTP 1024 2 7 0000000030 2163<	<u>File V</u> iew	Capture	Statistics Dat	tabase (Call Detail <u>R</u>	ecords (<u>C</u> onfigure	<u>H</u> elp										
2 3 00000000282 691 Internet IP(IPv4) 1921681.233 1921681.235 SIP 54098 2 4 000000003282 389 Internet IP(IPv4) 1921681.235 1921681.233 SIP 54098 2 5 0000000022835 214 Internet IP(IPv4) 1921681.235 1921681.235 RTP 1024 2 7 000000023937 214 Internet IP(IPv4) 1921681.235 1921681.235 RTP 1024 2 7 000000023937 214 Internet IP(IPv4) 1921681.235 1921681.235 RTP 1024 2 8 000000023937 214 Internet IP(IPv4) 1921681.235 1921681.235 RTP 1024 2 8 000000023937 214 Internet IP(IPv4) 1921681.235 RTP 1024 1024 1025 114 Internet IP(IPv4) 1921681.235 RTP 1024 1024 1921681.235 Internet IP(IPv4) 1921681.235 RTP 1024 1025 Internet IP(IPv4) 1921681.235 Internet IP(IPv4) 19	📽 🗳	1 🦉	0. 🖉 🎴	E			4 92	SET 🖷	* 🕱 🛛 z	Ç 🚚 🔒	a 0			GoT	`o			
2 4 00:00:00:003282 383 Internet IP(IPv4) 192:168.1.235 192:168.1.233 SIP 54098 2 5 00:00:00:0023895 214 Internet IP(IPv4) 192:168.1.235 192:168.1.233 RTP 1024 2 6 00:00:00:00:23937 214 Internet IP(IPv4) 192:168.1.235 192:168.1.235 RTP 1024 2 8 00:00:00:00:00:00:00:00:00:00:00:00:00:	Dev	Frame#	TIME (F	Relative)	Len	Error P	rotocols		Sourc	e IP Addr	ess 🛛 🛛	Destination	IP Addre	ss IP	Packet Ty	vpe l	UDP Source	
2 5 00.00.00.004224 214 Internet IP(IPv4) 192.168.1.235 192.168.1.233 RTP 1024 2 6 00.00.00.023995 214 Internet IP(IPv4) 192.168.1.235 192.168.1.235 RTP 1024 2 7 00.00.00.023937 214 Internet IP(IPv4) 192.168.1.235 192.168.1.235 RTP 1024 2 8 00.00.00.034303 214 Internet IP(IPv4) 192.168.1.235 192.168.1.235 RTP 1024 evoice2 Frame=3 at 00:00:00.00.02632 OK Len=691 1124 Internet IP(IPv4) 192.168.1.235 RTP 1024 evoice2 Frame=3 at 00:00:00.00.02632 OK Len=691 1124 Internet IP(IPv4) 192.168.1.235 RTP 1024 evoice2 Total Address = ×001320E21520 = ×0011320E21520 = ×0011116AF6D7 = = = 0100 (4) = = 1010 (4) = = 01011 (5) = 0101 (5) = 0101 (5) = 0101 (5) = 0101 (5) = 0101 (5)	$\sqrt{2}$	3	00:00:00.	.002632	691	In	iternet IP(IPv4)	1	32.168.1.2	233	19:	2.168.1.2	35	9	SIP	54098	
2 6 000000023895 214 Internet IP(IPv4) 192168.1.233 192168.1.235 RTP 1024 2 7 0000000023937 214 Internet IP(IPv4) 192168.1.235 192168.1.235 RTP 1024 2 8 0000000023937 214 Internet IP(IPv4) 192168.1.235 192168.1.235 RTP 1024 2 8 0000000043403 214 Internet IP(IPv4) 192168.1.235 192168.1.235 RTP 1024 4	V 2	4	00:00:00.	.003282	389	In	iternet IP(IPv4)	1	92.168.1.2	235	19:	2.168.1.2	33	9	SIP	54098	
1 7 00:00:00:00:3937 214 Internet IP(IP∨4) 192:168.1.235 192:168.1.233 RTP 1024 1 2 8 00:00:00:043403 214 Internet IP(IP∨4) 192:168.1.235 192:168.1.235 RTP 1024 1	V 2	5	00:00:00	.004224	214	In	iternet IP(IPv4)	1	92.168.1.2	235	193	2.168.1.2	33	R	TP	1024	
2 8 00:00:00:043403 214 Internet IP(IPv4) 192:168.1.233 192:168.1.235 RTP 1024 Device2 Frame=3 at 00:00:00:00:00:00:00:00:00:00:00:00:00:	V 2	6	00:00:00	.023895	214	In	iternet IP(IPv4)	1	92.168.1.2	233	193	2.168.1.2	35	B	TP	1024	
evice2 Frame=3 at 00:00:00.002632 OK Len=691 thernet Frame Data Destination Address = x001320E21520 Source Address = x0011116AF6D7 Length/Protocol Type = x0800 Internet IP(IPv4) ========= IP Layer ===== Version = 0100 (4) Internet Header Length (In 32 bit words) =0101 (5) Tvpe of Service = Version = 0100 (4) Internet Header Length (In 32 bit words) =0101 (5) Tvpe of Service = Version = 0100 (4) Ithernet Header Length (In 32 bit words) =0101 (5) Tvpe of Service = Version = 0100 (4) Ithernet Header Length (In 32 bit words) =0101 (5) Tvpe of Service = Ite Das 22 13 C4 02 91 22 3D 53 49 50 2F 32 2E eOR Å ''=SIP/2. 0 232 30 30 20 4F 4B 0D 0A 56 69 61 3A 20 53 0 200 OK Via: S 9 50 2F 32 2E 30 2F 55 44 50 20 31 39 32 2E 31 IP/2.0/UDP 192.1 Iterme Count(Device #) III Frame Count(Error Code) Iterme Count(Device #) III Frame Count(Error Code) Iterme Count(Device #) <t< td=""><td>V 2</td><td>7</td><td>00:00:00.</td><td>.023937</td><td>214</td><td>In</td><td>iternet IP(</td><td>IPv4)</td><td>1</td><td>92.168.1.2</td><td>235</td><td>193</td><td>2.168.1.2</td><td>33</td><td>B</td><td>TP</td><td>1024</td></t<>	V 2	7	00:00:00.	.023937	214	In	iternet IP(IPv4)	1	92.168.1.2	235	193	2.168.1.2	33	B	TP	1024	
Device2 Frame=3 at 00:00:00.002632 OK Len=691 Cthernet Frame Data ====== MAC Layer Destination Address Source Address Source Address Source Address ======= Internet IP Layer Version Internet Header Length (In 32 bit words) Tvoe of Service ====== Version 0 13 20 E2 15 20 00 11 11 6A F6 D7 08 00 45 00 12 A5 AB 6E 00 00 80 11 07 B5 C0 A8 01 E9 C0 A8 ¥ <mt td="" ´="" µå="" éå`<="" €=""> ½ A5 AB 6E 00 00 80 11 07 B5 C0 A8 01 E9 C0 A8 19 50 27 32 2E 30 2F 55 44 50 20 31 39 32 2E 31 IP/2.0./UDF 192.1</mt>	V 2	8	00:00:00.	.043403	214	In	iternet IP(IPv4)	1	92.168.1.2	233	193	2.168.1.2	35	R	TP	1024	
Internet Frame Data =	•																•	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	Inter Tvpe	net Hea of Serv	vice	`	32 bit	words))										Þ	
12 A5 AB 6E 00 00 80 11 07 B5 C0 A8 01 E9 C0 A8 \neq cn \notin μ Å'' \neq Å'' <t< td=""><td>1ex Dum </td><td>ιρ οι τι +-</td><td>ne Frame Da</td><td>ata -+</td><td></td><td>+</td><td></td><td></td><td>++-</td><td>+</td><td>+</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	1ex Dum 	ιρ οι τι +-	ne Frame Da	ata -+		+			++-	+	+							
2 0 2511 2511 otal 2 Total 2511	02 A5 AB 6E 00 00 80 11 07 B5 C0 A8 01 E9 C0 A8 ¥<∩ € µÅ` éÅ` 01 EB D3 52 13 C4 02 91 22 3D 53 49 50 2F 32 2E ëÓR Ä ´ "=SIP∕2. 30 20 32 30 30 20 4F 4B 0D 0A 56 69 61 3A 20 53 0 200 OK Via: S																	
2 0 2511 2511 otal 2 Total 2511	- Dow	ioo 44 🛛 🗖	Error Code		romo Court	/Douise 4	a 🗔	Exome	Count/Erro	r Codo								
otal 2 Total 2511 2511			Error Code		rame count	(Device #	/	Frame	Count(Erro	r code)								
		*	4-1															
	iotal 2	10	tai	2511			2511											
					5			-								_		

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**.

	evice # ror Code otocol Flag me Stamp fl estination Address hernet Encoded TF ength/Protocol Type jority Value purce Address AN ID are Internet Packet	PIDe	Ethernet Encoded TPID Use Type (single selection) Total Key Field Statistic Type(s) (calculated, Frame Count Frame Percent Byte Count Byte Percent Value Set V LAN (802.1Q) C Cumulative C Separ Add/Mod Remove	
Layer	Field Name	Use Type	Statistic Type	Remove Sel
Discusional		Total		
Physical	Error Code	Key	Frame Count	Remove All
Physical Physical MAC	Ethernet Enco	Total	Frame Count	

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^M and the field for respective layers will be displayed as shown in the figure below:

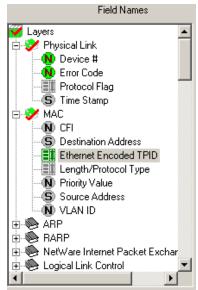


Figure 79: Selecting Filed Names

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.

tistics			×	
Field Names	Γ	Time Stamp - Use Type (single selection)		
/ Layers	_	Total Key		
Device # Error Code		Field		Numeric
S Time Stamp		Statistic Type(s) (calculated,	multiple selection)—	String
MAC CFI S Destination Address		Frame Count Frame Percent Byte Count Byte Percent		String
Ethernet Encoded TF Length/Protocol Type N Priority Value		Wildcard (*,?)		Enumerat
N VLAN ID ARP RARP NetWare Internet Packet	Exchar	Cumulative Separ	ate	
🤊 😓 Logical Link Control	• •	Add/Mod Remove		
Selected Statistic Information —				
Layer Field Name	Use Type	Statistic Type	Remove Sel	
Physical Device # MAC Ethernet Enco Pluminal Time Charge	Total Total Total	Frame Count	Remove All	
Physical Time Stamp	rotar		1 Apply	

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 <u>Classifying Fields</u> <u>under Field Names</u> 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)

Ethe Ethe Constant Constant	ce # Code Stamp ination Address met Encoded TP th/Protocol Type ty Value ce Address N ID Internet Packet ink Control		Ethernet Encoded TPID Use Type (single selection) – Total Key Field Statistic Type(s) (calculated, Frame Count Frame Percent Byte Count Byte Percent Value Set V LAN (802.1Q) C Cumulative © Sepa [Add/Mod] Remove	•
Layer F	ield Name	Use Type	Statistic Type	Remove Sel
)evice #	Total		
		Kau	Frame Count	Bemove All
Physical E	fror Code thernet Enco	Key Total	Frame Count	Hemove Air

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.

Statistics	<u>×</u>
Field Names Field Names Physical Link Protocol Flag Fror Code Protocol Flag From Stamp MAC ARP NetWare Internet Packet Exchar Decical Link Control Internet Datagram Protocol DECnet Routing Protocol DECNet Local Area Transport <lat:< td=""> DECNet MOP Dump/Load DECNet MOP Remote Console DEC Local Area System Transport DEC Local Area System Transport</lat:<>	Protocol Flag Use Type (single selection) Total Key Field Statistic Type(s) (calculated, multiple selection) Frame Count Frame Percent Byte Count Byte Percent Byte Percent Value Set RTCP RTP SIP
Layer Field Name Use Type Physical Protocol Flag Key	Statistic Type Frame Count Remove All Apply

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:

		PA) SIP-3261	c b					_ 🗆 ×
Eile View	v Captur			etail <u>R</u> ecords Configure	e <u>H</u> elp Sã ₩ ※ -5 -2	to O	GoTo	
Dev	Fra	TIME (Relative)	Len	Protocols	Source IP Address	Destination IP Address	IP Packet T	NSAP 🔺
√2	0	00:00:00.000000	807	Internet IP(IPv4)	192.168.10.45	192.168.10.14	SIP	
V 2	1	00:00:00.071193	60	Internet IP(IPv4)	192.168.10.14	192.168.10.45	RTP	
V 2	2	00:00:00.071331	60	Internet IP(IPv4)	192.168.10.14	192.168.10.45	RTP	
V 2	3	00:00:00.071379	60	Internet IP(IPv4)	192.168.10.14	192.168.10.45	RTP	
🗸 2	4	00:00:00.071694	114	Internet IP(IPv4)	192.168.10.14	192.168.10.45	RTCP	
🗸 2	5	00:00:00.082744	782	Internet IP(IPv4)	192.168.10.14	192.168.10.45	SIP	
🗸 2	6	00:00:00.187621	58	Internet IP(IPv4)	192.168.10.45	192.168.10.14	RTP	
🗸 2	7	00:00:00.187805	58	Internet IP(IPv4)	192.168.10.45	192.168.10.14	RTP	
∢(^			50	1	100,100,10,45	100,100,10,11	575	Þ
🤶 Pro	tocol Flag	🛛 🔝 Frame Count(P	rotocol I	Flag)				
SIP (1)		10						
RTCP (2)		29						
RTP (3)		4157						
			[D:\Program Files\GL Con	nmunication 4228 Frames			/

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.

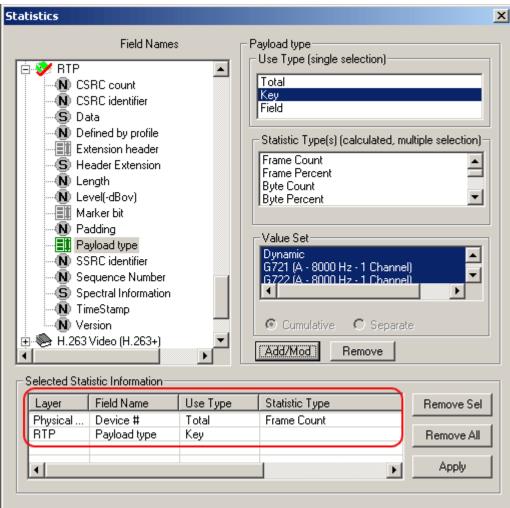


Figure 84: Define Statistics with a Total & Key UT

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

PacketS	APacketScan (VPA) SIP-3261										
<u>F</u> ile ⊻iew	· ·										
🖻 🖆	1 🖉	🗢 🖉 🌄 🏹			86 88 ⁴ 81	4 sei	; 📽 🕱 🛃 🔛	a 0	GoTo		
Dev	Fram	TIME (Relative)) Le	n Error	Protocols		Source IP Address	Destination IP Addre	ss 🛛 RTP Payload Type 🛛 🔺		
√2	12	00:00:00.231749	9 21	4	Internet IP(I	Pv4)	192.168.10.45	192.168.10.1	14 PCMU (A - 8000 Hz		
V 2	13	00:00:00.232040) 21	4	Internet IP(I	Pv4)	192.168.10.45	192.168.10.1	14 PCMU (A - 8000 Hz		
✓ 2	14	00:00:00.249136	6 44	5	Internet IP(I	Pv4)	192.168.10.45	192.168.10.1	4		
V 2	15	00:00:00.251055	5 21	4	Internet IP(I	Pv4)	192.168.10.45	192.168.10.1	4 PCMU (A - 8000 Hz		
√ 2	16	00:00:00.271147	21	4	Internet IP(I	Pv4)	192.168.10.45	192.168.10.1	14 PCMU (A - 8000 Hz		
√ 2	17	00:00:00.291388	3 21	4	Internet IP(I	Pv4)	192.168.10.45	192.168.10.1	14 PCMU (A - 8000 Hz		
V 2	18	00:00:00.311290) 21	4	Internet IP(I	Pv4)	192.168.10.45	192.168.10.1	14 PCMU (A - 8000 Hz 🔤		
▲	10	00-00-00 220460	21	A	Internet ID(I	D()	102 100 10 AE	107 100 10 1			
Device	e# 🢡	Payload type	E F	Frame Coun	t(Device #)						
2	PC	MU (A - 8000	2725								
2	Re:	served (A) (19)	30								
2	Dyi	namic (105)	1402								
total 2	Tot	al	4157								
,				D:\Prog	ram Files\GL	Commu	nicatior 4228 Frames				

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.
- 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.

tatistics	
Field Names Field Names Field Names Field Names Field Na	Source Port Use Type (single selection) Total Key Field
Checksum N Checksum Destination Port N Length (Header + Data) Source Port TCP GRE (Generic Routing Encapsula	Statistic Type(s) (calculated, multiple selection) Frame Count Frame Percent Byte Count Byte Percent
GRE IP GRE IPV6 GRE IPV6 WiMAX USPS Protocol Semicle Procedure Call	Range List
AppleTalk Transaction Protocol F Apple	Cumulative Separate
Selected Statistic Information	Statistic Type Remove Sel
Physical Protocol Flag Total UDP Source Port Field	Frame Count Remove All
	Apply

Figure 86: Define Statistics with a Total and Field UT

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

PAP	acketS	5can ((VPA) S	IP-3261							_ 🗆 🗵
File	⊻iew	Capt	ture <u>S</u> ta	atistics	<u>D</u> atabase – Call Detail <u>R</u> ec	:ords <u>⊂</u> on	figure <u>t</u>	<u>H</u> elp			
	É	-	<u>a</u> t C	ا 🖳 (99 98, S	Hu sei	🌋 🛫 z		GoTo	
Dev	T	Slot	SubCh	Fram	TIME (Relative)	Len	Error	Protocols	UDP Source P	UDP Destination Port	Sour 🔺
	2	0	0	0	00:00:00.000000	807		Internet IP(IPv4)	5060	5060	1
	2	1	0	1	00:00:00.071193	60		Internet IP(IPv4)	8432	6146	1
	2	1	0	2	00:00:00.071331	60		Internet IP(IPv4)	8432	6146	
√:	2	1	0	3	00:00:00.071379	60		Internet IP(IPv4)	8432	6146	1
$ \checkmark$	2	0		4	00:00:00.071694	114	Dec	Internet IP(IPv4)	8433	6147	1
$ \checkmark$	2	0	0	5	00:00:00.082744	782		Internet IP(IPv4)	5060	5060	1
$ \checkmark$	2	1	0	6	00:00:00.187621	58		Internet IP(IPv4)	6146	8432	1-
											►
Σ	Protoc	col Fla	eg [Fram	ne Count(Source Port)						
SIP	(1)		10)							
total	SIP (1)		10)							
RTP	(3)		1:	809							
total	RTP (3))	1:	809							
ľ					D:\Prog	ram Files\Gl	. Commu	nicatior 4228 Frame	s		

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.

 Statistic Type(s) (calculated, multiple select 	tion) –
Frame Count	•
Frame Percent Byte Count	
Byte Percent	-
– Range List	
1 12 15 4 0	_
1 12-15 4-6	
C Cumulative C Separate	
Add/Mod Remove	

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.

Statistic Type(s) (calculated, multiple selection)
Frame Count
Frame Percent
Byte Percent
- Range List
301*5?4*
🔿 Cumulative 💿 Separate
Add/Mod Remove

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.

Statistic Type(s) (calculated, multiple selection)
Current Bytes/Sec
MAX Frames/Sec
MAA bytes/sec
Value Set
Information
Supervisory
Unnumbered
J
Cumulative C Separate
Add/Mod Remove

Figure 90: Specifying Value Sets

8.1.5 Modifying and/or removing configured statistics

Layer	Field Name	Use Type	Statistic Type	Remove Sel
	Device #	Total		
Physical	Time Stamp	Field	Frame Count	Remove All
•				Apply

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 dialogue 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.

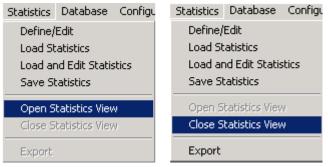


Figure 92: Opening and Closing Statistics View

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).

Open	?×
Look <u>i</u> n: 🗀	PacketScan 🔽 🖛 🗈 💣 🎟 -
Docs Examples hlp Release No Statistics Video	Captsip sipProt sipProtCallTrace sipProtStatistics TfAnCfg
File <u>n</u> ame:	sipProt <u>O</u> pen
Files of <u>type</u> :	Statistic Definition Files (*.ini)
	Open as read-only

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).

Save As		? ×
Save jn: 🔂	G711_alaw 💌 🖛 🛍 📸 📰 🗸	
🐻 G711.ini		
File <u>n</u> ame:	G711.ini <u>S</u> ave	•
Save as <u>t</u> ype:	Statistic Definition Files (*.ini)	el

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.

Save As					? ×
Save jn: 🔂	G711_alaw	•	← 🗈	💣 🎟 •	
File <u>n</u> ame:			_	<u>S</u> av	e
	p Chabialia Europet Eilea (* 440)		-	Cano	_
Dave as type.	Statistic Export Files (*.sef)		<u> </u>	Cano	

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.

	etScan (All-in-Or									_ 8
ile Vie	w Capture Stat	istics Databas	e Call Detail Records C							
r 🖉						GoTo				
Dev	Fr	ame# TIME (Len Err	or Protocols	IP Packet T	ype	NSAP Operation	STP Message	CLNP Message
/1		0 00:00:		845	Internet IP(IPv4)	SIP				
1		1 00:00:		829	Internet IP(IPv4)	SIP				
(1		2 00-00-		000	Internet (D((Dr.d))	CID				F
			0.000000 OK Len=	845						
	et Frame Da			127						
	estination			- = x386077DF0	150					
					77.50					•
ex Du	mp of the F	rane Data	l	755 772	11. 11.					
8 60	77 DF C1 50	38 60 77	DF C8 81 08 00	45 00 8`wßáP8'	++ wßÈ Е					
3 3F	3F 6E 00 00	80 11 00	00 CO A8 01 71	C0 A8 ??n €	A' gA'					
				54.45 äÓRÄ-	AINVITE					
0 73 9 2F	69 70 3A 30 31 2F 32 32	30 30 31	40 31 39 32 2E	31 36 sip:000 30 00 8 1 228	1@192.16 STP/2 0					
IIID	Call Status	Protocol	Call Originating (Nu	. Call Destination (Nur	nb Call Star	t Date & Time	Call Duration			Protocol Specific Inf
)	Completed	SIP	0001@192.168.1.11:		228 2013-03-04 15	:10:01.470458	00:00:05.408	<sipcaliid> GLPG60</sipcaliid>)537502438375 < Release Cau	ise> Normal Call Clearin
	Completed	SIP	0001@192.168.1.11			10:07.910354			181502438381 <release cau<="" td=""><td></td></release>	
2	Completed	SIP	0001@192.168.1.11				00:00:01.541		691502438387 <release cau<="" td=""><td></td></release>	
3	Completed	SIP	0001@192.168.1.11				00:00:05.110		3466602438393 < Release Cau	
4	Failed	SIP	0001@192.168.1.11				00:00:57.363		> GLPG69945602438399 <re< td=""><td></td></re<>	
5	Failed	SIP	0001@192.168.1.11				00:00:32.374		444502438402 <release cau<="" td=""><td></td></release>	
6	Failed Active	SIP	0001@192.168.1.11				00:00:17.384	<sipcaliid> GLF</sipcaliid>	PG73943502438405 <release< td=""><td>Cause> Not Acceptabl D> GLPG7568170243840</td></release<>	Cause> Not Acceptabl D> GLPG7568170243840
(Active	SIP	0001@192.168.1.11	3 0001@192.168.1	228 2013-03-04 15	012:32.910904	00:00:00.002		<sipcallit< td=""><td>J> GLPG/5681/0243840</td></sipcallit<>	J> GLPG/5681/0243840
					-					
	ate : 0.01 Mbps			C:\Temp.H	जी		Captured 1 409	ferman	Missed Frames : 0	

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.

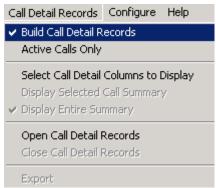


Figure 97: Build Call Detail Record

9.2 Active Calls Only

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

<u> </u>		PA) SIP-3			Call Detail Rec		C 61	Uala								_ 5	<u>1</u> >
File Vie				10ase (neip 🚰 🚟 🖇	8 -4 :			Go	То				
Dev	Frame#	TIME (Diff		Len	Protocols		RTP Paylo			IP Packet	T [Source IP Addr	Destination IP Ad		Sourc	e IPv6 Address	
/ 2	123963	00:00:00.	003894	214	Internet IP(I	Pv4) I	PCMU (A ·	8000 Hz -	1 Channel	RTP		192.168.1.54	192.168.1.56				
/ 2	123964	00:00:00.	000037	214	Internet IP(I	P∨4)	PCMU (A ·	8000 Hz -	1 Channel	RTP		192.168.1.54	192.168.1.56				Π.
/ 2	123965	00:00:00.	000021	214	Internet IP(I	P∨4)	PCMU (A ·	8000 Hz -	1 Channel	RTP		192.168.1.54	192.168.1.56				
/ 2	123966	00:00:00.	000011	214	Internet IP(I	Pv4)	PCMU (A ·	8000 Hz -	1 Channel	RTP		192.168.1.54	192.168.1.56				
/ 2	123967	00:00:00.	000010	214	Internet IP(I	Pv4)	PCMU (A ·	8000 Hz -	1 Channel	BTP		192.168.1.54	192.168.1.56				
/ 2	123968	00:00:00.	013596	234	IPv6		PCMU (A ·	8000 Hz -	1 Channel	BTP				2001:0918	:0000:0012:0001:0	000:0000:0054	I I
/ 2	123969	00:00:00.	000041	234	IPv6		PCMU (A ·	8000 Hz -	1 Channel	RTP				2001:0918	:0000:0012:0001:0	000:0000:0054	1
/ 2	123970	00:00:00.	000011	234	IPv6		PCMU (A -	8000 Hz -	1 Channel	BTP				2001:0918	:0000:0012:0001:0	000:0000:0054	1
/ 2	123971	00:00:00.	022388	234	IPv6		PCMU (A ·	8000 Hz -	1 Channel	RTP				2001:0918	:0000:0012:0001:0	000:0000:0054	Ļ
/ 2	123972	00:00:00.	000031	234	IPv6		PCMU (A -	8000 Hz -	1 Channel	BTP				2001:0918	:0000:0012:0001:0	000:0000:0054	1
/ 2	123973	00:00:00.	000010	234	IPv6		PCMU (A -	8000 Hz -	1 Channel	BTP				2001:0918	:0000:0012:0001:0	000:0000:0054	į į
/ 2	123974	00:00:00.	000759	214	Internet IP(I	Pv4)	PCMU (A -	8000 Hz -	1 Channel	BTP		192.168.1.56	192.168.1.54				
/ 2	123975	00:00:00.	000100	214	Internet IP(I	Pv4)	PCMU (A -	8000 Hz -	1 Channel	RTP		192.168.1.56	192.168.1.54				
/ 2	123976	00:00:00.	000062	214	Internet IP(I	Pv4)	PCMU (A ·	8000 Hz -	1 Channel	RTP		192.168.1.56	192.168.1.54				
/ 2	123977	00:00:00.	000060	214	Internet IP(I	Pv4)	PCMU (A ·	8000 Hz -	1 Channel	RTP		192.168.1.56					
/ 2	123978	00:00:00.	000061	214	Internet IP(I	Pv4)	PCMU (A -	8000 Hz -	1 Channel	BTP		192.168.1.56	192.168.1.54				
/ 2	123979	00:00:00.	000059	214	Internet IP(I	Pv4)	PCMU (A -	8000 Hz -	1 Channel	BTP		192.168.1.56	192.168.1.54				
(100000	00.00.00	00050	01.4	Lata and the	D()		000011-	1 01	птп		100 100 1 50	100 100 1 54			I	۰ſ
Call ID	Call 9	St		Sourc	ce Address	:	Dest	ination A	ddress	Call S	Start D	late & Time	Call Duration	DevNo	SIPCalIID	Release (Cε
2543	ac	;ti∨e	0	nna@1	92.168.1.56		000	8@192.1	68154	2012-03-16	11:03	3:30.899942	00:13:00.887032	2	GLPG-193		-
544		tive.			92.168.1.56			9@192.1				3:30.965565	00:13:00.821409	2	GLPG-193		
545		tive .			92.168.1.56			0@192.1				3:30.988260	00:13:00.798714	2	GLPG-193		
957					8:0:12:1::56			1:918:0:1				5:06.060844	00:00:25.726130	2	ProtScriptI		
958					8:0:12:1::56			1:918:0:1				6:06.079973	00:00:25.707001	2	ProtScriptI		
959					8:0:12:1::56			1:918:0:1				6:06.082934	00:00:25.704040	2	ProtScriptI		
960					8:0:12:1::56			1:918:0:1				6:06.094067	00:00:25.692907	2	ProtScriptI		
961					8:0:12:1::56			1:918:0:1				6:06.112100	00:00:25.674874	2	ProtScriptI		
962					8:0:12:1::56			1:918:0:1				6:06.392314	00:00:25.394660	2	ProtScriptI		
963					8:0:12:1::56			1:918:0:1				6:06.401969	00:00:25.385005	2	ProtScriptI		
964					8:0:12:1::56			1:918:0:1				6:06.428250	00:00:25.358724	2	ProtScriptI		
965					8:0:12:1::56			1:918:0:1				6:06.441733	00:00:25.345241	2	ProtScriptI		
966					8:0:12:1::56			1:918:0:1				6:06.445442	00:00:25.341532	2	ProtScriptI		
000	ac		or e (r	551.510	0.0.10.100	000	3[-00		e. (2012 00 10		5.55. HIS HIE	55.50.E5.5 H 35E		r rotoonpa		
						1											
							D-\TPV6	lov6 IPv	Trace bdl		11	52 907 Frames					

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.

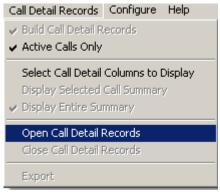


Figure 99: Open Call Detailed Record

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.

Warning	×
Call Detail Record view cannot be opened when <call build="" call="" detail="" records=""> menu item is unchecked Please set the menu item <call build="" call="" detail="" records=""> to the CHECKED state first.</call></call>	ł.
(OK]	

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 ($\mathbf{\hat{x}}$) 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 ($\textcircled{\bigcirc}$) 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			
l 🗃 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:

Call ID	Call Status	Source Address	Destination Address	Call Start Date & Time	Call Duration Dev N	0
Ö	completed	0001@192.168.1.231	0001@192.168.1.237	2008-03-05 16:14:57.444060	00:00:41 656708	2 6
0 01 02	completed	0002@192.168.1.231	0002@192.168.1.237	2008-03-05 16:14:58.44363	Find CDR	6
* @'2	completed	0003@192.168.1.231	0003@192.168.1.237	2008-03-05 16:14:59.30791	Select Columns	6
		Ŭ	U		Export Call Trace Records	
	CDR Search C	riteria		×	Close Call Trace View	
•	CDR Scarch C					1 - 1
						الك
	• A	ND O OR	Include	C Exclude		
	- Column	M	-Value Wildcard			
	Call State	st 🗾	completed	Add		
	– Search Cri	iteria, double click to modil	hu			
			y			
	CDR C	olumn Name	Value Wildcard			
	Call ID		1			
	Call Sta	tus	completed			
	L					
	OK	Delete Selected	Delete All	Cancel		
I						

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 0 1 2 2	completed	0001@192.168.1.231	0001@192.168.1.237	2008-03-05 16:14:57.444060	00:00:41.656708	2	6
1	completed	0002@192.168.1.231	0002@192.168.1.237	2008-03-05 16:14:58.443636	00:00:41.865879	2	6
* @'2	completed	0003@192.168.1.231	0003@192.168.1.237	2008-03-05 16:14:59.307919	00:00:42.015382	2	6
Esc - exit Next							
						۰I	
Off-line Viewing D:\Program Files\GL Communica 9581 Frames						7	

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	
Ö	completed	test4@192.168.10.45	test3@192.168.10.14	2002 10 05 14 20 22 202205 00:00:28.004 Find CDR	
				Select Columns	
				Export Call Trace Records Close Call Trace View	
•					

Call Detail Records Configure Help	Select Call Trace Columns to Display	×
 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 	Call ID Call Status Source Address Destination Address Call Start Date & Time Call Duration DevNo SIPCallD 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 <u>Connecting to</u> <u>Remote Database</u>

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.

Save As					? ×
Save jn: 🔂	G711_alaw	•	(🔁	💣 🎟 •	
File <u>n</u> ame:				<u>S</u> av	е
Save as <u>t</u> ype:	Statistic Export Files (*.cte)		•	Cano	el

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.

Select summary columns to display	DISPLAYED summary columns	HIDDEN summary columns
Menu checked options	Ctrl-Up, Ctrl-Down to rearange columns, DEL to remove, Ctrl-Z to undo delete, Ctrl-A - display all columns	
Protocol standard selection		< Display Selected Columns
Network/User side selection	to delete	
🕐 Time Format	Device Frame#	Called#
Yiew Filter	Time Length (Bytes)	CLTP Message CLTP Message
View Search	Error Protocols	COTP Message DNS QuervName
	RTP Payload Type IP Pasket Type	EIGRP Packet Type Opcode FTP Message
Periodic Trace Saving Options	Source IP Address Destination IP Address	GRE Destination IP Address
Startup Options	Source IPv6 Address	GRE Source IP Address
Data Link Groups	Destination IPv6 Address RTCP Packet Type	GRE Source IPv6 Address HTTP Message
F_{F_r} View Font Size	SIP Call ID SIP CSeq	IGMP Message Type ISUP Message Type
INI Decode Options	SIP From SIP Method	LDP Message Type Marker bit
Define Summary Columns	SIP To TCP Destination Port	NSAP Operation PIM Destination IPv6 Address
C Capture Options	TCP Source Port	PIM Source IPv6 Address
	UDP Destination Port UDP Source Port	PIM TCP Destination Port PIM TCP Source Port
		PIM UDP Destination Port PIM UDP Source Port
		POP3 Message
		PPPoE Ether Type PPPoE TLV Tag
		RIEP Message
		RSVP Class RSVP Message Type
		RTP Sequence #
		RTP SSRC ID
	Sel Only All Columns Undo Delete Restore	

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.

Save As		<u>? ×</u>
Save <u>i</u> n: 🔂	PacketScan 💽 🖛 🗈 💣 🏢	
Docs		
Examples		
📄 Release No	tes	
Catistics		
🛛 📴 sipProtAnal	lyzer.Acf	
		_
File <u>n</u> ame:	sipProtAnalyzer.Acf Sa	ve
Save as <u>t</u> ype:	Configuration Files (*.ACF)	icel

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.

Open		? ×
Look jn: 🔁	PacketScan 💽 🖛 🗈 📸 📰 🕶	
Docs		
Examples		
Release N	otes	
Statistics SipProtAna	alyzer.Acf	
I		-1
File <u>n</u> ame:	<u>O</u> pen	
Files of type:	Configuration Files (*.ACF)	
	C Open as read-only	1.

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

Menu checked options Save Load Default		
Select summary columns to disple Menu checked options Protocol standard selection Network/User side selection Time Format View Filter	✓ View Latest Frame/Packet ■ Enable Periodic Trace Saving	▲

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 <u>Protocol List</u> 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

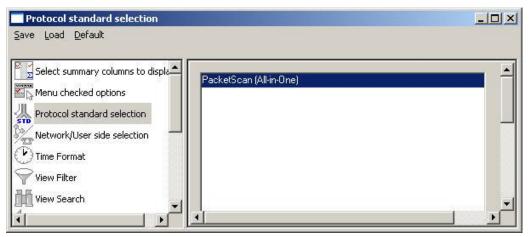


Figure 111: Protocol Standard Selection

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.

Network/User side selection	×
Save Load Default	
Select summary columns to displation Menu checked options Protocol standard selection Metwork/User side selection Time Format View Filter View Search Deriodic Trace Savion Options Deriodic Trace Savion Options	

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.

Time Format		_ 🗆 🗡
<u>Save Load D</u> efault		
Select summary columns to displation Menu checked options Protocol standard selection Network/User side selection Time Format View Filter	Relative to the frame 0 System Time Date and Time Time Difference between frames	

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

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.

IP Address (127.0.0.1 Local) IP Port 127.0.0.1 20019 Test Connection	
Probe Name	
Select Information to be Sent over TCP/IP	
Default	
Send Call Detail Records Send Traffic Summary	
Frame/Packet Information to Send	
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 CLNP Message CLTP Message CUTP Message CUTP Message UDP Source Port UDP Destination Port TCP Source Port	
	<u> </u>

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 msecs.
- **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 msecs.
- **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 PacketScanWebTM.

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.

- 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 X** 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 <u>Periodic Trace Saving Options</u>.

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

	- Load Options from File and Execute Tasks on Analyzer Startup
	Enable periodic trace saving
	- Startup Tasks
	C Activate Filter
	Euild call detail records
	Connect to a remote database via TCP/IP
	Start real-time tracing
	✓ Open PDA
	Execute
_	

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.

🔤 View Font Size			_ 🗆 🗙
<u>Save Load D</u> efault			
Select summary columns to display Menu checked options Protocol standard selection Network/User side selection Time Format View Filter View Filter View Search CP Connection Options Periodic Trace Saving Options Startup Options Startup Options Data Link Groups Fre View Font Size INI Decode Options Capture Options	Summary, Statistics, CDR Font Size © Extra large © Large © Normal © Small © Very small	Detail, Hex View Font Size Extra large Large Normal Small 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 From Configure > Protocol and GUI Options > INI Decode Options screen.

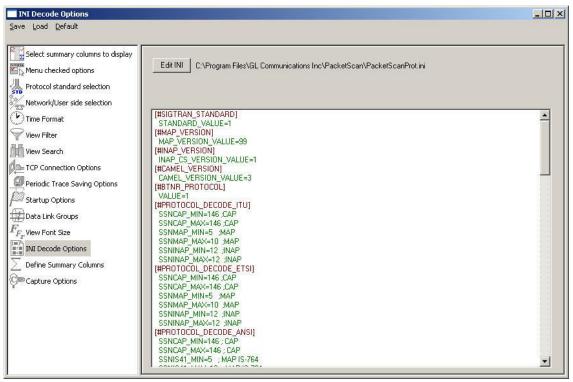


Figure 117: INI Decode Options

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

📕 PacketScanProt.ini - Notepad	- 🗆 🗡
Eile Edit Format View Help	
; Sigtran Configurations	
; Set 1 for ITU. Set 2 for ANSI. Set 3 for ETSI. [#SIGTRAN_STANDARD] STANDARD_VALUE = 1	
: Set 99 for Release 99. Set 4 for Release 4. [#MAP_VERSION] MAP_VERSION_VALUE = 99	
: Set 1 for INAP CS-1. Set 2 for INAP CS-2. [#INAP_VERSION] INAP_CS_VERSION_VALUE = 1	
: Set 3 for Camel Version 3. Set 6 for Camel Version 6. [#CAMEL_VERSION] CAMEL_VERSION_VALUE = 3	
: Set 1 for IUP. Else TUP. [#BTNR_PROTOCOL] VALUE = 1	
: SCCP SSN values for Itu. [#PROTOCOL_DECODE_ITU] SSNCAP_MAX = 146 :CAP SSNCAP_MAX = 146 :CAP SSNMAP_MAX = 5 :MAP SSNMAP_MAX = 10 :MAP SSNINAP_MAX = 12 :INAP SSNINAP_MAX = 12 :INAP	
: SCCP SSN values for Etsi. [#PROTOCOL_DECODE_ETSI] SSNCAP_MIN = 146 ;CAP SSNCAP_MAX = 146 ;CAP SSNMAP_MIN = 5 ;MAP SSNMAP_MIN = 10 ;MAP SSNINAP_MIN = 12 ;INAP SSNINAP_MAX = 12 ;INAP	

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:

IPCapt - Notepad <u>- 🗆 ×</u> <u>File E</u>dit Format ⊻iew <u>H</u>elp [#CAPTURE_OPTIONS] * ;Enable or disable (1/0) COTP packets processing COTP_ENABLE=1 ;Enable or disable (1/0) H323 packets processing H323_ENABLE=1 ;Enable or disable (1/0) SCTP packets processing SCTP ENABLE=1 ;Enable or disable (1/0) GRE packets processing GRE_ENABLE=1 ;Enable or disable (1/0) SIP packets parsing for extracting RTP port numbers SIP_ENABLE=1 ;Enable or disable (1/0) SCCP(Skinny client control protocol) packets processing SCCP_ENABLE = 1

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.

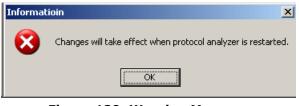


Figure 120: Warning Message

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

option.

10.13 Define Summary Columns

User can define the required summary columns through \sum Define Summary Columns

- 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.

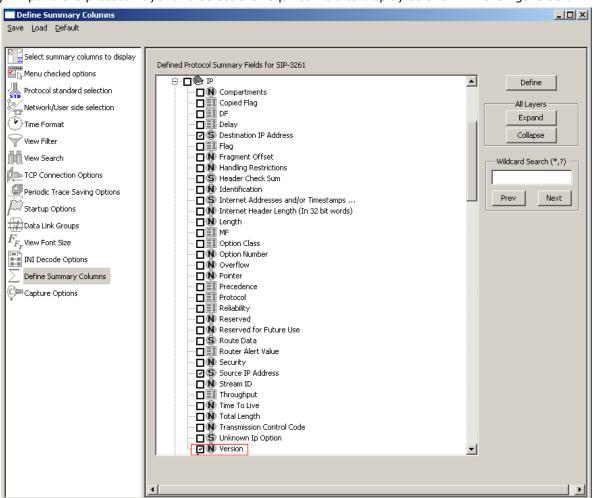


Figure 121: Define Summary Column

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

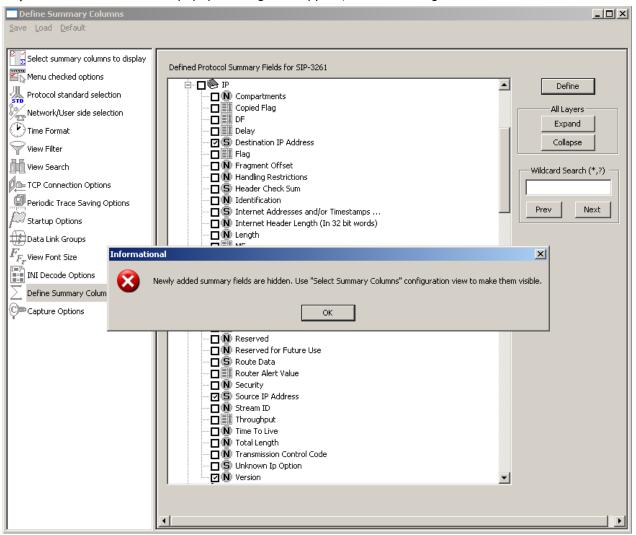


Figure 122: Popup Message

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".

Select summary column	ns to display	<u> </u>
<u>S</u> ave <u>L</u> oad <u>D</u> efault		
Select summary columns Menu checked options Protocol standard select Network/User side select View Filter View Filter View Search Periodic Trace Saving Op Startup Options Data Link Groups F_{r_F} View Font Size INI Decode Options Define Summary Column Capture Options	DISPLAYED summary columns Image: ChtUp, ChtDown to rearange columns, DEL to remove, ChtZ to undo delete, ChtA - display all columns Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to delete Image: ChtUp, ChtDown to rearange, drag out of the list box to	
	•	•

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:

PacketSca	an (¥PA) H32	:3								<u>_ 0 ×</u>
<u>F</u> ile ⊻iew C	apture <u>S</u> tatis	tics <u>D</u> atabase	Call Deta							
学 🖆 💙	2 0	ا 🛂 🖳 🖳		• ₩	₩, ₩,	\$1 ₩ ₩ ± ₩	ра	GoTo		
Dev	Frame# TIME (Relative) Len Prot					. Source IP Address	Destination IP Address	IP Pack	Version	NSAP Operation 🔺
$\sqrt{1}$	0	00:00:00.0	00000000	707		192.168.20.54	192.168.20.231	SIP	4	
√ 1	1	00:00:00.0	00034300	332		192.168.20.231	192.168.20.54	SIP	4	
√1	2	00:00:00.0	00045180	354		192.168.20.231	192.168.20.54	SIP	4	
√ 1	3	00:00:00.0	26202200	689		192.168.20.231	192.168.20.54	SIP	4	
√ 1	4	00:00:00.0	26393320	486		192.168.20.54	192.168.20.231	SIP	4	
√ 1	5	00:00:00.0	26551690	94		192.168.20.54	192.168.20.231	RTP	4	
√ 1	6	00:00:00.0	26738040	94		192.168.20.231	192.168.20.54	RTP	4	
	7	00-00-00 0	00751000	04		102 100 20 54	100 100 00 001	DTD	4	`
										<u> </u>
Devicel F Ethernet		00:00:00	. 000000	000 OK	Len=7	07				
		.a Laver ===:								
	tion Addr					= x000B82008BE	3			
Source						= x000B82008F2				
	Protocol					= x0800 Interne	et IP(IPv4)			
	==== IP I	ayer ====		-	-	= 0100 (4)				-
•										•
Hex Dump	of the Fr	rame Data								
+	+	+				- +++	+			
00 0B 82 02 B5 EA		00 0B 82 FA 11 29 !		E 08 0 8 14 3						
14 E7 13					9 54 4					
20 73 69					E 31 3					
38 2E 32			53 49 5	0 2F 3	2 2E 3	0 8.20.231 S	IP/2.0			
OD 0A 56										
44 50 20			38 2E 3							•
I										F
Off-line Viewing	,			D:\Prog	ram Files\G	L Communications I 2 511	Frames			

Figure 124: Added summary field

Note:

To remove the selected summary field, do the following:

- 1. Select Configure Menu \rightarrow Protocol and GUI Options \rightarrow 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:

Р	acket	Scan (¥P	A) 5IP-326	51						- D ×
Eile	⊻iew	Capture	<u>S</u> tatistics	<u>D</u> atabas	e Call D	etail <u>R</u> ecords	<u>C</u> onfigure <u>H</u>	elp		
	E	1	- , -				4 94 set	₩₩)
Dev		Frame#	TIME (F	Relative)	Len	Error	Protocols	9	Source IP Address	Destinat 🔺
		0	00:00:00	.000000	60		Undefined			
$\sqrt{1}$		1	00:00:00	.041916	60		Undefined			
$ \sqrt{1}$		2	00:00:00	083854	60		Undefined			
1/1		3	00:00:00	125782	60 Undefined					
┖										
				0:00:0	0.0000	00 OK Len=	:60			
Ethe		t Frame	e Data MAC Lav				-			
De			Address				_	x0180C2	2000001	
S	ourc	e Addre	ess	_			=	x000000	0000000	
	_	-	r Proto		_			x8808 T	Undefined	
			Unsuppo	orted (Layer					
	ata						-			(x00)
Cantu	ire Rat	:e : 0.00 M	hns		:\Temp.H	dl	Captured 31	10 frames	Missed Frames	

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, GSMA, 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/Packet information) to be sent over TCP/IP to a central database. For more details refer to <u>Connecting to Remote Database</u>.

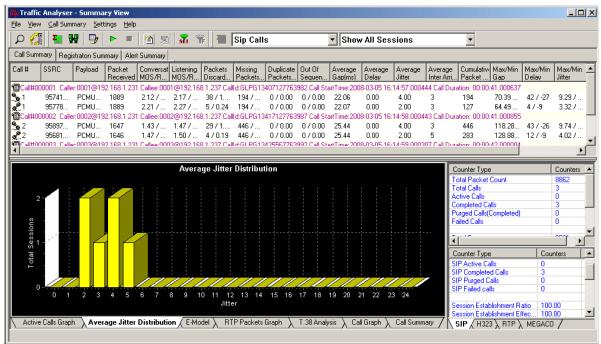


Figure 126: Packet Data Analysis – Traffic Analyzer Summary View

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> Calld: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 relevant columns will have valid information, the rest will reflect a default (zero) value.

<mark>မ</mark> ျာ Traffic A	nalyser -	Summary	/ View															_ 🗆 🗵
<u>E</u> ile ⊻iew	<u>C</u> all Summ	ary <u>S</u> ettin	igs <u>H</u> elp															
D 🚰	2	9	▶ ■ 🗎	图 🖬 🎙	🌾 🛛 📲 🛛 Sip	Calls		Show All S	essions			-						
Call Summary Registraton Summary Alert Summary																		
Call # SSR(C Payload	Packet Received	Conversational MOS/R-Factor	Listening MOS/R-Factor	Packets Discarded/(%)	Missing Packets/(%)	Duplicate Packets/(%)	Out Of Sequence Packets/(%)	Average Gap(ms)				Cumulativ Packet	Max/Min Gap			Max/Min RTDela	
Call#0000	001 Caller:	UA01@192	.164.1.64 Callee	:UA01@192.16	8.1.21 Calld:GLF	PG231006472	2738 Call Sta	tTime:2009-03-24 15	5:01:55.000	0390 Call	Duration: (00:03:24.0	00858					,
% 1 27	PCM	7632	1.30 / 23	1.33/24	133 / 1.30	2595 / 25	0 / 0.00	0 / 0.00	26.75	0.00	8.00	3	0	143.18	86 / -45	16.48	0.217	0.127
g ⁰ 1 27	PCM	10250	3.91 / 82	3.98 / 84	208 / 2.03	0 / 0.00	0 / 0.00	0 / 0.00	20.01	0.00	1.00	8	1658	219.84	1997	23.51	4.805	0.896
Call#0000	004 Caller:	UA04@192	164.1.64 Callee	UA04@192.16	8.1.21 Calld:GLF	PG231584472	2747 Call Star	tTime:2009-03-24 15	5:01:55.000	0773 Call	Duration: (00:00:00.0	00000					
% 4 27	PCM	8474	1.18/19	1.21 / 20	1180 / 9.86	3510 / 29	0 / 0.00	2076 / 17.34	28.24	0.00	24.00	4	0	617.00	600 /	92.66	1.394	0.502
e 4 27	PCM	12001	3.95 / 83	3.98 / 84	207 / 1.73	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
@Call#0000	005 Caller:	UA05@192	.164.1.64 Callee	:UA05@192.16	8.1.21 Calld:GLF	G231693472	2750 Call Sta	tTime:2009-03-24 15	5:01:55.000	0927 Call	Duration: (0:00:00.0	00000					
S 27	. PCM	12942	1.43 / 27	1.50 / 29	294 / 1.78	3553 / 21	4510 / 2	0 / 0.00	18.48	0.00	22.00	4	0	514.98	482 / •	89.48	0.589	0.325
6 5 27	PCM	12002	3.98 / 84	4.01 / 85	195 / 1.63	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
•																		Þ

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 <u>Connecting to Remote Database</u>.

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:

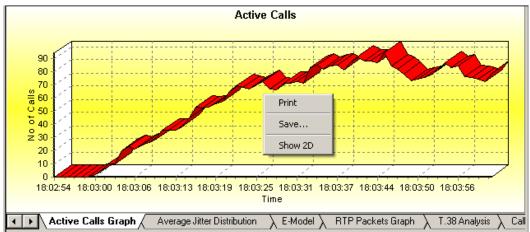


Figure 131: Active Calls Graph

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.

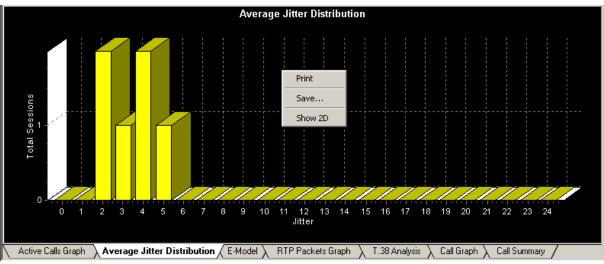


Figure 132: Average Jitter Distribution

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 rightclicked 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.

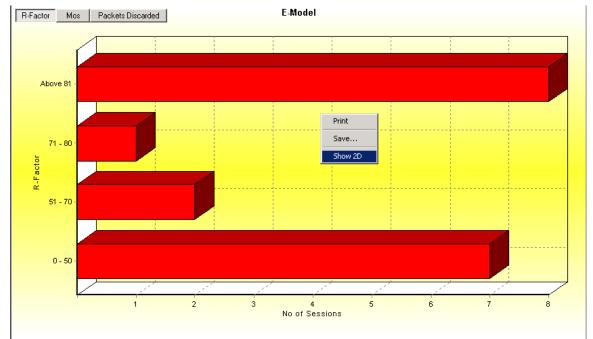


Figure 133: R-Factor

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.

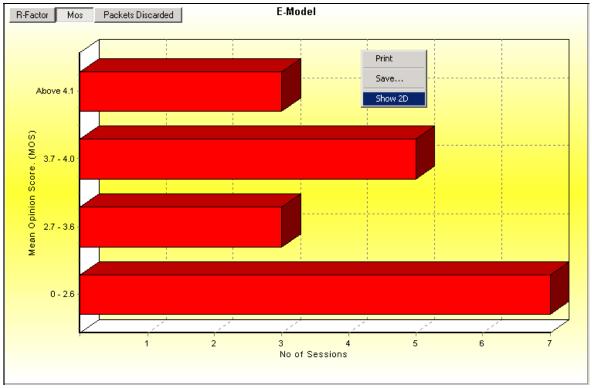


Figure 134: Mean Opinion Score

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.

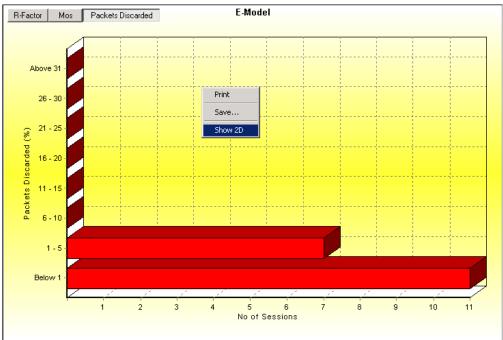
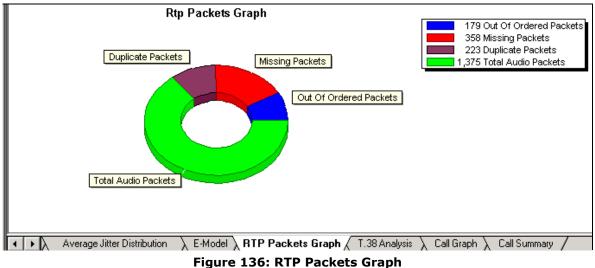


Figure 135: Packets Discarded

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.



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.

کې T File	raffic <i>i</i> View		<mark>r - Summa</mark> mary Seti													_ 🗆 X
٦	-		 H 🌗		2 2	SET 1	¥ 1	Sip Cal	s		- Sho	w Fax C	alls		•	
Cal	Call Summary Registraton Summary Alert Summary															
Call	1	SSRC	Payload	Packet	Conversat MOS/R			Missing . Packets	Duplicate Packets		Average Gap(ms)	Average Delay	Average Jitter	Average Inter Arri.	Cumula Packet	tivi Max/Min Gap
F	Call#000 1 1	001 Calle 24899 56526	er:55510000 PCMA PCMA	@suman.co 321 322	m Callee:98 4.18 / 4.18 /	4.207	. 0/0.00	0 / 0.00	ohone Callid 0 / 0.00 0 / 0.00	:35542752 0 / 0.00 1 / 0.31	041200012 20.00 19.87	939@192.1 0.00 0.00	168.2.175 C 0.00 0.00	all StartTim 0 0	e:2009-05 0 0	007 11:40:37.0 21.10 20.03
				Ladder di	agram sho	wing the	FAX Call									Þ
5	5004 NSF 5004 DIS:DSR:ITU-T V.27 ter and V.29 5004 no-signal 5004 v21-preamble 5004 TSI NUM: 5004 DCS:DSR:9600bps, ITU-T V.29 5004 v29-9600-training 5004 v29-9600-training								UDPTI seq Cont prin Leng IFP Pres ty Cha dat dat dat	Packet number cents aary-ifp gth Packet amble be-of-ms bice Ind ata ttensibi ontents ca-field ara-field ata-fiel	-packet g ex lity Man Count d	splays the the sele	decoded ir		= II = 4 = 0; = 1: = 5: = 1 = C = 1 = C = 1 = B; = 0 = 0 = S = 2 = 1;	EQUENCE NTEGER 2 EQUENCE HOICE NUMERAT(V21(0) EQUENCE nstance EQUENCE
	<u>-λ</u>	Average	e Jitter Distri	bution λ	E-Model >	RTPP	'ackets Gra	ph <u>}</u> T.38	l Analysis	Call Gra	ph <u>)</u> Call	Summary	/			

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 Ethereal *.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 Ethereal format file *.PCAP and vice-versa. Refer to <u>Appendix E: Additional Utilities</u> for more details.

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

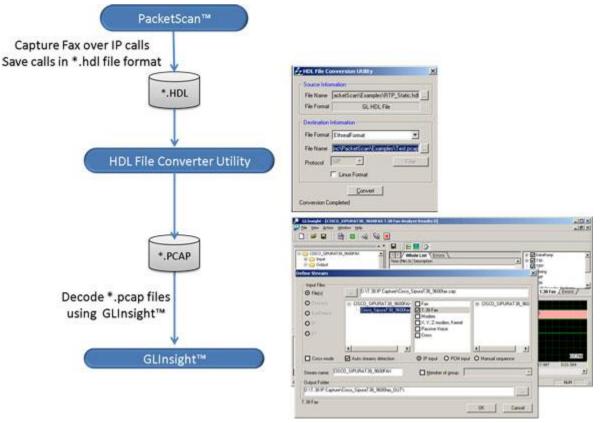


Figure 138: Decode PacketScan™ Captured Fax files in GLInsight™

12.2.2.6 Call Graph

The Call Graph displays the message sequence of captured SIP, H323, MEGACO, IuCS, and GSM A) calls. This iincludes 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.

1	P 🔚	W 🖵		首为	👬 🌾 Fa	× Sip Ca	alls	Show All Sessions								
all Sum	mary Reg	jistraton Sum	mary Alert	Summary												
all #	SSRC	Payload	Packet Received	Conversat Lister MOS/R MOS		Missing Packets	Duplicate Packets	Out Of Sequen	Average Gap(ms)	Average Delay	Average Jitter	Average Inter Arri	Cumulative Packet	Max/Min Gap	Max/Min Delay	Max/M Jitter
Call#00	95741	er:0001@19 PCMU PCMU	1889		92.168.1.237 Ca 4 / 4 / 0.19 4 / 0 / 0.00	194 /	0/0.00	3982 Call Sta 0 / 0.00 0 / 0.00	artTime:200 22.06 22.07	08-03-05 16: 0.00 0.00	14:57.444 4.00 2.00	Call Duration 3 3	194 127	000638 70.39 64.49		9.29 / 3.32 /
2 2 2		PCMU	1647		92.168.1.237 Ca 2 / 3 / 0.14 2 / 0 / 0.00	446 /	0/0.00	987 Call Sta 0 / 0.00 0 / 0.00	25.44 25.44 25.44	0.00 0.00 0.00	4.00 2.00	Call Duration 3 5	446 283	118.28	43 / -26 12 / -9	9.74 4.02
imeStar		192.16	81231		192.16	8.1.237				30192.16						
	mp	INV/ITE						Uin. CT								
00.00.00					•	1	60		wards: INVITE,	70 BYE,CANCI	RL,ACK,	INFO, PRAC	R, COMET,	OPTIONS	,SUBSCR	
	00 ! 01 01		• •	SIP/2.0 100 Tr SIP/2.0 180 Rin SIP/2.0 200 C	lying nging	1	198 198	Max-For Allow: From: 0 To: 000 Call-ID CSeq: 1 Contact	wards: INVITE, 003 <si 3 <sip: : GLPG1 INVITE : 0003 -Type:</sip: </si 	70 BYE,CANC p:0003019 00030192 342556779 <sip:000 applicat</sip:000 	BL,ACK, 92.168.1.3 168.1.3 53992 30192.10	INFO,PRAC 1.231>;ts 237>	Disp	OPTIONS	,SUBSCR 76-3994	
10.00.00 10.00.00 10.00.00	00 ! 01 01 07 09 !	54098 5060 5060		SIP/2.0 100 Tr SIP/2.0 180 Rin	rying nging OK	500 540 540	198 198 198 60	Max-For Allow: From: 0 To: 000 Call-ID CSeq: 1 Contact Content Content v=0	wards: INVITE, 003 <si 3 <sip: : GLPG1 INVITE : 0003 -Type: -Length</sip: </si 	70 BYE,CANC p:0003019 00030192 342556779 <sip:000 applicat</sip:000 	8L,ACK, 92.168.1 168.1.3 53992 30192.10 ion/sdp	INF0, PRAC 1.231>;ts 237> 58.1.231>	Displinfor	options 13425567 lays de matior	s, SUBSCR: 776-3994 coded	IBE,NO
10.00.00 10.00.00	000 1 01 07 09 98 00	54098 5060 5060 5060 54098		SIP/2.0 100 Te SIP/2.0 180 Rin SIP/2.0 200 C ACK	eying nging DK 1000)	540 540 540 540 540	198 198 198 60 28 28	Max-For Allow: From: 0 To: 000 Call-ID Contact Content Content Content v=0 o=0003 s=- c=IN IP t=0 0 m=audio	wards: INVITE, 003 <si 3 <sip: : CLPGL INVITE : 0003 -Type: -Length 4449486 4 192.1 1028 R</sip: </si 	70 BYE,CANC: p:00030192 342556770 <sip:0003 applicat: : 351</sip:0003 	RL,ACK, 32.168.1 168.1.1 53992 30192.10 100/sdp 72 IN I	INF0, PRAC 1.231>;ts 237> 58.1.231> 58.1.231> 94 192.16	Displinfor	options 13425567 lays de matior	coded	IBE,NO

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.

Page 1	P 📲	W 9		1	SET 1	Fax	Megac	o Calls		▼ Sh	ow All Se	ssions		*						
all Summary Registraton Summary Alert Summary																				
all #	SSRC	Payload	Packet Received	Conversat MOS/R			Missing Packets	Duplicate Packets		Average Gap(ms)	Average Delay	Average Jitter	Average Inter Arri	Cumulativi Packet	Max/Min Gap	Max/Min Delay	Max/M Jitter			
		ler:aaln/3 Ca																		
1	29282	PCMU	1533		4.20 /		0/0.00	0/0.00	0/0.00	20.01	0.00	0.00	0	0	40.04	20/.9	1.26 /			
1	42949	PCMU ler:aaln/3 Ca	-		0.00/0	0/0.00	0/0.00	0 / 0.00	0/0.00	0.00	0.00	0.00	0	U	0.00 /	070	0.00/			
	13842	PCMU	2055		4.20 /		0/0.00	0 / 0.00	0 / 0.00	20.01	0.00	0.00	0	0	40.02	20/-10	1.26/			
2	42949		0		0.00/0	0/0.00	0/0.00	0/0.00	0/0.00	0.00	0.00	0.00	0	0	0.00 /		0.00			
Call#0	00003 Cal		llee:\$ Calld		ime:2009-0		46.259 Call													
3	0	Unkno	0	0.00/0	0.00/0	0/0.00	0/0.00	0/0.00	0/0.00	0.00	0.00	0.00	0	0	0.00/0	0/0	0.00/			
		I false a		11101201	11 OCAT	11241100	11/41100	10/01/00	0,000							11.20	•			
00.00.0		2944		Add R		•	294		{C=\$ {A=aaln {	/3										
00.00.0	86	2944	•				294	14	Media (Stream	= 1(Displ	ays dec	oded				
0.00.0		30000	◀	RTP (PCM	(U/8000)		300	00	LocalCo					infor	mation	of the				
	20	30000							Mode =	SendRec	eive			select	ted Me	gaco				
00.00.1	556		4 Subtract Request 2944				294	14	A=\$					Com	mand					
00.00.0 00.00.1 00.30.6	556	2944				30.866 2944 Subtract Reply 2944						(H (0								
00.00.1	57	2944 2944	•	Subtract	t Reply		294	14												
00.00.1 00.30.6	57		•	Subtrac	t Reply		294	14	{0 (M0=sen	dreceiv	e},									
00.00.1 00.30.6	57		•	Subtrac	t Reply		294	14	{0 (M0=sen L{	dreceiv	e),									
00.00.1 00.30.6	57		•	Subtrac	t Reply		294	14	{0 (M0=sen		e},									
00.00.1 00.30.6	57		•	Subtrac	t Reply		294	14	(0 (MO=sen L(v=0	4 \$										

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.

Traff وال	ic Analyze	r - Summa	ary View																_ 8 ×
File Vie	w Call Sur	nmary Set	tings Help																
E	<u>۵ ا</u> ۹	¥ 🦻	• 🕨 🗉	1	🖄 🧏	* 1	H323	Calls			- She	w All Se	essions		-				
	nmary Reg	istraton Sun	nmary Aler	t Summary	1														
Call #	SSRC	Payload	Packet Received		at Listening MOS/R		Missing Packets	Duplicate				Average Delay	Average Jitter	Average Inter Arri.	Cumulativ Packet	Max/Min Gap	Max/Min Delay	Max/Min Jitter	Max/I▲ RTD€
								8B03001676											
% 1	18820	PCMU	472	3.65 /	3.65 /	38 / 8		0/0.00	070			2.00	39.00	61 64	0	101.20 98.73	71 / -30	42.82	0.000
And a second sec								8804001676										47 41	
% 2	34278	PCMU	445	3.61 /		38 / 8			070		31.91	1.00	39.00	61	0	98.39	68 / -30	42.91	0.000
a ² 2	24127	PCMU	445	3.61 /	3.65 /	37 / 8	0 / 0.00	0/0.00	070	0.00	31.90	2.00	39.00	64	0	98.98	68 / -30	42.73	0.00(-
•									_	_								<u> </u>	_ <u>`</u>
TimeSta	amp	192.10	68.1.200		/	192.16	8.1.182			۹ I	Protocol Call Refe	Discrim	inator	all Sign	haling La		0000100	0 0931/3	1.451
00.00.0	000	2745		SE	ETUP		17	720			all Refe						5092 (.)		1110(
00.000	200	0745		CALLPR	OCEEDING		1.	720			Call Refe Message 7		lag				0		side t
00.00.0	103	2745					1	/20			IESSage I IEI Bear		bility				0000010		c Cap:
00.00.0	040	2745		ALE	RTING		17	720					ility Le				3 (x03)		
				00	NNECT						Informat Coding S		nsfer Ca	pability	7		0100		
00.00.1	110	2745	-				17	720			Informat	ion Tra	nsfer Ra	te		=	1001	1 384 ki	oit/s
00.00.3	382	5004	4	RTP (PC	CMU/8000)		50	010			Transfer User Inf		n Layer	1 Brotos	AL (PC)		.00		
				BTP(P	CMU/8000)										ol Ident		.01		
00.00.4	421	5004		(, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		- 50	010			IEI Disp						0010100	0 Displa	ay IE
00.15.4	107	2745		RELEASE	COMPLETE		17	720			IE Lengt Display		tion				8 (x08) x4E6167	61726163	100
00.10.		2140	1					20			IEI User						0111111		Jser :
											IE User		ngth minator()	u222)			741 (x0)		and)
																	0000010	1 7.000	and ,
											1323-User						SEQUENC	E	
											xtensibi reamble	lity Ma	rker	icnlave	decod		0		
									_		h323-uu-	pdu					SEQUENC	E	
											Extensit				tion of		1		
											Preamble b323-me	ssage-b	odv Se	electec	H323 I	messa	CHOTCE		
												bilitv					0		_
										•						_			►
\ Activ	/e Calls Grap	oh λ Av	/erage Jitter	Distribution	n ∖E-Mo	odel 🔪 RT	P Packet	s Graph 🔪	T.38	Anal	lysis λ Cal	l Graph 📈	Call Summ	hary /					

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.

	w <u>C</u> all Summ	immary View ary <u>S</u> etting															_	
<u> </u>	o 🛛 🏭 🖢		▶ ■ 🖺	🖄 🚮	*	GSI	VA Calls			• S	how All	Session	IS	-]			
Call Sum	Call Summary Registraton Summary Alert Summary																	
Call #	SSRC	Payload	Packet Received	Conversat MOS/R					olicate C kets S		Average Gap(ms)	Average Delay	Average Jitter	Average Inter Arri		lativ Max/Mi st Gap	n Max/Min Delay	n Max/ Jitter
			1 Callee:x11111															
% 1	2558136321 2563981057				4.11 /)/0.00)/0.00	20.01 20.01	0.00	0.00	0	0	40.05 40.01		1.31
9	2063961007	G2W/800	JU 1497	4.117	4.117	070.00	070.00	07	0.00	17 0.00	20.01	0.00	0.00	U	U	40.01	. 207-1	1.30
•																		F
											GSM P	hase2+	Laver ==			-		
TimeStar	mp	192.168.1	228		192.	168.1.225					ation bi	t D	-				.0 BSSMAN	₽
00.00.00	00 250		CM SER	VICE REQU	EST		26000			sage L	ength DURCE ME	CCACRC				= 26 (x1.	A)	
00.00.00	JU 200	00					26000			ssage '		SSAGES				- = 010101	11 COMPLE	ETE
00.00.00	00 250	00 ┥	CONNECT	TION COMP	LETE	_	26000		Ce	ll Iden	ntifier					=		
			AUTHENTI	ATION BE	QUEST						ifier(C	I) Identif				= 000001 = 8 (x08)	01 Cell 1 、	[de
00.00.00	00 250	00				-	26000					(Cell I				=00	•	
00.00.00	00 250	m L	AUTHENTIC	ATION RES	PONSE		26000			сс						= 404		
00.00.00	50 2.50					1	20000			NC Scetion	area o	ode				= 006	00000011	11
00.00.00	00 250	00 ┥	LIPHER M	IODE COM	MAND		26000			ell Id		.oue				= 1000 (0		
			CIPHER M	IODE COMP	LETE						Informat					=		
00.00.00	00 250	00 -				7	26000				ifier(I) Of Lever	.3INFO) : 3 Info				= 000101 = 13 (x0)		3
00.00.00	00 250	on 🖌	IDENTI	TY REQUE	ST		26000		L	ayer 3	Informs	tion					103000000	005
		··· •	TMSI REALLO									-		=		=		
00.00.00	00 250	00 ┥	TMOT NEALLU	JUATION C	JMMAND	-	26000				N MANAGE Discrim	MENT ME	SSAGE			=01	01 Mobili	itv
00.00.00	00 050		TMSI REALLO	CATION CO	OMPLETE		2000	T		та.			1			- 0000	77-12-3	
00.00.00	00 250 e Calls Graph		e Jitter Distribut		Model \lambda	_	26000 tets Graph	_	.38 Ana		Call Grand	n / Call Si						<u> </u>
/ Active	e calls Graph	A Averag	le onter Distribut	γr_{r}	model A	nirrack	leis uraph	_∧_'	. Jo Ana	Asis Yr	an urapi	A cars	unimary /					

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.

Mp Traffic File ⊻ie	: Analyzer - S w <u>C</u> all Sumi		iew tings <u>H</u> elp																_ 🗆 X
	ې 🎦 🤉	8 9		121 2	S SET	Ŧ		luCS Ca	ills			- Show	w All Ses	sions		-			
Call Sum	Call Summary Registraton Summary Alert Summary																		
Call #	SSRC	Payl		Packet Received	MOS/F		5/R			s		Sequen			Average Jitter	Average Inter Arri	Cumulativ Packet	Max/Min Gap	Max/Min I Delay ,
	00001 Caller: 235970329		9811 Callee: 378000	404060000 2498				tartTime:20 0 / 0.00			:41:25.96 ⁺ 0 / 0.00		on: 00:00:5 20.01		0.00	0	Ω	40.06	20/-12
% 1	235970323		7/8000 7/8000	2498				0/0.00	0/0.0		070.00	0 / 0.00	20.01	0.00	0.00	0	0	40.06	
										-				0.00					
-																			<u> </u>
TimeSta	mp	192.16	8.1.228			19:	2.168.1	.225		-	RANAI		RANAP La	yer ===		-	= = CH0	ICE	-
00.00.0	100 25	000	C	M SERVICE	E REQUE	EST	-	26000)		Choid	sibilit; e Index	•				= 0 = 0		
00.00.0	106 25	000	< ^{CO}	NNECTION	I COMPL	ETE		26000)		Pro	iatingM cedureC tents					= INT	UENCE EGER id-Init:	
00.00.0	107 25	000		HENTICATI	ION REC	QUEST		26000	כ		Cri	tents ticalit; tents	7				= ENU	id-Init: MERATOR ignore(
00.00.0	112 25	000	AUTH	IENTICATIO	ON RES	PONSE	-	26000) ,	-	Val							n Type	- /
00.00.0	117 25	000	◀	SecurityMo	odeContr	ol	_	26000	כ		Ext	tialUE-1 ensibil:		er			= 0	UENCE	
00.00.0	122 25	000		SecurityMo	odeContr	ol	-	26000)		Pi	amble otocolI		ner				UENCE O	F
00.00.0	126 25	000	◀───	IDENTITY F	REQUES	6T	_	26000)		Pi	eration otocolI rotocol	E-Contai					tance O UENCE	
00.00.0	135 25	000		REALLOCAT	TION CO	MMAND		26000	D			Protocol. Protoco. Content:	LIE-ID	L			= INT	EGER	nainInd -
00.00.0	139 25	000	TMSI F	EALLOCAT	TION CO	MPLETE		26000	1	•	•		•						
	e Calls Graph		erage Jitter D	istribution	λE-N	lodel λ	RTP	Packets G			.38 Analys	is 🔪 Call	Graph 🖉	Call Summ	ary /				
		~			~							~	~ ~						

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.

		and the second s	mmary ¥iew																	- 8
ile Vie	ew (Call Summary	Settings Help																	
5	Q	2	🕞 🕨 🔳	首图	sêr 🌾 📲	Sip Ca	lls	💌 SI	now All S	essions		-								
Call Sur	mmar	y Registrator	n Summary Alert S	ummary																
Call #	SS	SRC	Payload	Packet Received	Conversational MOS/R-Factor	Listenin MOS/R			issing ackets/(%)	Duplicate Packets/(%)	Out Of Sequen	Average Gap(ms)	Average Delay	Average Jitter	Average Inter Arri.	Cumulativ Packet	Max/Min Gap	Max/Min Delay	Max/Min Jitter	Max/M RTDela
Call#0	0000	01 Caller:000*	1@192.168.1.113 C	allee:0001@	192.168.1.228 Ca	IIId:GLPG72	55996165997 0	Call StartTime:20	13-03-04 12	48:51.761 Call D	uration: 00:00:	42.385	1							
61	1;	249503489	PCMU/8000	2119	4.20 / 93	4.20 /	93 070	.00 0	/ 0.00	0 / 0.00	0 / 0.00	20.01	0.00	0.00	0	0	40.00	20 / -1	1.32 /	0.000
e 1	1;	248450049	PCMU/8000	2121	4.20 / 93	4.20 /	93 070	.00 0	/ 0.00	0 / 0.00	0 / 0.00	20.01	0.00	0.00	0	0	40.03	20 / -1	1.31 /	0.000
Call#0	0000	02 Caller:0002	2@192.168.1.113 C	allee:0002@	192.168.1.228 Ca	IIId:GLPG72	56006166000 0	Call StartTime:20	13-03-04 12	48:51,762 Call D	uration: 00:00:	42.385								
2	1	250553089	PCMU/8000	2118	4.20 / 93	4.20 /	93 070	.00 0	/ 0.00	0 / 0.00	0 / 0.00	20.01	0.00	0.00	0	0	40.02	20/-1	1.317	0.000
2 2	1	246755841	PCMU/8000	2120	4.20 / 93	4 20 /			/ 0.00	0/0.00	0 / 0.00	20.01	0.00	0.00	0	0	40.01	20/-1	1.30 /	0.000
	0000	03 Caller 0003	3@192.168.1.113 C	allee:0003@		IIId:GLPG72	56016166003 0	Call StartTime:20	13-03-04 12	48:51 762 Call D		42 385								
		247025153	PCMU/8000	2118	4.20 / 93	4.20 /			/ 0.00	0 / 0.00	0/0.00	20.01	0.00	0.00	0	0	40.03	20/-1	1.30 /	0.000
303 23		248864769	PCMU/8000	2121	4 20 / 93	4 20 /			/ 0.00	0/0.00	0/0.00	20.01	0.00	0.00	ů.	ů.	40.01	20/-1	1.307	0.000
(•
Signalli	ing Pa	arameters		Value			Audio Parame	ters		Value	,		Video I	arameters				Va	alue	Î
Caller				0001@1	192.168.1.113		Src RTP Chan	nel		192	68.1.113: 102	4	Src Vid	eo Channe	1					
Callee					192.168.1.228		Src Media Tvp				J/8000			dia Type						
Calld				GLPG72	255996165997		Src SSRC			1249	503489		Src SS	c						
Call Sta	atus			Termina	ited		Src Packets C			2119				ket Count						
							Src Packets L			0/0				sing Pack						
Call Initi					3-04 12:48:51.761		Src Duplicate I			0/0				olicate Pac						
		ned Time			3-04 12:48:51.764			uence Packets .		0/0			Src Ou	of Sequer	nce / (%)					
Call Sto					3-04 12:49:34.150	_		onal MOS/R-Fac	stor	4.20				eo Frame o						
Call Dur				00:00:43	2.385		Src Listening N			4.20					rames/sec)					
Call Ter Call Fail				Caller			Src Discarded	Packets / [%] iter Arrival Jitter [DTCD	0/0	00		Src Ave Src Ave							
Call Fall	lure r	reason		-			Src Average In Src Average Ji		niurj	0.00				juap LIDF:MLR	1					
Section	Rea	uest Delay (m:	eec)	2.968			Src Average D			0.00				MDI(DF:M						
		connect Delay		0.738			Src Average G			20.0			JIC MY	prior(or .n	ien)					
0000001	10100	con noor b oldy	(11000)	0.100			olor noidgo a	op		20.0			Dest Vi	deo Chanr	nel					
Total Si	ignali	ng Frames		5			Dest RTP Cha	nnel		192.1	68.1.228: 102	4		edia Type	1990					
1 - 2 - 20	1972	33					Dest Media Ty	pe		PCM	J/8000		Dest St							
							Dest SSRC				450049			acket Cour						
							Dest Packets I			2121				issing Pacl						
							Dest Packets I			0/0				uplicate Pa						
							Dest Duplicate	Packets / (%)		0/0				ut of Seque						
•						+	AL. 0.4 - (C-	n-1/1/1	1.(%)	0.10	00	- LEG		deo Frame						
							12.17						I Dect Fr	ame Ratel	Frames/sec					

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 msecs.

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 msecs.

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 timestamp 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.



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	
	7	
Total SIP Packets		
Total SIP Packets SIP Calls	1	
Total SIP Packets SIP Calls SIP Active Calls	1	
Total SIP Packets SIP Calls SIP Active Calls SIP Completed Calls	1 0 1	
Total SIP Packets SIP Calls SIP Active Calls SIP Completed Calls SIP Purged Calls	1 0 1 0	
Total SIP Packets SIP Calls SIP Active Calls SIP Completed Calls SIP Purged Calls SIP Failed calls	1 0 1 0 0	
Total SIP Packets SIP Calls SIP Active Calls SIP Completed Calls SIP Purged Calls SIP Failed calls SIP Timed Out Calls	1 0 1 0 0 0 0	
Total SIP Packets SIP Calls SIP Active Calls SIP Completed Calls SIP Purged Calls SIP Failed calls SIP Timed Out Calls SIP ForceClosed Calls	1 0 1 0 0 0 0 0 0	
Total SIP Packets SIP Calls SIP Active Calls SIP Completed Calls SIP Purged Calls SIP Failed calls SIP Timed Out Calls SIP ForceClosed Calls Session Establishment Ratio	1 0 1 0 1 0 0 0 0 0 0 0 1 1 0 1 1 0 1 0	
Total SIP Packets SIP Calls SIP Active Calls SIP Completed Calls SIP Furged Calls SIP Failed calls SIP Timed Out Calls SIP ForceClosed Calls Session Establishment Ratio Session Establishment Effectiveness Ratio Session Defects	1 0 1 0 1 0 0 0 0 0 0 1 1 0 0 1 1 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1	
Total SIP Packets SIP Calls SIP Active Calls SIP Completed Calls SIP Purged Calls SIP Failed calls SIP Timed Out Calls SIP ForceClosed Calls Session Establishment Ratio Session Establishment Effectiveness Ratio	1 0 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0	

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	
	4 1000	
\setminus SIP \langle H323 $ angle$ RTP $ angle$ MEGACO $ angle$ GSN	иA λ 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 codes480, 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 codes500, 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
\setminus SIP λ H323 \langle RTP λ MEGACO λ GS	MA λ IUCS /

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 -
\setminus SIP λ H323 λ RTP λ MEGACO \langle GSI	MA λ 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	-
\setminus SIP λ H323 λ RTP \bigwedge MEGACO λ G	sma λ 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	
_		

I > ↓ 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 luCS(RANAP)Packets	30
TuCS Calls	1
IuCS Active Calls	0
IuCS Completed Calls	1
IuCS Purged Calls	0
TuCS Failed Calls	0
Voice Calls	1
SMS Calls	0
Location Update Calls	0
Setup Messages	1
Connect Messages	1
DisConnect Messages	1

 $|| \rangle$ RTP λ MEGACO λ GSMA λ 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 (commadelimited) 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

Export File Name ications Inc\PacketScan\Examples\DefaultExport.txt Columns to Export Call # SSRC Payload Packet Received Conversational MOS/R-Factor Listening MOS/R-Factor Listening MOS/R-Factor Listening MOS/R-Factor Listening MOS/R-Factor Duplicate Packets/(%) Duplicate Packets/(%) Average Gap(ms) Average Delay Average Jitter	Mp Export Displayed Summary	X
Call # SSRC Payload Packet Received Conversational MOS/R-Factor Listening MOS/R-Factor Listening MOS/R-Factor Packets Discarded/(%) Missing Packets/(%) Duplicate Packets/(%) Out Of Sequence Packets/(%) Average Gap(ms) Average Delay	Export File Name	
Call # SSRC Payload Packet Received Conversational MOS/R-Factor Listening MOS/R-Factor Packets Discarded/(%) Missing Packets/(%) Duplicate Packets/(%) Out Of Sequence Packets/(%) Average Gap(ms) Average Delay	ications Inc\PacketScan\Examples\E	DefaultExport.txt
Call # ▲ SSRC Payload Packet Received Select All Conversational MOS/R-Factor Export Listening MOS/R-Factor Export Packets Discarded/(%) Export Missing Packets/(%) Exit Out Of Sequence Packets/(%) Exit Average Gap(ms) Average Delay	Columns to Export	Export Headers
Average Jitter	SSRC Payload Packet Received Conversational MOS/R-Factor Listening MOS/R-Factor Packets Discarded/(%) Missing Packets/(%) Duplicate Packets/(%) Out Of Sequence Packets/(%) Average Gap(ms)	<u>S</u> elect All
	Average Jitter	-

Figure 153: Export Displayed Summary

- Select a directory to export the statistics using the browse button under the **Export File Nam**e 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

Export	Terminated Ca	alls Summary		×
Expo	ort To File			
C:	Program Files\GL	Communications Inc	\PacketScan\	
	Activate	Deactivate	<u>E</u> xit	

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, 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.xIsm 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.

Find Dialog	×
Tables Summary Table Columns Packet Received	Direction Down Up
Find What ? 800 Numeric Conditions C < • > • =	Find Next Get Count 6 Close
Alphanumeric Conditions Case Sensitive C Exact C Anywhere	

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 \red{P} 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

μα Traffic Analyzer - Summary View			_ 🗆 ×
File View Call Summary Settings Help			
🌠 🔎 🍓 兄 🕞 🕨 🖉 🕷 🎆 🖀	GSMA Calls	Show All Sessions	
Call Summary Registraton Summary Alert Summary	Sip Calls H323 Calls	<u> </u>	
Received MOS/P MOS/P Discord	Auto Detected RTP Calls Megaco Calls	rage Average Average Average Cumula [ms] Delay Jitter Inter Arri Packet	tiv Max/Min Max/Min M Gap Delay Ji
t	GSMA Calls luCS Calls	-	

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.

Document Number: PKV100-3.11.22-03

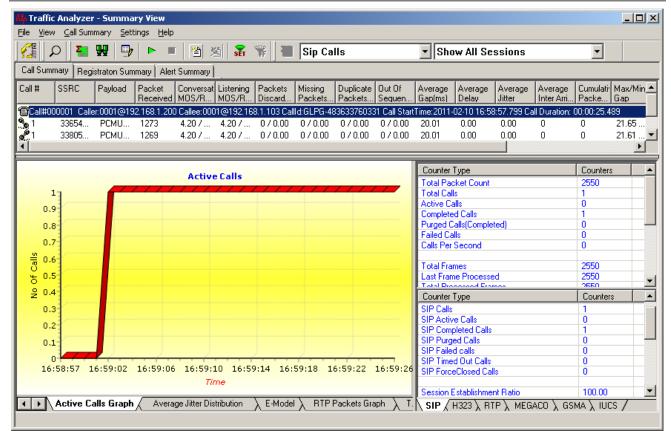


Figure 158: SIP Calls

GL Communications Inc.

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.

jie ⊻ie	w <u>C</u> all Sur	r - Summa Imary <u>S</u> et					_			_									
	<u>۵</u>	₩ 🖢		r 🛛 🖀 🗦	🗐 🔓	* 1	H323	Calls		🔹 She	ow All Se	ssions		•					
Call Sur	nmary Reg	istraton Sun	nmary Aler	t Summary	1		L												
Call #	SSRC	Payload	Packet Received			Packets Discard	Missing Packets	Duplicate Packets		Average Gap(ms)	Average Delay	Average Jitter	Average Inter Arri		Max/Min Gap	Max/Min Delay	Max/Min Jitter	Max/Min RTDela	
	000001 Call																		
9 1 1	18820 10234	PCMU PCMU	472 469	3.65 / 3.57 /		38 / 8 39 / 8		0 / 0.00 0 / 0.00	0 / 0.00 0 / 0.00	31.92 31.90	2.00 1.00	39.00 40.00	61 64	0 N	101.20 98.73	71 / -30 68 / -30	42.82 42.91	0.000 0.000	0.) 0.)
	10234 100002 Call							070.00 804001676			2010-12-15			~			42.91	0.000	0.
	34278	PCMU				38 / 8		0 / 0.00	0 / 0.00	31.91	1.00	39.00	61	0	98.39	687-30	42.91	0.000	0.1
2 2 2	24127	PCMU	445	3.61 /	3.65 /	37 / 8	0 / 0.00	070.00	0 / 0.00	31.90	2.00	39.00	64	0	98.98	68 / -30	42.73	0.000	0.1
1																			P
_													-			1	(
					Activ	e Calls						Counter	Type cket Count			Counte	rs		_^
	15											Total Pa				1860			
												Active C				ō			
	1.8											Complete				0			_
												Failed C	Calls(Comple	etedj		0			
	1.7												Second			Ő			
- Õ - T	1.6																		
ъ,	.5											Total Fra	ames ne Process			1860			
20	1,4											Counter				Counte	ers		
0	1.3											H323 Ca	alls			2			
0	.2												tive Calls			0			
C	.1												mpleted Ca irged Calls	lls		0			
	0	mm	mm	mm	mm	111111	<u>mm</u>	mm	TTTTT I			H323 Fa				0			
1	8:21:14 1	8:21:23	18:21:34	18:21:4	4 18:21	:54 18:2	2:04 18	:22:14 1	8:22:24	18:22:3	4								
					TI	ime						SetUp m	iessages Messaries			2			_

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.

Traffic Analyzer - Summary View																			
	<u>ہ</u>		• •	• 12 3	ST ST	¥ 1	Auto D	etected	RTP Call	s 🔻 Sh	ow All Se	ssions		•					
Call Summary Registraton Summary Alert Summary																			
Call #	SSRC	Payload	Packet	Conversat d MOS/R	Listening MOS/R	Packets Discard	Missing Packets	Duplicate Packets	Out Of Seguen	Average Gap(ms)	Average Delay	Average Jitter	Average	Cumulati Packe	Max/Min	Max/Min Delav	Max/Min Jitter	Max/Min RTDela	
n Call‡	#000001 Call	er:192.168.1		_							ion: 00:00:3		Tinter Ant.	.]1 dcke	Trap	[Deidy	Toricer	THI Dela	
0 1	32774	PCMU		4.20 /			0/0.00	0/0.00	0/0.00	20.01	0.00	0.00	0	0	21.58	17-1	0.72 /	0.000	0.0
2 1	42949	PCMU	0	0.00 / 0	0.00 / 0	0 / 0.00	0/0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.007	0/0	0.007	0.000	0.1
•																			Ī
												Counter	Tune			Counte			
					Activ	e Calls							icket Count			1487	15 <u> </u>		
		///	111	111	111				111	111		Total Ca				0			
												Active C				0			
	0.9											Complet				0			
	0.8											Failed C	Calls(Compl	eted)		0			_
	0.7												aiis r Second			0			
												Canor o	0000110			- ⁻			
Calls	0.6											Total Fra				1487			
ų	0.5												me Process			1487			
	0.4												ocessed Fra	ames		1487			_
_												Counter				Count	ers		4
	0.3												P Packets P Sessions			1483			
	0.2												P Sessions TP Session			0			
													ed RTP Se			2			
	0.1											RTP By				23728	0		
	0 16:26:36 1	6:26:39	16:26	:43 16::	26:47	16:26:5:	L 16:2	6:55 1	6:26:59	16:27	:03		CP Packel			4			
					T	ime							ender Repo			4			
												RTCP R	eceiver Re	ports		0			_
• •	Active C	alls Graph	Ave	rage Jitter Dis	tribution	∑ E-Mode	∥ <u>}</u> RTP	Packets Gr	aph) T	.38 Analysi	s ∖ CallG			TP / ME	GACO 🔪 (gsma λ il	ics /		

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.

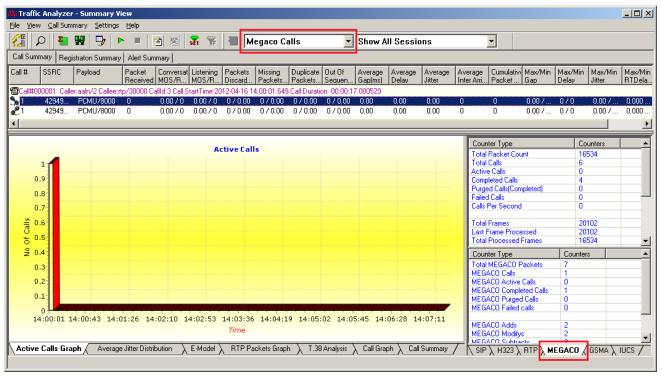


Figure 161: MeGaCo Calls

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.

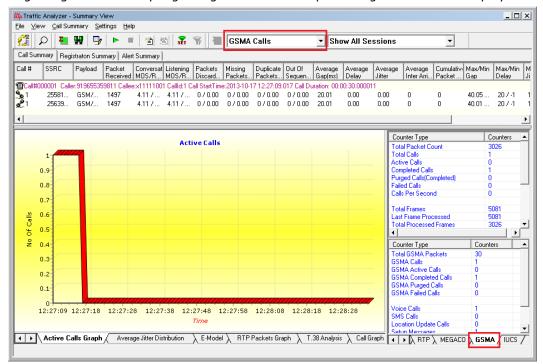


Figure 162: GSM A Calls

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.

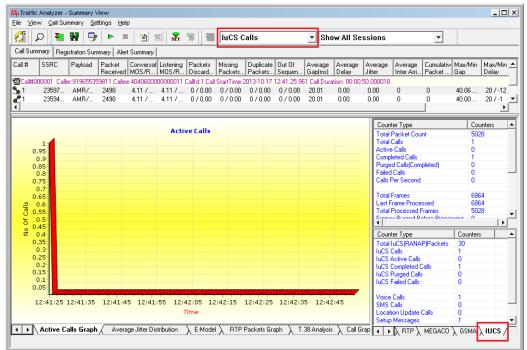


Figure 163: IuCS Calls

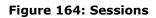
12.5.2 Filters

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 <u>Triggers and Action Settings</u> 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.

🕼 Tra	ffic Analyser - S	ummary	/ View							J×
File V	iew – Call Summar	y Settin	gs Help							
P	🅼 🎦 🔛	9	🕨 🔳 🛅 🤌	🖺 🛃 🏋	📲 Sip Ca	alls	•	Show All Sessions	•	
Call St	ummary Registrat	on Summ	ary Alert Summary	Show All Sessions						
Call #	SSRC	Payload	Packet Received	Conversational MOS/R-Factor	Listening MOS/R-Factor	Packets Discarded/(%)	Missing Packets/(%)	Show Active Sessions Only Show Completed Sessions Only Show Video Sessions Only		erage lay
			168.1.231 Callee:0	001@192.168.1.	.237 Callid:GLPG	6134071277639	182 Call StartT	Show User Defined Sessions	0	0:00:4
% 1	957412353 957785601	PCM PCM	1889 1889	2.12 / 43 2.21 / 45	2.17 / 44 2.27 / 46	38 / 1.83 5 / 0.24	194 / 9.33 194 / 9.32	Show Fax Calls		00 00
9 .	337763601	гсм	1003	2.21743	2.27740	570.24	1347 3.32	Show Failed Calls Show GSM Voice Calls	þ	
								Show SMS Calls Show Location Update Calls	•	



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 ቻ 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.

CallNum_1.rtf - WordPad	
File Edit View Insert Format Help	
Signalling Parameters	
Call#:	1
Caller:	55523230192.168.30.15
Callee:	54000@192.168.30.200;user=phone
Start Time:	2007-11-08 01:16:19.000677
Stop Time:	2007-11-08 01:16:42.000152
Call Duration:	00:00:22.000450
Audio Session Parameters	
Src IP:	192.168.30.15
Src Port:	6520
Dest IP:	192.168.30.200
Dest Port:	17800
Codec Type:	PCMU/8000
Fax Session Parameters	
Src IP:	192.168.30.15
Src Port:	6522
Dest IP:	192.168.30.200
Dest Port:	17800
Codec Type:	T.38
 For Help, press F1	NUM

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.

🚜 Save Call	<u>×</u>
Call(s)	Selected Call(s)
CallNum_2 CallNum_3	CallNum_1
O HDL File 💿 PCAP File	🔽 Call Summary
Path D:\Program Files\GL Communic	cations Inc\PacketScan\Examples\Othe
✓ Overwrite Files Save Call	(s) Exit

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:

Reports	×
All Calls	
C Current Calls	
🔿 Call Range 🖉	
Choose Format PDF	•
Rtp	
 SSRC PayLoad PacketReceived ConversationalMOS-R-Factor ListeningMOS-R-Factor PacketsDiscarded MissingPackets DuplicatePackets OutOfSequencePackets 	
File Name s\Nagaraj\Desktop\1.pdf	
🗖 Overwrite Files	
Save Cancel	

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.

×
CallSummary Report Exported Successfully
OK

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

reate 🗸 🛛 🎮		ې چ چ	3 🖪 🖪	a. Sa									
eate •													
	/ 3 🔘 🔘 🗍	V V	Q ^{\$} 😑	71.4	% 🔻 🔝) 🚨 🗄	i 🕀 🗄 🛛) KK DD		R =	Tools Co	mment S
_													
	\sim T												
	Τ			C	all St	umma	ry Re	eport					
Communic	ations Inc										Report Generated On:	3/4/2013 2:1	7:44PM
Communic	auons me.												
Call# 1	Callid: GLPG7255996165	5997	c	aller: 0001@1	92.168.1.228		Callee: 0001@1	92.168.1.113	Ca	allStartTime: 20	13-03-04 12:48:51.761	CallDuration: 0	0:00:42.385
SSRC	Payload	Total Packets Count	CMOS /R-factor	LMOS/ R-Factor	Packets Discarded(%)	MissingPacket Count(%)	Dupl.Packet Count(%)	OutofSequence Packet count(%)	Avg InterArrivalJitter	Cumulative Packet lost	Gap(Max/Min/Avg)	Delay(Max/Min/Avg)	Jitte(Max/Min/Avg
1249503489	PCMU/8000		4.20 / 93	4.20/93	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0	0	40.00 / 18.98 / 20.01		
1248450049	PCMU/8000		4.20 / 93	4.20/93	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0	0	40.03 / 18.96 / 20.01		
Call# 2	CallId: GLPG7256006166	3000	c	aller: 0002@1	92.168.1.228		Callee: 0002@1	92.168.1.113	Ca	allStartTime: 20	13-03-04 12:48:51.762	CallDuration: 0	0:00:42.385
SSRC	Payload	Total Packets Count	CMOS /R-factor	LMOS/ R-Factor	Packets Discarded(%)	MissingPacket Count(%)	Dupl.Packet Count(%)	OutofSequence Packet count(%)	Avg InterArrivalJitter	Cumulative Packet lost	Gap(Max/Min/Avg)	Delay(Max/Min/Avg)	Jitte(Max/Min/Avg
1250553089	PCMU/8000		4.20 / 93	4.20/93	0 / 0.00	0 / 0.00	0/0.00	0 / 0.00	o	0	40.02 / 18.95 / 20.01		
1246755841	PCMU/8000		4.20 / 93	4.20/93	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0	0	40.01 / 18.95 / 20.01		
Call# 3	CallId: GLPG7258018186	3003	c	aller: 0003@1	92.168.1.228		Callee: 0003@1	92.168.1.113	Ca	allStartTime: 20	13-03-04 12:48:51.762	CallDuration: 0	0:00:42.385
SSRC	Payload	Total Packets Count	CMOS /R-factor	LMOS/ R-Factor	Packets Discarded(%)	MissingPacket Count(%)	Dupl.Packet Count(%)	OutofSequence Packet count(%)	Avg InterArrivalJitter	Cumulative Packet lost	Gap(Max/Min/Avg)	Delay(Max/Min/Avg)	Jitte(Max/Min/Avg
1247025153	PCMU/8000		4.20 / 93	4.20/93	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0	0	40.03 / 18.94 / 20.01		
	-								0	0	40.01 / 18.95 / 20.01		

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:

🗤 Exract Fax Image from Call	×
Call(s)	Selected Call(s)
CallNum_1	
	←
<u> </u>	
Path C:\Program Files\GL Communi	cations Inc
✓ Overwrite Files Extract I	

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.

Play - Jitter Options	<u>×</u>
Options Corrected As Is Extract Mix Option Mix Stereo Seperate	Jitter Buffer Option Static Dynamic Jitter Buffer Len 100 msec Dynamic Jitter Buffer Option Min Delay 40 msec Max Delay 100 msec Fill with Last Packet Set Default
Start from beginning	Select other Sessions for Playback OK Cancel

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.

Write To File - Jitter	Options X							
- Options	Jitter Buffer Option							
Corrected	C Static 💿 Dynamic							
C As Is	Jitter Buffer Len 100 msec							
C Extract	Dynamic Jitter Buffer Option							
Mix Option	Min Delay 40 msec							
• Mix	Max Delay 100 msec							
C Stereo								
C Separate	Fill with Last Packet Set Default							
Start from beginning File Record Use SSRC for File Name								
D:\Program Files\GL Communications Inc\PacketScan\TRACE								
🔲 Invoke Cool Edi	t after write							
	OK Cancel							

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.

Document Number: PKV100-3.11.22-03

<mark>ስሻ</mark> ρ Traff	ic Analyzer	[.] - Summa	ry Yiew							_	
File Vie	w – Call Sum	mary Set	tings Help								
	ר¢	₩ 🛛 🗩	► ■	Write To File - Jitter	Dptions		×	how All Se	ssions		-
Call Sur	nmary Regi	istraton Sun	nmary Alert	Options	-Jitter Buffer Option-		[
Call #	SSRC	Payload	Packet	 Corrected C As Is 	 Static D Jitter Buffer Len 	ynamic 100 msec		e Average 3) Delay	Average Jitter	Average Inter Arri	Cumuk
	000001 Calle		192.168.20.	C Extract	Dynamic Jitter Buff	1	- I B	206@192.168	3.20.223 Cal	II StartTime:	2004-03
% 1	21693 22512	PCMU PCMU	2997 3534	Mix Option	Min Delay	40 msec		0.00 0.00	0.00 0.00	0 49	0 0
				Mix Stereo	Max Delay	100 msec					
				C Separate	Fill with Last Pac	cket Set Default					
				· · · · · · · · · · · · · · · · · · ·			- [Counter Typ	ре	
				🛛 🗖 Start from beginning]				Total Packe	et Count	
1			//////	File Record			- 1		Total Calls Active Calls		
				📃 🗖 Use SSRC f 🗗	e Name				Completed (Calls	
S S S S S S S S S S S S S S S S S S S				D:\Program Files\GI	. Communications Inc\P	acketScan\Exampl	-		Purged Calls Eailed Calls		<u>1)</u>
ů,				-	file will be written				4		
No of Calls					oth left and right see				Counter Typ		•
-									Total SIP Pa SIP Calls	ackets	
_		1	4	🔲 Invoke Cool Edit	after write				SIP Cails SIP Active (Calls	
16	38:42 16:38	3:48 16:3	8:55 16:39						SIP Complet	ted Calls	
	Active Ca	alla Grach	Auero		OK Cancel			isis 🗼 Cal 🗔			
لغنعا	ACUVE	ans urapr	A Averag				ənay			IP / H323	Увін

• **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.

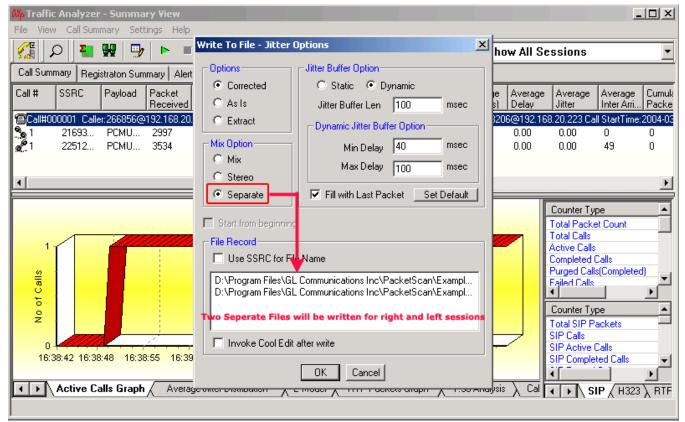


Figure 173: Write to File with Separate Option Selected

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

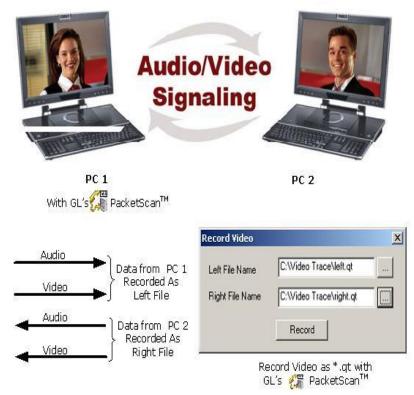
This option will allow the user to record audio and video data of a session to a file in QuickTime format.

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.

🖧 Traffi	c Analyser	- Summa	ry View												_ 🗆 🗵
<u>File Viev</u>	v – <u>C</u> all Sum	mary <u>S</u> ett	ings <u>H</u> elp	l.											
	Ω ≅	W 🖓		1 🖀 3	र्ध 👔	¥ 4	Sip Ca	lls		- Sho	w Video	Sessior	is Only	•	
Call Sum	mary Regi	straton Sum	mary Aler	t Summary											
Call #	SSRC	Payload	Packet Received	Conversat MOS/R			Missing Packets	Duplicate Packets			Average Delay	Average Jitter	Average Inter Arri	Cumulativ Packet	
	00001 Calle	r:test4@19	2.168.10.4	5 Callee:test	3@192.168	3.10.14 Call	ld:211ea02	68e7e463d(@dGVzdD0	Q. Call Start	[ime:2002-1	10-05 14:30	:28.000157	Call Duratio	on: 00:00:22.0
S _1	20617	PCMU	1391	4.14 /	4.16 /	7 / 0.50	0 / 0.00	6 / 0.43	0 / 0.00	19.89	0.00	3.00	5	0	86.26 6
e 1	19892	PCMU	1355	4.14 /	4.18 /	3 / 0.22	0 / 0.00	3 / 0.22	0 / 0.00	19.96	0.00	2.00	15	0	105.93 5
% 1 % 1 % 1	22391	h263-2	996	n/a	n/a	n/a	0 / 0.00	0 / 0.00	070.00	n/a	n/a	n/a	n/a	n/a	n/a r
2 1	18161	h263-2	417	n/a	n/a	n/a	0 / 0.00	0 / 0.00	0 / 0.00	n/a	n/a	n/a	n/a	n/a	n/a r
															Þ

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 <u>Video Parameters</u>.

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.

Record Video	×
Left File Name	C:Wideo Trace\left.qt
Right File Name	C:\Video Trace\right.qt
	Record

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.

Record Video	X
Audio Session ID	1
Video Session ID	2
File Name	C:\Video Trace\video.q
	Record

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
Т	Mean one way delay of the echo path
Tr	Roundtrip delay in a closed 4-wire loop
Та	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
А	Advantage factor

E-model Base Parameters			×
Send Loudness Rating (SLR)	8	÷	dB
Receive Loudness Rating (RLR)	2	÷	dB
Sidetone Masking Rating (STMR)	15	÷	dB
D-Value of handset, Send Side (Ds)	3	÷	
D-Value of handset Receive Side(Dr)	3	÷	
Talker Echo Loudness Rating(TELR)	65	÷	dB
Weighted Echo Path Loss(WEPL)	110	÷	dB
Mean one-way Delay of the Echo Path(T)	0	÷	msec
Round Trip Delay in a 4-wire Loop (Tr)	0	÷	msec
Absolute Delay in echo-free Connections(Ta)	0	÷	msec
Equipment Impairment Factor(Ie)	0	÷	
Packet-loss Robustness Factor(Bpl)	1	÷	
Random Packet-loss Probability(Ppl)	0	÷	%
Circuit Noise referred to 0 dBr-point(Nc)	.70	Ŧ	dBmOp
Room Noise at the Send Side(Ps)	<u> </u>	Ē	dB(A)
Room Noise at the Receive Side(pr)	<u> </u>	Ē	dB(A)
	100	-	, í
Ok Set Default Valu	ies		

Figure 178: E-model Parameters

12.6.2 VQMon Settings

VQMon Settin	gs	×				
Jitter Buffer	Emulator - Summa	ary —				
Туре	Adaptive 💌					
Minimum	40	ms				
Nominal	40	ms				
Maximum	100	ms				
Jitter Buffer	Jitter Buffer Emulator - Detail Analysis					
Туре	Adaptive 💌					
Minimum	40	ms				
Nominal	40	ms				
Maximum	100	ms				
-VQMon Star	ndards					
O Japan	North Americ	ca				
-VQMon CMI	VQMon CME Modal					
C Linear	O Linear 💿 Non Linear					
<u>0</u> k	Set <u>D</u> efa	ault				

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 PacketScanTM.

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:

Audio Codec	PayLoad 🔺
ALAW	8
MuLAW	0
G726_40	96
G726_32	97
G726_24	98
G726_16	99
G723	4
G729	19
G729B	18
GSM610	3
AMR	100 🗸
€linn	
▲	

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

Document Number: PKV100-3.11.22-03

- 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, ½ 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, ½ and 1) (optional codec)
- EVRC_C (optional codec)
- G711 application II (A-law and μ -law with Voice Activity Detection).
- <u>H.263+</u> providing video capture and videoconference monitoring capability.
- <u>H.264</u> 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.

Codec Parameters Settings				
Codec Type G726 AMR EVRC G722_1 AMR_WB EVRCB EVRCB EVRCC G726_VAD	G726 Selection			

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.

Codec Parameters Settings				
Codec Type G726 AMR EVRC G722_1 AMR_WB EVRCB EVRCB EVRCC G726_VAD	Rtp Packet Format Band Width Effective Mode Band Width Effective Mode Octate Aligned Mode			

Figure 182: AMR Codec Type

In EVRC / EVRCO 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.

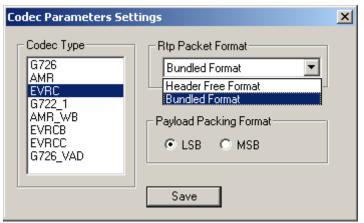


Figure 183: EVRC Codec Type

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.

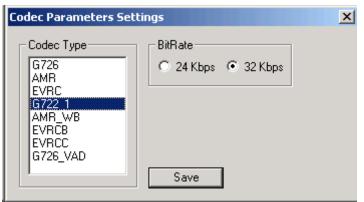


Figure 184: G722.1 Codec Type

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.

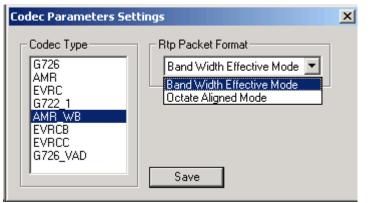


Figure 185: AMR_WB Codec Type

In **EVRCB / EVRCBO 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.

Codec Parameters Settings				
Codec Type G726 AMR EVRC G722_1 AMR_WB EVRCB EVRCC G726_VAD	Rtp Packet Format Bundled Format Header Free Format Bundled Format Payload Packing Format © LSB © MSB Save]		

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.

Codec Parameters Settings				
Codec Type G726 AMR EVRC G722_1 AMR_WB EVRCB EVRCB EVRCC G726_VAD	Rtp Packet Format Bundled Format Header Free Format Bundled Format Payload Packing Format © LSB © MSB Save			

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.

odec Parameters Settings				
Codec Type G726 AMR EVRC G722_1 AMR_WB EVRCB EVRCB EVRCC G726_VAD	G726VAD Selection RTP C AAL Save			

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:

Trigger List	Filter Selection	
☑ Trigger1	Calling Party Calling Party Called Party Called Party Calles Calls Call complete Calls Failed Calls Call Duration (mins) Call Duration (mins) Session Disconnect Dek	
Enter Trigger Name	Enter String Value	ditions
Add Delete	Activate DeActivate	And Or
Save Call Audio Recording User Defined Send e-mail	ave Call To File Options ile Name Mask &]_%Y_%M_%D_%h-%m-%s	Save Options HDL File PCAP File
Alert Summary Call Detail Record	iles Destination Directory C:\Program Files\GL Communications reate File Options If File Exists Overwrite C Skip Operation C Append	Call Summary
		o oquence muniber

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.

Action Save Call	Save Call To File Options	Save Options-
Audio Recording	File Name Mask	HDL File
User Defined	%I_%Y_%M_%D_%h-%m-%s	C PCAP File
 ✓ Send e-mail ✓ Alert Summary ✓ Call Detail Record 	Files Destination Directory C:\Program Files\GL Communications	🗖 Call Summary
Extract Fax Image	Create File Options If File Exists Overwrite O Skip Operation O Append	Sequence Number

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-%. 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.

- Action	
Save Call	Audio Recording Options
Audio Recording	Audio File Name Mask
🗹 User Defined	%I_%Y_%M_%D_%h-%m-%s.wav
Send e-mail	Audio Files Destination Directory
Alert Summary	\GL Communications Inc\PacketScan
Extract Fax Image	Audio Mixing Options
	Create File Options If File Exists © Overwrite © Skip Operation © Append Sequence Number

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-%**. 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 Numbe**r.

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 (`;').

Action Save Call Audio Recording	🔽 Call Summar	y 🔽 Save to HDL File 🔽 Audio Recording
User Defined	Server Name	gl.com
✓ Send e-mail ✓ Alert Summary	From	user@gl.com
Call Detail Record	To	user1@abc.com
	CC	user2@abc.com, user3@xyz.com
	BCC	user4@abc.in
	Subject	Files

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.

Action	
Save Call	Alarm Type Warning 💌
Audio Recording	
🗹 User Defined	Alarm Message Triggers at the specified value
Send e-mail	
Alert Summary	
Call Detail Record	
Extract Fax Image	

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 <u>Call Data Records</u> and <u>Voice Band Application</u> 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.

Action
✓ Save Call ✓ Call Side Record Probe Name VolPProbe ✓ Audio Recording ✓ Call Master Record ✓ Call Master Record ✓ Send e-mail ✓ Call Events Record ✓ Call Events Record ✓ Call Detail Record CSV Files Destination Directory ✓ Call Detail Record C:\Program Files\GL Communications ✓ Extract Fax Image ✓ Use Sub Folders Folder Prefix ✓ OIPCaptures Create Subfolder Every 1 → hr Create File Options If File Exists Overwrite O Verwrite Skip Operation Append Sequence Number

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

R	V	DIPProb	GLPG-	870468	7841631	2012 0	07_12_15-13	3-54 csr.csv	- Micros	oft Excel														- 0	= x
		AE			6		f∝ Min Ji																		≯
	1	Α	В	С	D	E	F	G	н	1	K	M	0	Q	R	S	Т	U	Х	AA	AD	AE	AF	AG	
1	P	robe ID	Call ID	Side	Address	File	NSSRC	Codec	Tot Pkts	Mis Pkts	Dup Pkts	Reo Pkts	Del Pkts	Conv MOS	Conv R	Lstn MOS	Lstn R	Avg Gap	Avg Del	Avg Jit	Avg IA Jit	Cum Pkts	Inband M	Outband N	лс і 🚍
2	V	olPProb	GLPG-	87 Left	0004@1	VolP	F 2.59E+09	PCMU/800	53	0	0	0	0	4.2	93	4.2	93	27.34	0	0	2	0		1.23E+09	
3	V	olPProb	GLPG-	Right	0004@1	VolP	F 2.59E+09	PCMU/800	72	0	0	0	0	4.2	93	4.2	93	25.22	0	0	2	0		1.23E+09	
4																									
5																									
H	•	► H _ \	/oIPPro	be GL	PG-8704	6 878 4	1631 20	2																	
Re	ead	у 🛅															Av	erage: 0	Count: 6	Sum: 0		85%)0		Ð.,;

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.

	/oIPProbe_G	LPG-1173483	7841613_201	12_07_12_15-	-08-54_cmr.cs	v - Microsoft	Excel								-	= X
	A1	•		∫∗ Prob	e ID											×
	А	В	С	D	E	F	G	Н	1	J	К	L	М	N	0	-
1	Probe ID	Call ID	Side 1	Side 2	Protocol	Start	Released	Duration	Orig	Term	Rel Code	Src Dir	Arch Dir	P-D Delay	SD Delay	
2	VolPProb	GLPG-117	Left	Right	SIP	*****	*****	0:00:19	Left	Left	Normal Ca	C:\Docum	ents and S	3	2	2
3																w
14 4	VoII	PProbe_GLP	PG-1173483	87841613_2	<u>/</u> \$7/					1 4						
Rea	dy 🎦												100%		0	+ ,;;

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

9	- (°I -	<u>à</u> =														
	A1	-	(<i>f</i> _∞ P	robe ID											
4 ^{mmn}	А	В	С	D	E	F	G	н	- I	J	К	L	М	N	0	Р
Pro	obe ID	Call ID	Side	Class I	D Class	Code ID	Code	Data	Start	Dur	Src IP Add	Dest IP Ad	Src Port	Dest Port	SIP CSeq	Values
Vo	IPProbe	GLPG-8704	Left		6 SIP	C	INVITE		0	0	192.168.1.	192.168.1.	54098	5060	1 INVITE	
Vo	IPProbe	GLPG-8704	Right		6 SIP	C	SIP/2.0 10	0 Trying	0.002351	0	192.168.1.	192.168.1.	54098	5060	1 INVITE	
Vo	IPProbe	GLPG-8704	Right		6 SIP	C	SIP/2.0 18	80 Ringing	0.002864	0	192.168.1.	192.168.1.	54098	5060	1 INVITE	
Vo	IPProb e	GLPG-8704	Right		6 SIP	C	SIP/2.0 20	00 OK	1.523548	0	192.168.1.	192.168.1.	54098	5060	1 INVITE	
Vo	IPProbe	GLPG-8704	Left		6 SIP	C	ACK		1.524939	0	192.168.1.	192.168.1.	54098	5060	1 ACK	
Vo	IPProb e	GLPG-8704	Right		7 Out-Band	C	MF 1		14.02465	0.1			0	0		pwr = 15.0
Vo	IPProb e	GLPG-8704	Right		7 Out-Band	C	MF 2		14.20425	0.1			0	0		pwr = 15.0
Vo	IPProb e	GLPG-8704	Right		7 Out-Band	C	MF 3		14.38393	0.1			0	0		pwr = 15.0
Vo	IPProb e	GLPG-8704	Right		7 Out-Band	C	MF 4		14.56462	0.1			0	0		pwr = 15.0
Vo	IPProb	GLPG-8704	Right		7 Out-Band	C	MF 5		14.74442	0.1			0	0		pwr = 15.0
Vo	IPProbe	GLPG-8704	Right		7 Out-Band	C	MF 6		14.92498	0.1			0	0		pwr = 15.0
Vo	IPProbe	GLPG-8704	Right		7 Out-Band	C	MF 7		15.10461	0.1			0	0		pwr = 15.0
Vo	IPProbe	GLPG-8704	Left		7 Out-Band	C	MF 1		15.17658	0.06			0	0		pwr = 10.0
Vo	IPProb e	GLPG-8704	Left		7 Out-Band	C	MF 2		15.31625	0.06			0	0		pwr = 10.0
Vo	IPProbe	GLPG-8704	Right		7 Out-Band	C	MF 8		15.28423	0.1			0	0		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

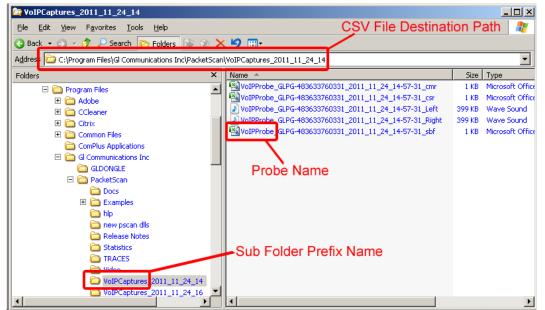
<Probe ID>_<Call ID>_<year>_<Month>_<Date>_<hour>-<minute>-<second>_cmr.csv

Example: VoIPProbe_GLPG-483633760331_2011_11_24_14-57-31_csr.csv

VoIPProbe_GLPG-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 Numbe**r.

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.

Action Save Call	Extract Image From Fax Call
Audio Recording	File Name Mask
User Defined	%I_%Y_%M_%D_%h-%m-%s
🗹 Send e-mail	Files Destination Directory
Alert Summary	C:\Documents and Settings\Shivanad
Call Detail Record	

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.
- 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.

<mark>Mp</mark> Traffic	: Analyzer	- Sur	nmary Vi	ew									- 🗆 🗵
File View	/ Call Sum	mary	Settings	Help									
Call Sum	O	997 strator	E-mod	ad Map Table el Base Parameters n Settings		* = 	Sip Calls	\$	1	Show	All Sess	ions	
Call #	SSRC	Paylo		Parameter Settings	rsa R	t Listening MOS/R	Packets Discard	Missing Packets	Duplicate Packets		Average Gap(ms)	Average Delay	Average Jitter
			🗸 Enable	rs and Action Settings #Disable Triggers tartup Options								•	

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

PDA Startup Options	×				
Execute Tasks On PDA Startup Startup Tasks Free Enable Triggers And Actions	Open Look in:	PacketScan		¢ € 💣	?×
Triggers And Actions Profile	My Recent Documents Desktop My Documents My Computer	Docs Examples Hip Release Notes Statistics TRACES Video			
	My Network Places	File <u>n</u> ame: Files of <u>type</u> :	Trigger1.tgr Trigger Files (".tgr) Open as <u>r</u> ead-only	•	<u>O</u> pen Cancel

Figure 202: Loading tgr Profile File

The Trigger and Action profile path will be displayed in sipProt.ini file. Refer to the figure below:

📄 sipProt.ini - Notepad	
Eile Edit Format View Help	
sum.0=Type	
[DEF_SUM_RSVP.4]	
sum.0=Class	
sum.1=Message Type [DEF_SUM_Cisco EIGRP.4]	
sum.0=Packet Type Opcode	
[DEF_SUM_USPS Protocol.4]	
[DEF_SUM_Remote Procedure Call.4]	
[DEF_SUM_AppleTalk Transaction Protocol Packet.4]	
[DEF_SUM_Routing Table Maintenance Protocol.4]	
[DEF_SUM_ICMPV6.4]	
[DEF_SUM_PIM-SM / PIM-DM.4]	
[[DEF_SUM_PIM IP.4] [[DEF_SUM_PIM Udp.4]	
sum. O=Destination Port	
sum.1=Source Port	
[DEF_SUM_PIM TCp.4]	
sum.0=Destination Port	
sum.1=Source Port	
[DEF_SUM_ICMP.4]	
[DEF_SUM_Cisco Inter-Gateway Routing Protocol (IGRP).4]	
[DEF_SUM_USPF.4]	
sum. O=Message Type	
[DEF_SUM_MOBileIP(IPv6).4]	_
[PDA_STARTUP_TASKS]	
ENABLE_STARTUP_TASKS=1	
ENABLE_TRIGGERS=1	
TRIGGERS_PROFILE_NAME=C:\Program Files\GL Communications Inc\PacketScan\Trigger1.	tgr
[PERIODIC_TRACE_SAVE] FILE_NAME_TYPE=0	
	• //

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 Courses Desidentes Courses Alert Summary													
Call Summary Registraton Summary Alert Summary													
Call# Protocol Message Type Threshold Value Caller Callee Callid													
	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					
	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					
	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					
	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					
	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					
	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					
	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					
	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					
	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					
	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					
	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 P 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 \wp from the tool bar.

	2	9	▶ ■ 🏝	湾 3	r 🐃 🔤 📲 🔤	Sip Cal	ls	•	Show	All Sessions		•	
Call Summar,	ע Registrat	on Summa	ry∫Alert Summa	w 📃									
Packet #	Sequen	RTP	Payload Type	Paylo	Packet Sequ	Ga▲	Packet #	Sequen	RTP	Payload Type	Paylo	Packet Sequ	Ga
M 5	49759	3939	PCMU/8000	160	Session In Pr	0.	118	48259	1766	PCMU/8000	160	Session In Pr	0.
6	49760	3939	PCMU/8000	160	Session In Pr	22.	121	48260	1766	PCMU/8000	160	Session In Pr	21
7	49761	3939	PCMU/8000	160	In Sequence	55.	122	48259	1766	PCMU/8000	160	Duplicate Pa	0.
8	49762	3939	PCMU/8000	160	In Sequence	10.	124	48261	1766	PCMU/8000	160	In Sequence	21
9	49763	3939	PCMU/8000	160	In Sequence	10.	127	48264	1766	PCMU/8000	160	Jump Within	64
10	49765	3939	PCMU/8000	160	Jump Within	21.	128	48261	1766	PCMU/8000	160	Duplicate Pa	0.
11	49764	3939	PCMU/8000	160	Out Of Order	0.0	131	48265	1766	PCMU/8000	160	In Sequence	10
12	49767	3939	PCMU/8000	160	Jump Within	42.	132	48266	1766	PCMU/8000	160	In Sequence	21
16								10005	1700	DOLULIO000	100	D F I D	-
13	49766	3939	PCMU/8000	160	Out Of Order	0.1	133	48265	1766	PCMU/8000	160	Duplicate Pa	U.
13 14	49766 49768	3939 3939	PCMU/8000 PCMU/8000	160 160	Out Of Order In Sequence	21.	135	48265	1766	PCMU/8000 PCMU/8000	160	In Sequence	21
13													0.
13 14			PCMU/8000	160		21.	135			PCMU/8000	160		21
13 14 Heading			PCMU/8000	160 		21.	135 ◀ Heading			PCMU/8000	160 Ie		21
13 14 Heading	49768		PCMU/8000	160 Je 4759169	In Sequence	21.	135	48267		PCMU/8000	160 160 160 160 160 160	In Sequence	21
13 14 Heading SSRC Source IP A	49768		PCMU/8000 Valu 351 192	160 	In Sequence	21.	135 ◀ Heading	48267		PCMU/8000 Valu 114: 192	160 Ie	In Sequence	21
13 14 Heading SSRC Source IP A Destination	49768 49768 uddress IP Address		PCMU/8000 Valu 351 192 192 102	160 4759169 .168.1.232 .168.1.195 4	In Sequence	21.	135	ddress IP Address		PCMU/8000 Valu 114: 192 192 102:	160 160 3281025 168.1.195 168.1.232 4	In Sequence	21
13 14 Heading SSRC Source IP A Destination Source Port	49768 Address IP Address Port		PCMU/8000 Valu 351 192 192 102 102	160 4759169 .168.1.232 .168.1.195 4	In Sequence	21.	135 ▲ Heading SSRC Source IP A Destination Source Port Destination	48267 ddress IP Address Port		PCMU/8000 Valu 114: 192. 192. 102: 102:	160 160 3281025 168.1.195 168.1.232 4	In Sequence	21
13 14 Heading SSRC Source IP A Destination Source Port Destination RTP Packe	49768 Address IP Address t Port ts Count		PCMU/8000 Valk 351 192 192 102 102 710	160 4759169 .168.1.232 .168.1.195 4	In Sequence	21.	135 ▲ Heading SSRC Source IP A Destination RTP Packe	ddress IP Address Port ts Count		PCMU/8000 Valu 114 192 192 102 665	160 160 3281025 168.1.195 168.1.232 4	In Sequence	21
13 14 Heading SSRC Source IP A Destination Source Port Destination RTP Pack RTP Pack	49768 Address IP Address Port its Count cets Count	3939	PCMU/8000 Valu 351 192 192 102 102 710 2	160 4759169 .168.1.232 .168.1.195 4	In Sequence	21.	135 ▲ Heading SSRC Source IP A Destination Source Port Destination RTP Packe RTCP Pack	ddress IP Address Port ts Count ets Count		PCMU/8000 Valu 114* 192 192 102* 102* 665 2	160 160 3281025 168.1.195 168.1.232 4	In Sequence	21
13 14 SSRC Source IP A Destination Source Port Destination RTP Packe Packets Wil	49768 address IP Address Port rts Count rets Count th Marker Bit	3939	PCMU/8000 Valu 351 192 192 102 102 710 2 11	4759169 168.1.232 168.1.199 4	In Sequence	21.	135 ▲ Heading SSRC Source IP A Destination Source Port Destination RTCP Packets Wi	48267 ddress IP Address Port ts Count ets Count th Marker Bit		PCMU/8000 Valu 114 192 192 192 102 102 102 02 0	160 9281025 168.1.195 168.1.232 4 4	In Sequence	21
13 14 Heading SSRC Source IP A Source Port Source Port Source Port Source Port Pestination NTP Packe Packets Wil Joak Wil	49768 IP Address IP Address Port ts Count ts Count th Marker Bit Bytes	3939	PCMU/8000 Valk 351 192 192 102 102 710 2 113	4759169 168.1.232 168.1.199 4	In Sequence	21.	135 ▲ Heading SSRC Source IP A Destination Source Port Destination RTP Packe RTCP Packe RTCP Packets Wi Total Audio	ddress IP Address Port ts Count ets Count th Marker Bit Bytes		PCMU/8000 Valu 114: 192 102: 102: 665 2 0 106:	160 9281025 168.1.195 168.1.232 4 4	In Sequence	21
13 14 Heading SSRC Source IP A Source IP A Destination Str Packe Str Packets Wil Orat Audio RTCP Send	49768 address IP Address Port rts Count rets Count th Marker Bit	3939	PCMU/8000 Valu 351 192 192 102 102 710 2 11	4759169 168.1.232 168.1.199 4	In Sequence	21.	Heading SSRC Source IP A Destination Source Port Destination RTP Packe RTCP Pack RTCP Packets Wi Total Audio RTCP Send	ddress IP Address Port ts Count ets Count th Marker Bit Bytes	1766	PCMU/8000 Valu 114 192 192 192 102 102 102 02 0	160 9281025 168.1.195 168.1.232 4 4	In Sequence	21

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.

Mp Traffic A	Analyser - De	tail ¥iew								
<u>File V</u> iew	Detail View S	jettings <u>H</u> elp								
18 🕼	2 W	∍ ► ■	🖹 🗏 🖬	📽 🛛 🕷 🛛	Sip Calls	•	Show All Ses	sions		
Call Summa	ary Registrator	n Summary 🛛 Alert S	iummary							
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	PCMI1/8000	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 <u>Marker Bit</u>.
- **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 Seque	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	Sync Scroll	0	0.96	
4496	13430	119	PCMA/8	160	In Sequence	1918		0	0.96	
4497	13431	119	PCMA/8	160	In Sequence	21.11	5how Latest	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	BTP Tim	Payload Lei	n Payloa	d 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:ff01:21fd: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:ff01:21fd:fd0d:5606:3df0:2bfb:b05
Source Port	8010	Source Port	8002
Destination Port	8002	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	1.58 \ 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:

Sender Re	eport 💌												
Frame	Sender's	RTP Tim	Packets	Octet	SSRC	Fracti	Frame	Sender's	RTP Tim	Packets	Octet	SSRC	Fracti
825	957412353	1832527	452	72320	957785	24	822	957785601	1446638	451	72160	957412	23
2472	957412353	1832672	1358	217121	957785	23	2456	957785601	1446782	1352	216320	957412	24
3783	957412353	1832787	2080	332641	957785	23							
•						Þ	•						▶
 ▶ ▶ ▶ 	TCP / Gap G	iraph 👌 Jitte	er Graph λ	Gap Distr	ibution Grap	hλ	Jitter Distribu	ution Graph	MOS Graph	ר ∕Quality	Factors)	ر Inband E	vents)

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

Frame Number	SSRC/CSRC	SDES Type	Content
907	907	CNAME	GL Communication
2509	2509	CNAME	GL Communication
•			• •

SDES Item (Source description items)

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.

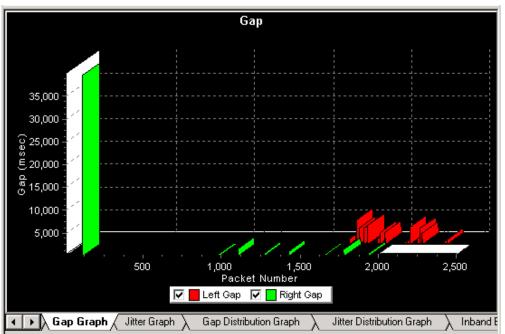


Figure 215: 3D Gap Graph

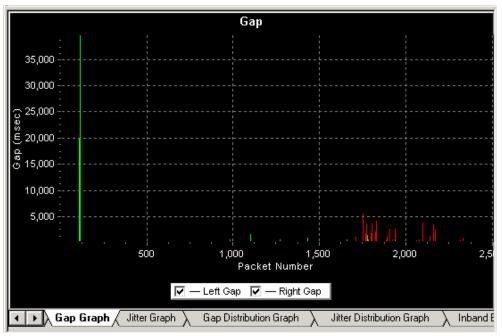


Figure 216: 2D Gap Graph

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 ii the figures below.

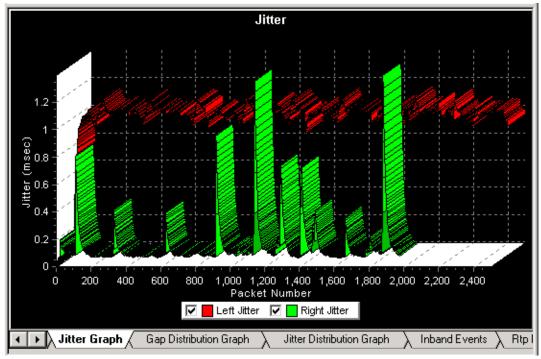


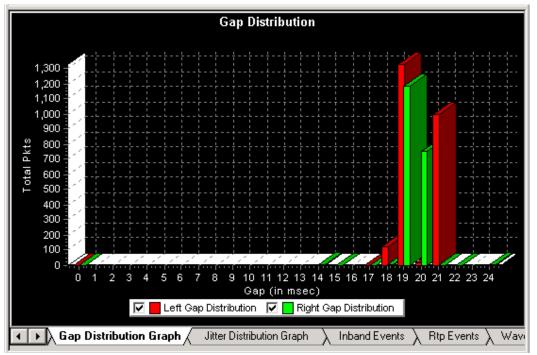
Figure 217: 3D Jitter Graph



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.





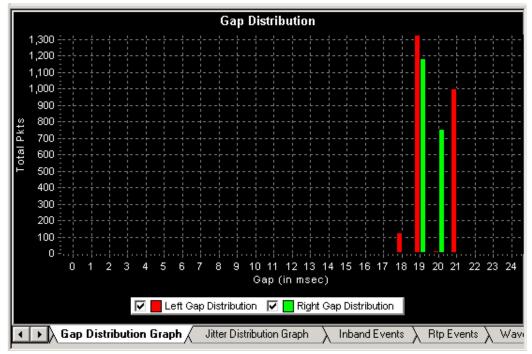
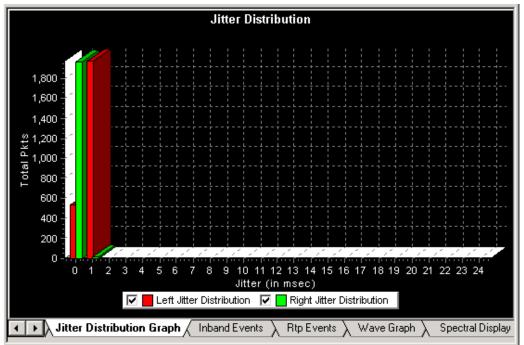


Figure 220: 2D Gap Distribution Graph

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.





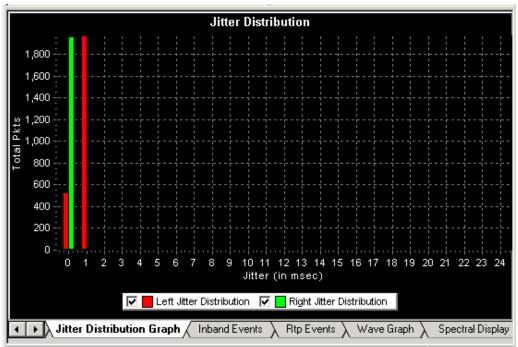
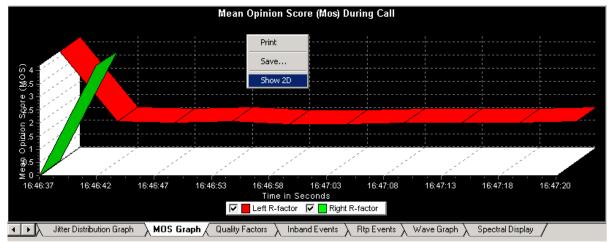


Figure 222: 2D Jitter Distribution Graph

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:





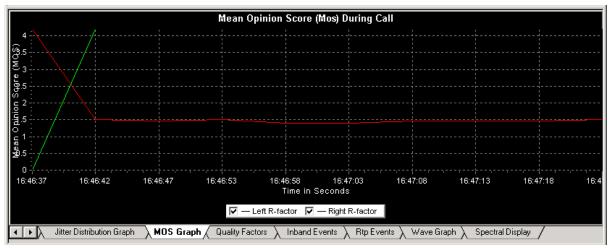


Figure 224: 2D MOS Graph

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	Туре	Event	On	Power	Fre 🔺	TimeStamp	Туре	Event	On	Power	Fre
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	65	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	65	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	65	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	- I
•						•					Ð

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	Туре	Event	On	Power	Fre 🔺	TimeStamp	Туре	Event	On	Power	Fre 🔺
00:00:00.430	DTMF	1	80	-1.89	65	00:00:54.350	MF	1	80	-1.86	70
00:00:00.590	DTMF	2	80	-1.87	65	00:00:54.510	MF	2	80	-1.89	70
00:00:00.750	DTMF	3	80	-1.85	65	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	65	00:00:56.270	MF	4	80	-1.86	70
00:00:02.510	DTMF	1	80	-1.89	65	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	65	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 🕶
•						•	1				
↓ ↓ Gap	Distribution	Graph 🗼	Jitter Distri	bution Graph	Inban	d Events Rtp I	Events 🔪	Wave Grap	h 🔪 Spec	tral Display	/

Figure 226: Digits Only

All Events: If this option is checked then all the events are displayed.

TimeStamp	Туре	Event	On	Power	Fre 🔺	TimeStamp	Туре	Event	On	Power	Fre ▲
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	65	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	65	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	65	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	ME	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	ME	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	-
•						•					
▲ ▶ λ Gap D	istribution (Graph 👌 J	litter Distrit	oution Graph	λ Inban	d Events Rtp B	Events λ	Wave Graph	} Spectr	al Display /	,

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:

Save As	? ×
Save jn: 🔁 G711_alaw 💽 🖛 🛍 🏕 🎟 🗸	
DefaultExport.txt	
File <u>n</u> ame: <u>sav</u>	/e
Save as type: Text Files (*.txt)	cel

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 - <u>INI</u> <u>Decode Options</u>

- 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	DTMF1	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			
\blacksquare MOS Graph λ Quality Factors λ Inband Events λ RTP Events \langle Wave Graph \rangle						

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.

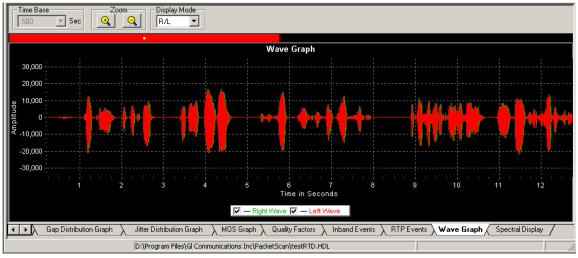


Figure 230: Wave Graph

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.

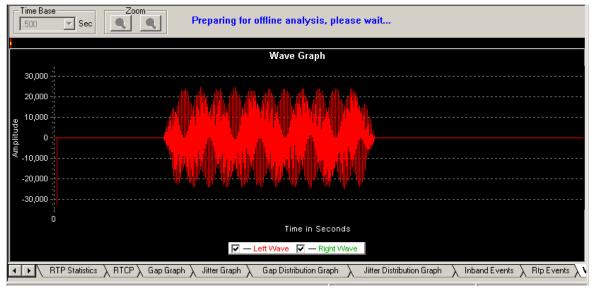


Figure 231: Offline Analysis

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.

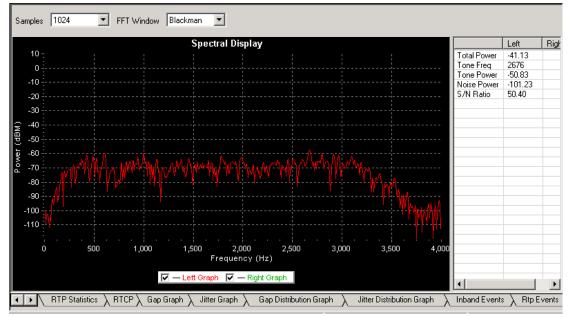
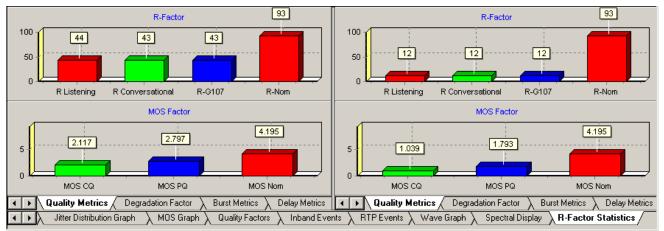


Figure 232: Spectral Display

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

GL Communications Inc.

Packet Data Analysis-- Detail View (RTP Diagnostic View)

Document Number: PKV100-3.11.22-03

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 bandwith.

• 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 <u>ITU-T</u> 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, $\frac{1}{2}$ 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, ¼, ½, 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 Perceptional 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.

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.

Some Definitions

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.

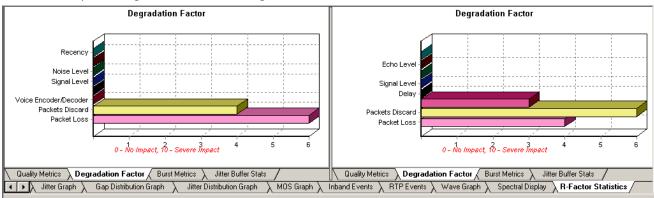


Figure 234: Degradation Factor

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 Lenght	40 msec	Avg Gap Lenght	402 msec
Quality Metrics λ Degradation Factor λ B	urst Metrics / Jitter Buffer Stats /	Quality Metrics Degradation Factor B	urst Metrics / Jitter Buffer Stats /
↓ Jitter Graph ↓ Gap Distribution Grap	wh λ Jitter Distribution Graph λ MOS Graph λ	Inband Events λ RTP Events λ Wave Graph	Spectral Display R-Factor Statistics

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

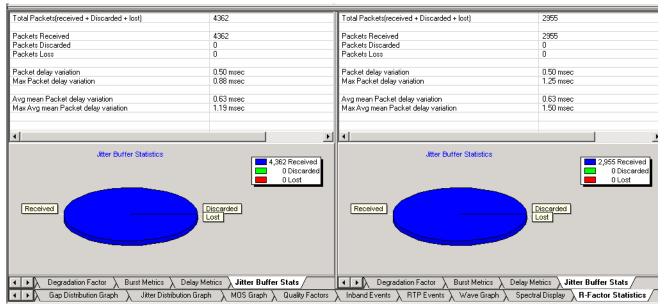


Figure 236: Jitter Buffer Stats

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 (commadelimited) 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

🎶 Export Displayed Summary	×
Tables	
Summary Table	
🔲 Detailed RTP Session (left)	
Detailed RTP Session (right)	
Export File Name	
D:\Program Files\GL Communications In	c\PacketSca
Columns to Export	1_
Call #	Export <u>H</u> eaders
SSRC	
Payload	Select All
Packet Received	
Conversational MOS/R-Factor Listening MOS/R-Factor	
Packets Discarded/(%)	<u>Export</u>
Missing Packets/(%)	
Duplicate Packets/(%)	<u>E</u> xit
Out Of Sequence Packets/(%) Average Gap(ms)	
Average Delay	
Average Jitter 💌	
Detailed View	

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 riangleq 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:

🖗 Inband Events Option D	ialog	X
User Options	Parameters	User Defined Tones
☑ DTMF		
MF		
🔲 User Defined		
Save To File	Load From File Apply for	current session

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:

ац	Inband Events Option Dialog
(User Options Parameters User Defined Tones
	Burst / Idle
	Power Threshold 27 * dB Inter-burst Length 20 * ms
	Hangover Time 20 ms Restore Defaults
	Detection Parameters
	Freq: Accept 1.5 🔹 % Reject 3.5 👗 %
	Max Twist (+-) 8 and dB Max Split Digit 20 and ms
	S/N Ratio Thold 8 dB Restore Defaults
	Save To File Load From File Apply for current session

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:

	Inband Events Option D	ialog			×
ĺ	User Options	Pa	rameters	User Defined Tones)
	User Defined Tone		Low Freq	High Freq	L
	abc		250	800	L
					L
					L
					L
					L
					L
					L
					L
					L
	In	sert A	dd Delete		
L	Save To File	Load From	File Apply for a	current session	

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.

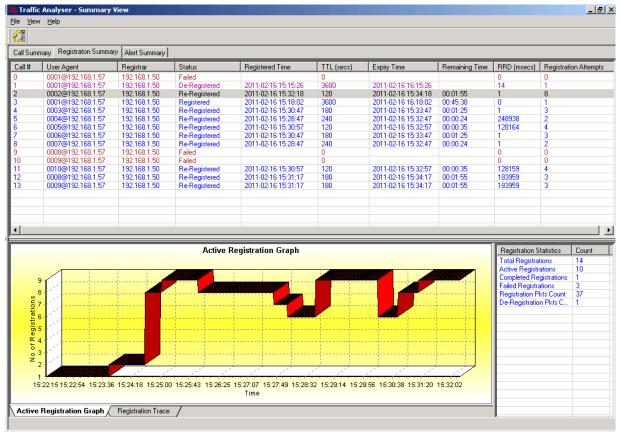


Figure 241: Registration Summary

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 PacketScanTM.

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.

E.									
Call Sum	mary Registraton Summary	Alert Summary							
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
)	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
1	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
)	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
)	0008@192.168.1.57	192.168.1.50	Failed		0			0	0
0	0009@192.168.1.57	192.168.1.50	Failed		0			0	0
1	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
2	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
3	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.

<mark>Ali</mark> p Trafi	ic Analyzer - Summar	y View					_ 🗆 🗵
File Vie	w Help						
				Show All Registrations	•		
Call Sur	mmaru Registraton Sumn	ary Alert Summary		Show All Registrations			
	initially 5		1.	Show Active Registrations			
Call #	User Agent	Registrar	Status	Show Completed Registrations		Expiry Time	Remaining
0	0001@192.168.1.115	192.168.1.190	Registered	Show Failed Registrations	-	2011-01-03 18:33:09	
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 DefinedRegistrations**: 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:

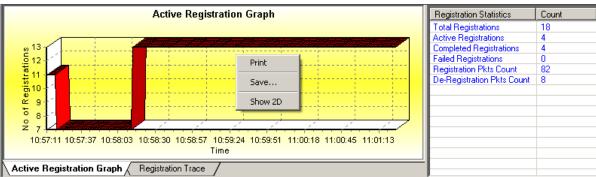


Figure 245: Active Registration Graph

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.

Traffic م <mark>الا</mark>	: Analyser - Summary Vi	iew							_ 8 ×
<u>File View</u>	<u>H</u> elp								
Call Sum	mary Registraton Summary	Alert Summary							
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		192.168.1.50	Re-Registered	2011-02-16 15:25:56	120	2011-02-16 15:27:56		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
•									
<u> </u>									•
				_	Dir.				
	192.168.1.57		192.168.1.50	<u> </u>		ip:192.168.1.50 SI			
			132.100.1.30			.0/UDP 192.168.1.5	7:5060;branch=	z9hG4bK7295	08016-3623
540		REGISTER	506		Max-Forward				
040	30		5000	,		ITE, BYE, CANCEL, ACK <sip:0002@192.168< td=""><td></td><td></td><td></td></sip:0002@192.168<>			
50	SIF	P/2.0 200 OK	500			<s1p:00020192.168. D20192.168.1.57</s1p:00020192.168. 	.1.5/>;tag=666	/G_/29508016	-3624
506	50 -		506	,		LPG7295080163622			
		REGISTER	N		CSeq: 1 RE				
540	98		5061)	Expires: 12				
		P/2.0 200 OK				20 DO2 <sip:00020192.1< td=""><td>160 1 575</td><td></td><td></td></sip:00020192.1<>	160 1 575		
506	50 ┥ 👘	72.0 200 010	5060)	Content-Ler		100.1.57/		
		REGISTER			Concenc her	igen. o			
540	98	neuisten	506)					
506	so 🖌 Sir	P/2.0 200 OK	506	1					
	1.		000						
540	99	REGISTER	506						
	30		5000						
•				•	1				
Activ	e Registration Graph 🔒 🔒	egistration Trac	e /					-	

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 [international, 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 RTCP 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 filed 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:

	w <u>C</u> all Summ	ary <u>S</u> ettii	ngs <u>H</u> elp														
Q 🐔	🖁 🎦 🕊	9	▶ ■	🎽 🖄	🛃 🏋	📲 Si	p Calls		-	Show A	ll Sessio	ns		•			
Call Sur	nmary Registr	raton Sumr	hary Alert S	ummary													
Call #	SSRC	Payload	Packet Received	Conversat MOS/R	t Listening MOS/R	Packets Discard	Missing Packets	Duplicate Packets	Out Of Sequen.	Average Gap(ms)	Average Delay	Average Jitter	Average Inter Arri	Cumulativ Packet	Max/Min Gap	Max/Min Delay	
Coll	000001 Cal	er.0005@	192.168.1	0.16 Calee	0001@19	32.168.10.	203 Call	1GLPG-10	5884386	41929 Cal	StartTime	18.33.02	653 Call D		00.00.00	0	Initiated Calls
	0 Unkno 0 Unkno			0	0	0		0	0	0	0	0		07 07 07 07		00 /	
E uuu Be Jime	0 Unkno 100001 Calleri		021001041	College U.A. D	1/01/02 100	1.69.05884	CL DC102	000000773	U Call Charl	U Time: 2009.0	0210-02	21 0001721	Call Duration				
ອູເລແ#ບ ໄ. 1	n Caller.	Unkno	0	n	0	0	0.00/0	0.00/0	0	0.00	0.00	0.00	O	0.00.00.00.	0.00/0	0/0	
6 1 1	ñ	Unkno	-	ñ	ñ	ñ	0.00/0	0.00/0	ñ	0.00	0.00	0.00	Ő	ñ	0.00/0	0/0	
Call#C	00002 Caller!	UA 02@15		Callee:UA_0	2@192.168	1.58 Calld	GLPG193	4068882723	7 Call Start	Time:2009-0	6-02 10:03	31.0006121	Call Duration	~	000000	0/0	In Progress Cal
	0	Unkno	0	0	0	0	0.00/0	0.00/0	0	0.00	0.00	0.00	0	0	0.00/0	0/0	
2	0	Unkno	0	0	0	0	0.00/0	0.00/0	0	0.00	0.00	0.00	0	0	0.00/0	0/0	
Call#C	00001 Caller:	UA_01@19	92.168.1.64	Callee:UA_0	1@192.168	1.58 Callid	GLPG192	9688882724	4 Call Start	Time:2009-0	6-02 10:03:	31.000173 (Call Duration	n: 00:00:04.	000891		Established
b 1	42949	PCMU	0	0.0070	0.0070	070.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0	or
e 1	42949	PCMU	0	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0	
	00002 Caller:												Call Duration	n: 00:00:04.			Active Calls
2 2	42949	PCMU	-	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00		0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0	
2	42949	PCMU	0	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0	
Call#0	000001 Caller:		92.168.1.64	Callee:UA_0		1.58 Calld			Call Start	Fime:2009-06			Call Duration				Failed Calls
0 1 0 1	0	Unkno		0	0	0	0.00/0	0.00/0	0	0.00	0.00	0.00	0	0	0.00/0	0/0	
21	0	Unkno	0	0	0	0	0.00/0	0.00/0	0	0.00	0.00	0.00	0	0	0.00/0	0/0	

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#0	00001 Caller:	UA_01@19	92,168,1	1.64 Callee:UA_01	0192.168	1.58 Callid:	GLPG1929	688882724	Call StartT	ime:2009	-06-02 10:03	:31.000173	3 Call Dura	ation: 00:00:1	4.000577	
S 1	28555	PCMU	2	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0
e 1	28546	PCMU	2	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0
	00002 Caller:	UA_02@19	92,168,1	1.64 Callee:UA_02	2@192.168	1.58 Callid:	GLPG1934	068882727	Call StartT	ime:2009	-06-02 10:03	:31.000612	2 Call Dura	ation: 00:00:2	22.000128	
2 2	28626	PCMU	3	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0
e 2	28611	PCMU	3	0.00 / 0	0.00 / 0	0 / 0.00	0 / 0.00	0 / 0.00	0 / 0.00	0.00	0.00	0.00	0	0	0.00 /	0/0
20.00			-										-	-		

Active Purged Calls: When the purging starts the color of the active calls is changed to indicating that the calls are getting purged.

-	er:0006@192.168.10	.16 Callee:0	006@19;	2.168.10.12	CallId:GLP	G-5197778	641958 Cal	StartTime:	18:42:01.72	24 Call Durat	ion: 00:03:22.9	955	
Solution 13782		10097		0	0	20	0	1	0	0	309.31	289 /	22.70
🧬 0000 13733	G726-40/8000	13	0	0	0	0	0	0	6	0	0.00 /	0/0	0.00 /

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	-
•	1		1				•		•	1						►	Г

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:

🦆 Traffi	c Analyser - Summary Vie	w					- O X	
No Viev	v Help							
1					Sho	w All Sessions		
Call Sum	mary Registraton Summary	Alert Summary						
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		De-Registered Stat
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	-	
				2009-05-19 12:47:22				
				2009-05-19 12:47:22				Expired State
				2009-05-19 12:47:22				- Lypireu State
				2009-05-19 12:47:22			J	
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	Registered State
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	2 Hogiotorea etato
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**.

HDL File Conversion Utility										
Source Information										
File Name gs\Srikanthr\Desktop\sip-ipv6.pcap										
File Format Ethreal/LibpCap File										
Destination Information										
File Format										
File Name d Settings\Srikanthr\Desktop\sip.hdl										
Protocol SIP Tilter										
Linux Format 🔲 Discard Duplicate Packets										
Reverse Bits Link Type Ethernet 💌 147										
Frames To Convert 0										
Skip Begin 0 Bytes ⊆onvert										
End O Bytes										

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.

Protocol Capture Configuration		<u>_ ×</u>
<u>S</u> ave Load <u>D</u> efault		
Capture File Options Card & Stream Selection Capture Filter Capture Filter	Capture Filters Filter Selection MAC MAC MAC MAC MAC STP MGCP MGCACO MGCACO MAC MAC <td></td>	

- 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 <u>Call Detail Record</u> 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 <u>Call Data Records</u> and <u>Voice Band Application</u> 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.

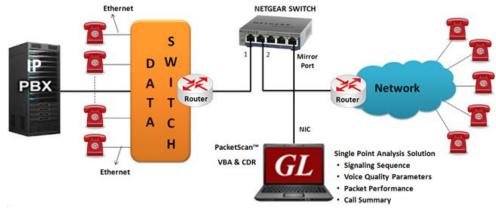


Figure 251: Packet over IP CDR Analysis System

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.

Probe ID Call ID VolPProbe GLPG-11734 VolPProbe GLPG-92265	Side 1 837841613 Left	Side 2	Protoco	01	1		
	837841613 Left		FIUCULA	Start		Released	Du
VolPProba GLPG-92265		Right	SIP	07-12-2012 15	08:32	07-12-2012 15:08:53	00
VOIL LODE OF 0-22203	57841625 Left	Right	SIP	07-12-2012 15	12:43	07-12-2012 15:13:04	00
VolPProbe GLPG-96531:	17841619 Left	Right	SIP	07-12-2012 15	12:00	07-12-2012 15:12:20	00
Filltered Calls: 3 of 5 Total (Calls; Filltering(, Criteria: Start O	7-12-2012	15:08:32 to	07-12-2012	15:12:43	
all Summary Call Side Informatio	on Call Events Voiceband	Measurements					
2							
	PProbe				C Play the		
	G-9226557841625				(requires the v	voice file path to have write permissi	onsj
Protocol: SIP					_		
	12-2012 15:12:43				C Downloa	d and Play the Voice Files	
	12-2012 15:13:04				C:\Test		
	00:21				<u> </u>	· 💙	
Call Originating Side: Left					(Enter the fi	older name only)	
Call Terminating Side: Left	-						
	rmal Call Clearing				Print Se	lected Record	
Post Dial Delay(PDD): 2							
Session Delay(SD): 2 Archive Folder: C:\I	netpub\ftproot\TestFiles [\]						

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 <u>Export Terminated Calls</u> feature in PacketScan^M. 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

				PacketScan	Report.xism	Microsoft Excel		- = ×			
8	Home	Insert	Page Layout	Formulas [Data Rev	iew View Develop	er Add-Ins	🔞 🗕 🗖 🗙			
Paste		ori ▼ <u> <i>I</i><u>U</u>▼ ▼ <u> </u> → <u> →</u> <u> →</u> <u> →</u> <u> →</u> <u> →</u> <u> →</u> <u> →</u></u>	Á ∧́ ≡		Seneral \$ - % , 00 -00 Number (Styles	∑ - Sort & Find & 2 - Filter - Select Editing	k V			
9	- (° - 😈	÷									
	A1	+ (1	fx					¥			
	A	В	C	D	E	F	G	H			
1	<u>^</u>		C	0		For Answered Calls	0				
2 3 4	Create Ne	ew Conne	ection	Calls Per	Day	Session Disconnect Delay					
5 6 7	Append	l New Tab	les	Call Duration	Per Day	Post Dial Delay					
8	Delete	e All Grapi	ns	Call Faile	ure	Conversational MOS					
10 11 12				Calls Answer	ed/Not	Listening MOS					
13						Average Packet Loss	Open				<u>? ×</u>
14								Design Design		-	
15						Average Delav	Look in:	Project-PacketScan	1] 🕲 • 🖄 X 🗳 💷 •
15 16						Average Delay	Look in:	Name		Size Type	🕲 • 🖄 X 📸 🎫 •
15 16 17							Look in: My Recent Documents	Name SuccessFullCalls.txt FailedCallsNew.txt			Image: Constraint of the second sec
15 16 17 18						Average Delay Average Jitter	Look in: My Recent Documents	Name SuccessFullCalls.txt FailedCallsNew.txt FailedCalls.txt		Size Type File Folder File Folder 24 KB Text Document	Image: Constraint of the second sec
15 16 17 18 19							Look in: My Recent Documents Desktop My Documents	Name SuccessFullCalls.txt FailedCallsNew.txt FailedCalls.txt SuccessfullCalls_210	: 00.txt	Size Type File Folder File Folder 24 KB Text Document 24 KB Text Document	Image: Constraint of the second sec
15 16 17 18 19 20							Look in: My Recent Documents Desktop My Documents	Name SuccessFullCalls.txt FailedCallsNew.txt FailedCalls.txt	: 00.txt	Size Type File Folder File Folder 24 KB Text Document	Image: Constraint of the second sec
15 16 17 18 19							Look in: My Recent Documents Documents My Documents My Computer	Name SuccessFullCalls.txt FailedCallsNew.txt FailedCalls.txt SuccessfullCalls_210	: 00.txt	Size Type File Folder File Folder 24 KB Text Document 24 KB Text Document 8 KB Text Document	Image: Constraint of the second sec
15 16 17 18 19 20 21 22	H Pivot						Look in: My Recent Documents Desktop My Documents	Name SuccessFullCalls.txt FailedCallsNew.txt FailedCalls.txt SuccessfullCalls_210	: 00.txt	Size Type File Folder 24 KB Text Document 24 KB Text Document 8 KB Text Document 936 KB Text Document	Image: Control of the second
15 16 17 18 19 20 21 22	Pivot	*				Average Jitter	Look in: My Recent Documents Desktop My Documents My Computer My Network	Name SuccessFullCalls.txt FailedCallsNew.txt FailedCalls.txt SuccessfullCalls_210	: 00.txt	Size Type File Folder 24 KB Text Document 24 KB Text Document 8 KB Text Document 936 KB Text Document	Image: Control of the second
15 16 17 18 19 20 21 22 R ↔		87				Average Jitter	Look in: My Recent Documents Desktop My Documents My Computer My Network	Name SuccessFullCalls.txt FailedCallsNew.txt FailedCalls.txt SuccessfullCalls_210	: 00.txt	Size Type File Folder 24 KB Text Document 24 KB Text Document 8 KB Text Document 936 KB Text Document	Image: Control of the second
15 16 17 18 19 20 21 22 R ↔		2				Average Jitter	Look in: My Recent Documents Desktop My Documents My Computer My Network	Name SuccessFuliCalls.bt FaledCalsNew.bt FaledCals.bt SuccessFuliCals_21 SuccessFuliCals_60 File game:	00.bd 00.bd	Size Type File Folder 24 KB Text Document 24 KB Text Document 8 KB Text Document 936 KB Text Document	Image: Control of the second
15 16 17 18 19 20 21 22 K ↔		2				Average Jitter	Look in: My Recent Documents Desktop My Documents My Computer My Network	Name SuccessFullCalls.bt FailedCallsNew.bt SaledCallsNew.bt SaledCalls.bt SuccessFullCalls_211 SuccessFullCalls_60	00.bd 00.bd	Size Type File Folder 24 KB Text Document 24 KB Text Document 8 KB Text Document 936 KB Text Document	Image: Control of the second

Figure 253: Import PacketScan[™] Text (*.txt) Sample Files

option.

- 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
- The CPD call details graph is generated and is displayed in CPD tab as seen in the figure below.

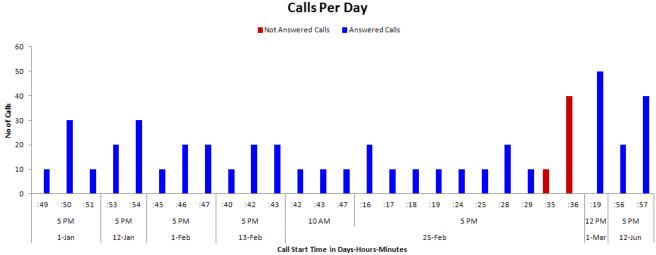


Figure 254: No. of Calls Per Day (CPD) graph

• 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 Tim			No of Calls 📃 💌		
Days_	Hours_	Minutes_	Not Answered Calls	Answered Calls	Grand Tota
🗏 1-Jan	■5 PM	:49	0	10	1
		:50	0	30	3
		:51	0	10	1
■ 12-Jan	■5 PM	:53	0	20	2
		:54	0	30	3
∃1-Feb	■5 PM	:45	0	10	1
		:46	0	20	2
		:47	0	20	2
■13-Feb	■5 PM	:40	0	10	1
		:42	0	20	2
		:43	0	20	2
■25-Feb	🗆 10 AM	:42	0	10	1
		:43	0	10	1
		:47	0	10	1
	■5 PM	:16	0	20	2
		:17	0	10	1
		:18	0	10	1
		:19	0	10	1
		:24	0	10	1
		:25	0	10	1
		:28	0	20	2
		:29	0	10	1
		:35	10	0	1
		:36	40	0	4
■1-Mar	■ 12 PM	:19	0	50	5
■12-Jun	■5 PM	:56	0	20	2
		:57	0	40	4
Grand Total			50	440	49

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**.