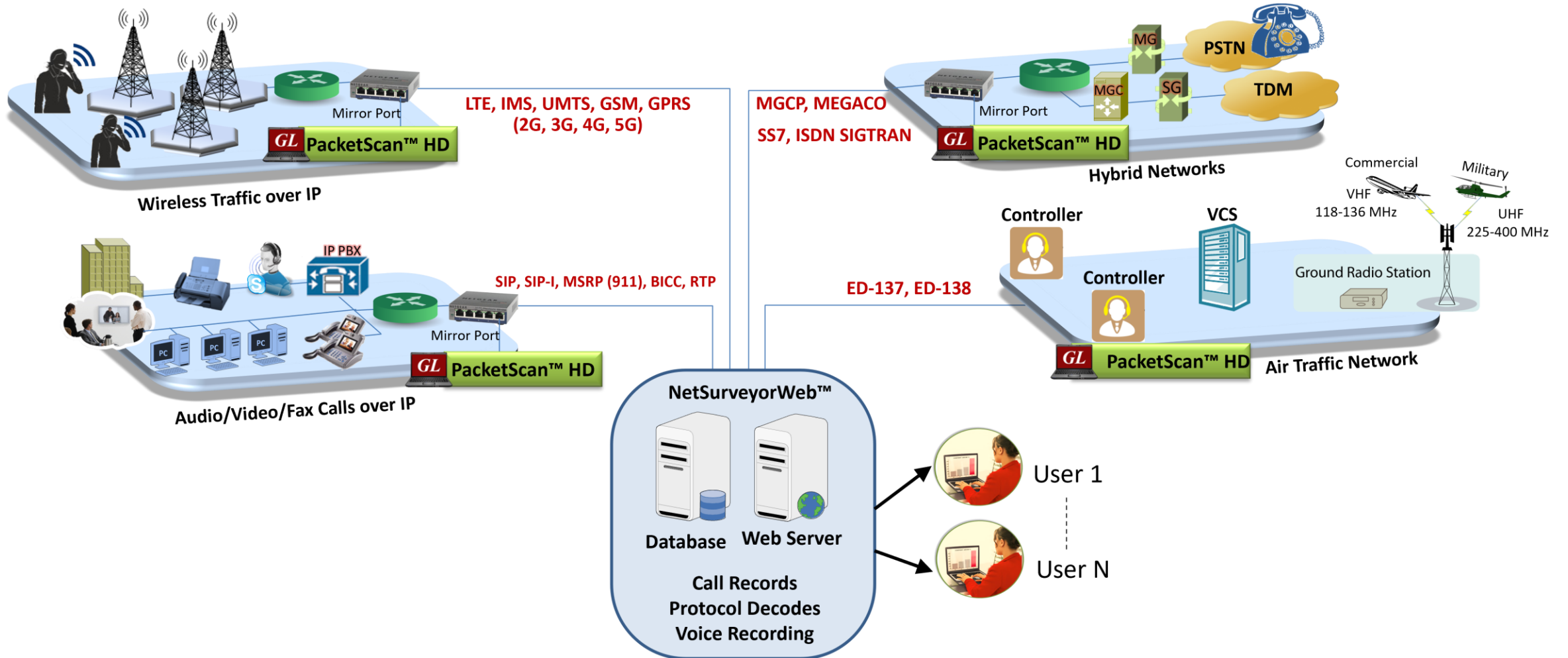

PacketScan™ High Density All-IP Analyzer (1, 10, 25, 40, or 100 GigE Networks)



818 West Diamond Avenue - Third Floor, Gaithersburg, MD 20878
Phone: (301) 670-4784 Fax: (301) 670-9187 Email: info@gl.com
Website: <https://www.gl.com>

PacketScan™ HD All-IP Signaling and Traffic Analysis (2G/3G/4G/5G/VoIP/RTP, RTCP/Fax Analysis)



PacketScan™ HD Features

- **Signaling** – Protocol analysis: SIP, MGCP, MEGACO, H.323, SCTP, SCCP (Skinny), SS7 SIGTRAN, ISDN-SIGTRAN, GSM A over IP, GPRS over IP, UMTS over IP, LTE, Diameter
- **Voice/Fax** - Captures, segregates, and monitors packets; perform voice quality testing in real-time over VoIP network. G.711, G726, GSM, GSM EFR, GSM HR, G729/B, G.722, G.722.1, ILBC, SPEEX, SMV, T.38
- **Video Calls** - Video quality statistics such as MDI (Media Delivery Index), Packet Lost, Duplicate, out of sequence and Frame Rates are provided for each video session
- **5G Analyzer** - Captures, decodes, and collects statistics over N1N2, N4, N8, N12 and N13 interfaces of the 5G network
- **NetSurveyorWeb** - Can be deployed as a Probe for a centralized monitoring system connected to an Oracle database

Why this product?

- Lossless wirespeed capture of IP traffic across high speed (1, 10, 25, 40, and 100 GigE) links
- Non-intrusive capture and record over Ethernet (Electrical and Optical) interfaces at nano-second time precision
- Filter on inner layer of GTP tunnel traffic like inner IPv4/IPv6 addresses
- Ability to capture and analyse high volume calls with traffic. Process up to 20000 simultaneous calls with bidirectional RTP traffic. Up to 50,000 calls can be achieved by scaling with higher configurations
- PacketScan™ HD available in both Portable as well as 2U rack mounted Network Monitoring Appliance w/ 4x 1GigE (PKV120) or 2x 10GigE (PKV122) network interface cards
- Create up to 10 user defined hardware filters to filter-out traffic based on MAC, 802.1Q (VLANs), IPv4, TCP, UDP, SIP, and RTP parameters
- Supports almost all industry standard IP and Wireless Protocols (from SIP to LTE)
- Supports all RTP traffic – Voice, Video, Fax T.38, Digits, Tones, Impairments
- Capture and Call processing is enhanced to handle different Tunnel traffic (VXLAN, GRE and GTP) and multiple tunnelling
- Support for eCPRI decode

Key Features

- User can create their own filters using custom filter option which provides flexibility to check the fields and use the logical conditions more efficiently
- Supports decoding of eCPRI protocol
- Long-Term activity reporting
- Captures, Segregates, Monitors, Build CDRs, and Collects Statistics on all IP calls
- In-depth real-time and post-process data investigation using Packet Data Analysis (PDA) feature
- Complex Filtering and Search capabilities to record all or filtered traffic into a trace file
- Supports TCP Analytics application analyzes TCP connections between both internal Local Area Network (LAN) and external Wide Area Network (WAN) computers including servers and clients. The application helps troubleshoot large bandwidth consumption, failed TCP sessions, packet loss, poor TCP throughput and more
- Provides Call Quality Scores like MOS, R-Factor, Delay, Jitter, Packet Loss and more
- Supports Centralized Remoter Network Monitoring with NetSurveyorWeb™ - a web-based client that can connect to PacketScan™ probes through a web server that facilitates display of call data records using a web interface

Supported Protocols and Codecs

Supported Codecs	Supported Protocols
<ul style="list-style-type: none">• G.711 A/μ-law• G.722, G.722.2 (AMR-WB), G.722.1, G.726, G.729A/B• GSM (EFR, FR and HR)• AMR (Narrowband and Wideband)• EVRC, EVRCB, EVRC-C, iLBC, Speex, SpeexWB, RFC 2833, and user-defined codecs for voice and tones.• EVS OPUS <p>Visit Voice Codec webpage for more details</p>	<ul style="list-style-type: none">• SIP, SIP-I, SIP-T, H.323, MEGACO, MGCP, Diameter, Skinny (SCCP)• LTE• 5G N1N2, N4, N12, N13• SIGTRAN – SS7, ISDN• GSM A and Abis over IP• GPRS Gb and Gn over IP• UMTS IuCS and IuPS over IP• T.38 Fax and Video calls <p>Visit Supported Protocols for more details</p>

For more information on other features, refer to PacketScan™ Basic (PKV100) presentation.

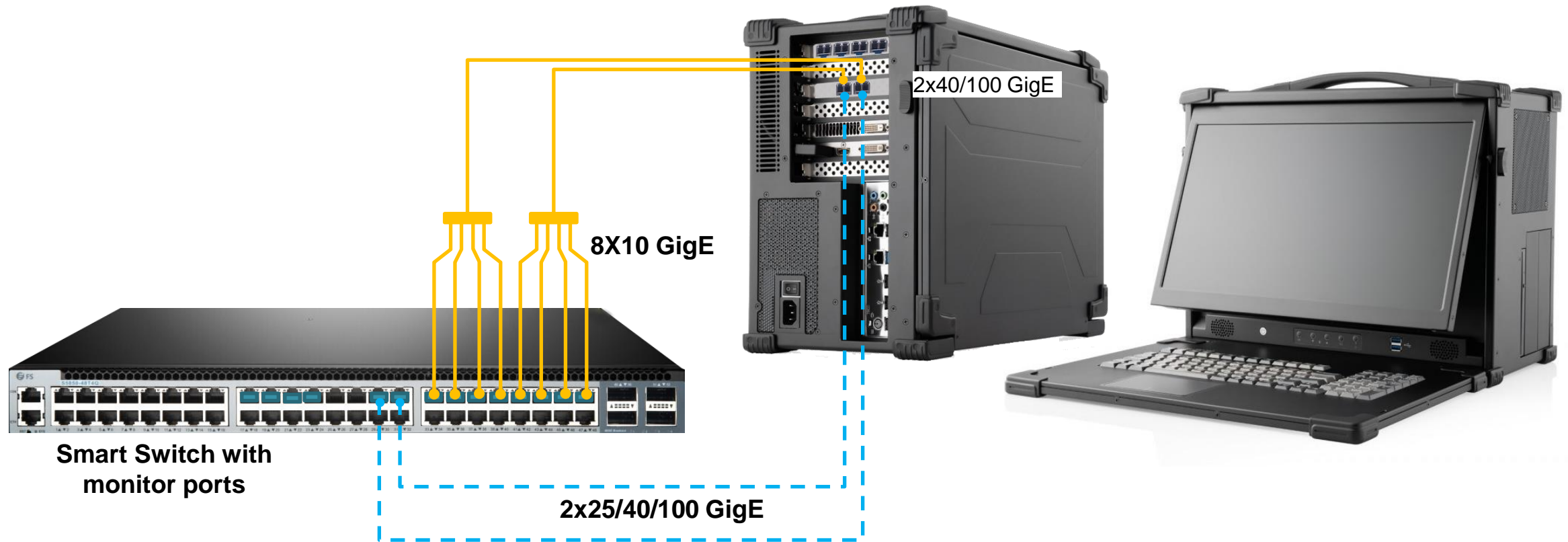
PacketScan™ HD

(4x1 GigE, 2x1/10 GigE, 2x25 GigE, 8x10 GigE, and 2x40/100 GigE)



****Also available as a rack mounted unit**

PacketScan™ HD with 2 x 25/40/100 GigE or 8 x 10 GigE



The above setup could manage rates as below:

- 2 x 25/40/100 GigE card can also be used as 8 x 10 GigE (with Breakout)
- System can also be outfitted with multiple cards with easy switching

PacketScan™ HD 2U Rack Appliance

Front Panel



PacketScan™ HD Hardware + Software
4 or 8 x1G / 2x1/10G / 2x25G / 2x40G / 2x100G

Back Panel

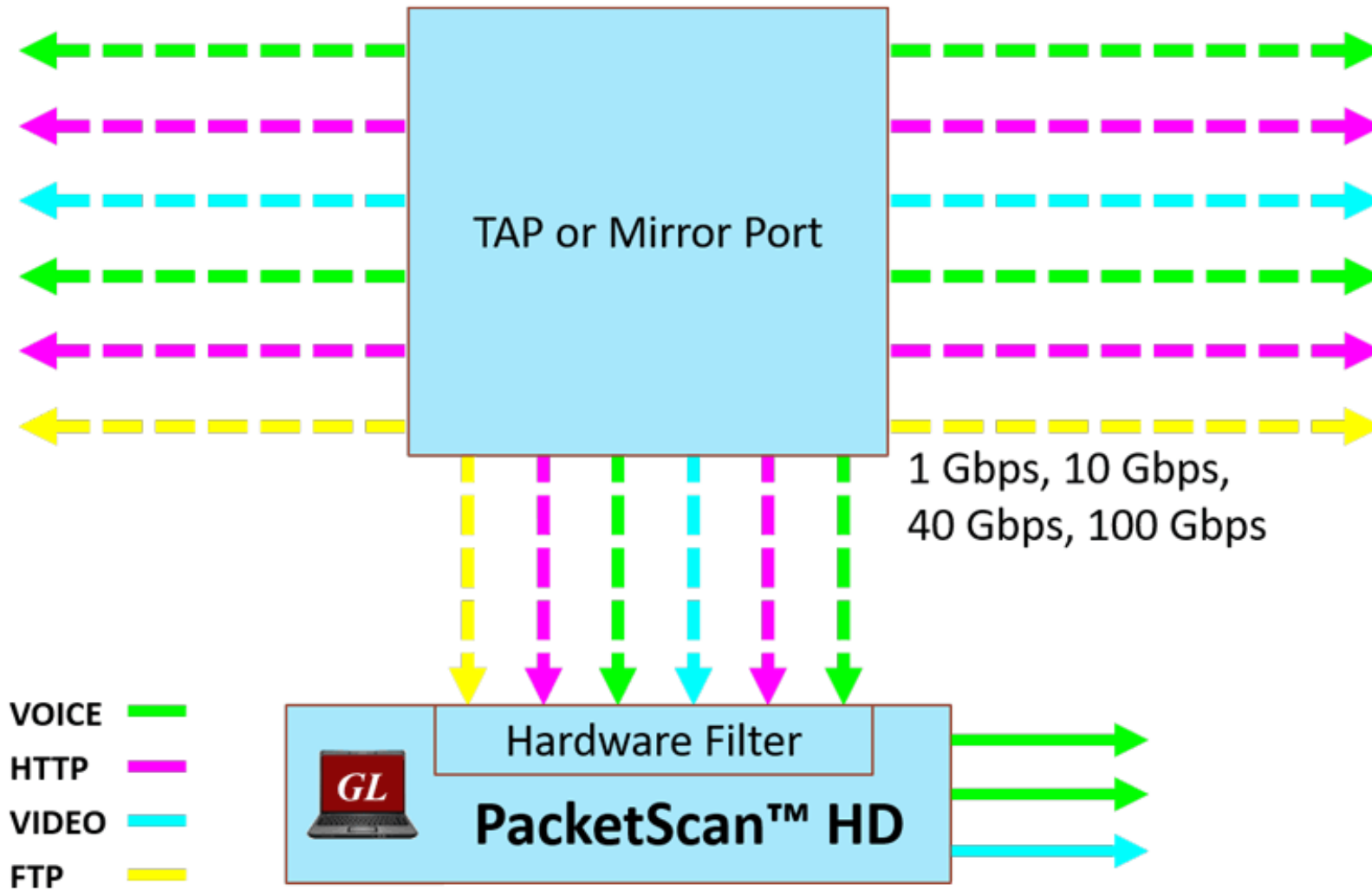


PacketScan™ HD Systems

- PacketScan™ HD appliance is also available in three systems “**Low End**”, “**Medium End**” and “**High End**”

	Low End	Medium End	High End
Data Rate	4x1GigE	4x1/10GigE Or 2x1/10GigE	8x10GigE, 2x10/25GigE, 2x40GigE, 2x100GigE
RAM	16 GB RAM	32 GB RAM	128 GB RAM
NVME Storage [SSD]	2 TB	4x SSDs user configurable disk size (4x 1.92 TB in the base configuration)	8x SSDs user configurable disk size (8x 3.84 TB in the base configuration)

High Density Traffic

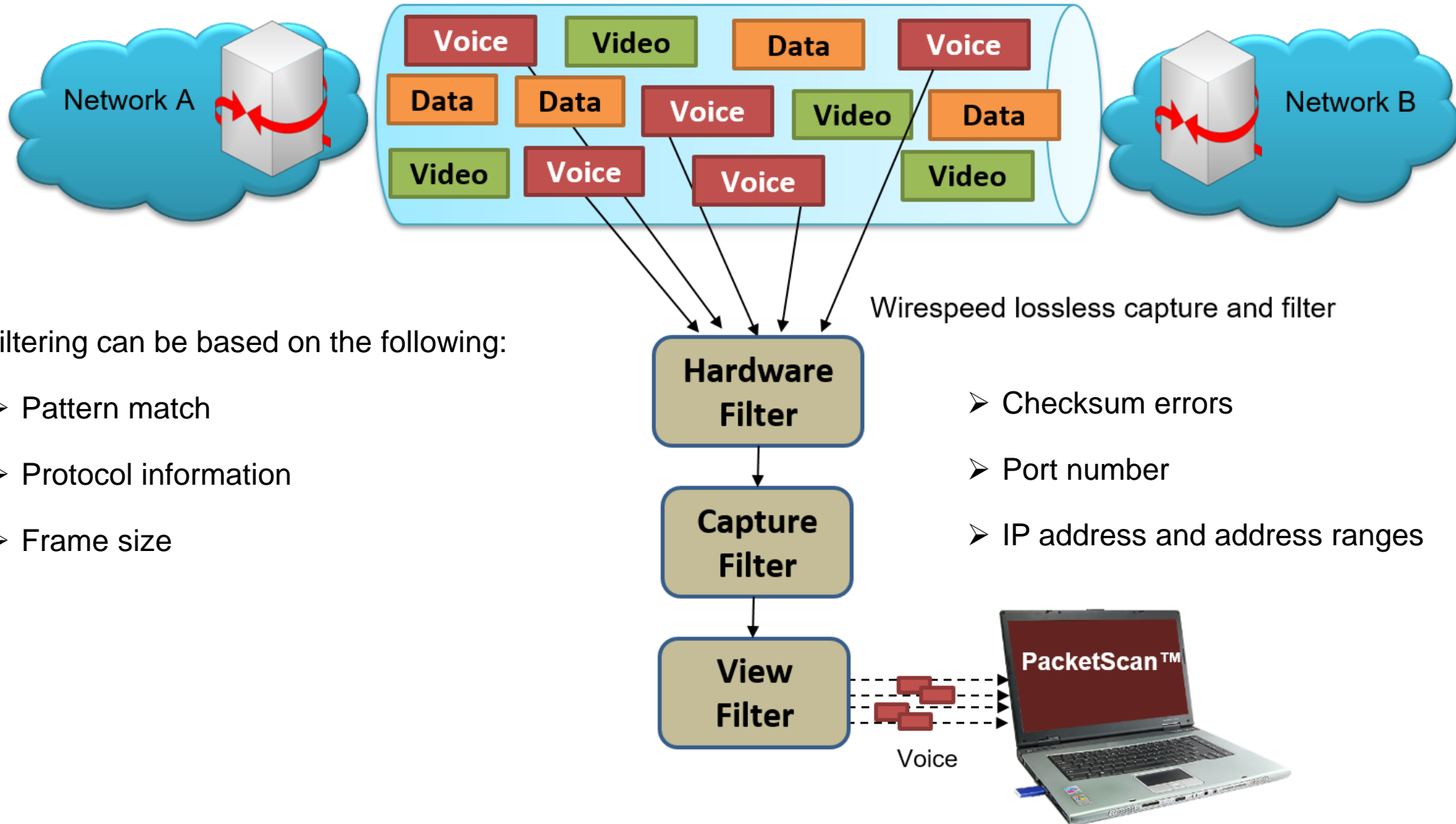


RTP Traffic Capabilities and Performance

Product Version	Max Simultaneous Calls
	Signaling + RTP Voice Traffic
PacketScan 1G (4x 1GigE) SIP 64-bit	20000 calls with bi-directional RTP traffic Extracting/recording voice <ul style="list-style-type: none">• 2500 simultaneous calls (maximum)• Option to record filtered calls of interest only
PacketScan 10G (2x 10GigE) SIP 64-bit	30000 calls with bi-directional RTP traffic Extracting/recording voice <ul style="list-style-type: none">• 2500 simultaneous calls (maximum)• Option to record filtered calls of interest only

** The above performance is evaluated on a high-end Core i7 system with typical 12GB RAM

Wirespeed Filtering



• Filtering can be based on the following:

- Pattern match
- Protocol information
- Frame size

- Checksum errors
- Port number
- IP address and address ranges

3 Stages of Filtering

- Hardware Filter (HWF) – “Special NIC” with hardware filtering - very fast
- Capture Filter (CF) – Powerful software filtering but a little slower
- View Filter (VF) – applies on the captured frames to filter only frames of interest
- PacketScan™ HD captured files to/from Wireshark®
- PacketScan™ HD PDA – for detailed voice, fax, and video analysis

3 Stages of Filtering (Contd.)



PacketScan™ HD Hardware



Standalone NIC

Hardware Filter

Filter Passed

Filter Not Passed



Packets Discarded

Capture Filter

Filter Passed

Filter Not Passed



Packets Discarded

Capture Buffer

Capture Saved to Files

Ex: SIP, RTP (100 Frames)

View Filter

Filter Passed

Filter only SIP (10 out of 100 Frames)

All SIP, RTP (100 Frames)

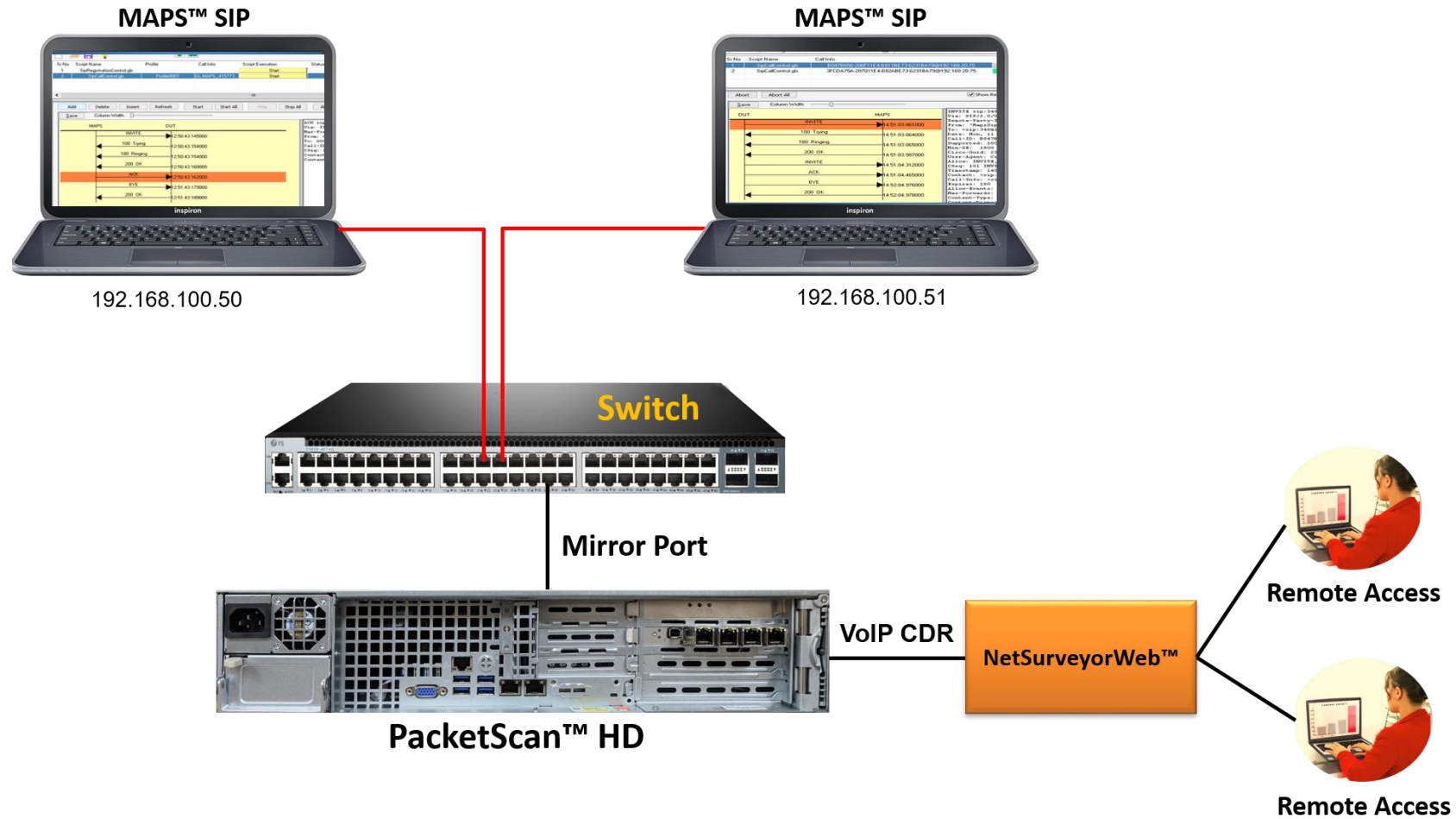
PacketScan Summary View

Device	Frame#	Time (Relative)	Length (Bytes)	Error	Length/Protocol Type	Packet Type	Destination IP Address	Source IP Address	Source Port	Destination Port	
✓	2	0	00:00:00:000000		836	Internet (IPV4)	SIP	192.168.1.103	192.168.1.200	54098	5060
✓	2	1	00:00:00:001952		354	Internet (IPV4)	SP	192.168.1.200	192.168.1.103	54098	5060
✓	2	2	00:00:00:001969		355	Internet (IPV4)	SP	192.168.1.200	192.168.1.103	54098	5060
✓	2	3	00:00:04:487598		820	Internet (IPV4)	SP	192.168.1.200	192.168.1.103	54098	5060
✓	2	4	00:00:04:488935		365	Internet (IPV4)	SP	192.168.1.103	192.168.1.200	5060	5095
✓	2	5	00:00:04:548072		214	Internet (IPV4)	RTP	192.168.1.103	192.168.1.200	1024	1024
✓	2	6	00:00:04:569795		214	Internet (IPV4)	RTP	192.168.1.103	192.168.1.200	1024	1024
✓	2	7	00:00:04:567664		214	Internet (IPV4)	RTP	192.168.1.103	192.168.1.200	1024	1024
✓	2	8	00:00:04:607187		214	Internet (IPV4)	RTP	192.168.1.103	192.168.1.200	1024	1024
✓	2	9	00:00:04:616308		214	Internet (IPV4)	RTP	192.168.1.200	192.168.1.103	1024	1024
✓	2	10	00:00:04:628685		214	Internet (IPV4)	RTP	192.168.1.103	192.168.1.200	1024	1024

PacketScan PDA View

Call ID	SSRC	Payload	Packet	Conversational	Listening	Packets	Missing	Duplicate	Out Of	Average	Average	Average	Average	Cumulative	Max/Min	Max/Min	Max/Min
1	95741	PCMU	1889	344 / .	344 / .	4 / 0 / 19	194 / .	0 / 0 / 0	0 / 0 / 0	22.05	0.00	4.00	3	137	64.45	4 / 9	332 / .
2	95687	PCMU	1647	282 / .	282 / .	3 / 0 / 14	446 / .	0 / 0 / 0	0 / 0 / 0	25.44	0.00	4.00	3	446	118.28	43 / 26	574 / .

Demo



- Generate VoIP calls (SIP signaling and RTP traffic) with MAPS™ SIP
- Connect PacketScan™ HD to a mirror port
- Capture and analyze the VoIP calls

Link and Ports Interface Testing

C:\Program Files\Napatech3\bin\monitoring.exe

Font

```
monitoring (v. 3.8.5.7-8a9442)
```

P	A	Type	Link	Down	Rx	Tx	Max	Temp.
0	0	SFP+	10G Full	2	499.99M	0.00M	9018	55.50 C
1	0	SFP+	10G Full	15	2.25M	0.00M	9018	53.80 C
2	1	SFP-CU	1G Full	0	0.00M	0.00M	9018	N/A
3	1	SFP-CU	1G Full	0	0.00M	0.00M	9018	N/A
4	1	SFP Empty	Down	0	0.00M	0.00M	9018	N/A
5	1	SFP Empty	Down	0	0.00M	0.00M	9018	N/A

Port 0 - Adapter 0 Intf 0: NT20E2 network adapter

<u>RX RMON1 counters</u>				<u>Totals</u>			
Packets	:	#000000000701452306	Octets	:	#000000526089229846		
Broadcast	:	#000000000000000000	Multicast	:	#000000000701451020		
64 octets	:	#000000000000000000	65-127 octets	:	#000000000000000000		
128-255 octets	:	#000000000000000000	256-511 octets	:	#000000000000000000		
512-1023 octets	:	#000000000701452306	1024-1518 octets	:	#000000000000000000		
Undersize	:	#000000000000000000	Oversize	:	#000000000000000000		
Fragments	:	#000000000000000000	Collisions	:	#000000000000000000		
Drop events	:	#000000000000000000	Crc/Align errors	:	#000000000000001286		
Jabbers	:	#000000000000000000	Ext drops	:	#000000000011943856		

Reset Tx/Rx 0RMON 1ExtrMON 2Checksum 3Decode 4Drop 5IPF Dec/Hex Tot/Spd
Quit Sensors Color stat XTimeSync 1EEE 1588 PTP 3Stream EDump

Ethernet Frame Structure

RTP

Protocol - UDP

RTP ports – even

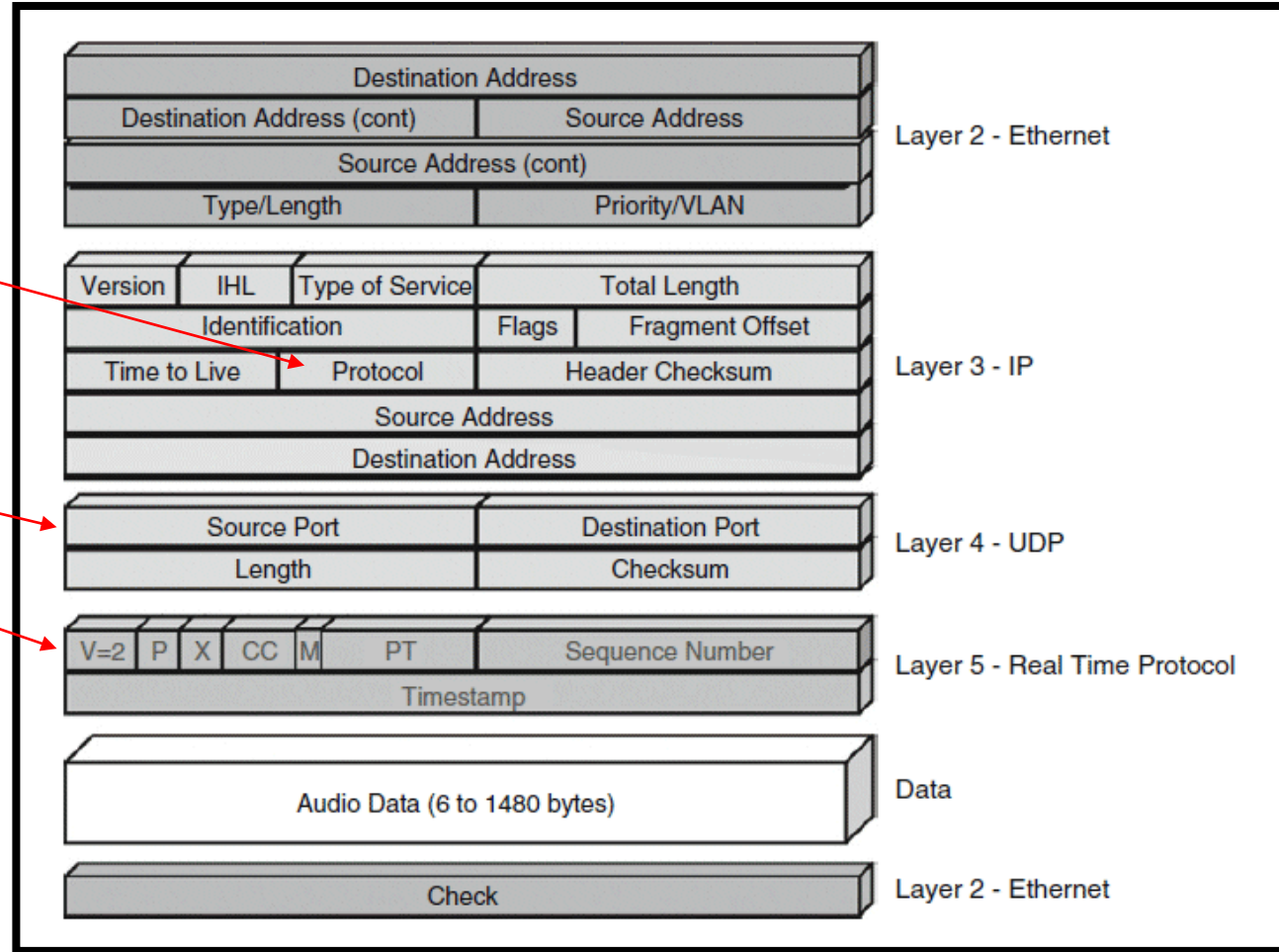
RTCP ports - odd

1024-65534

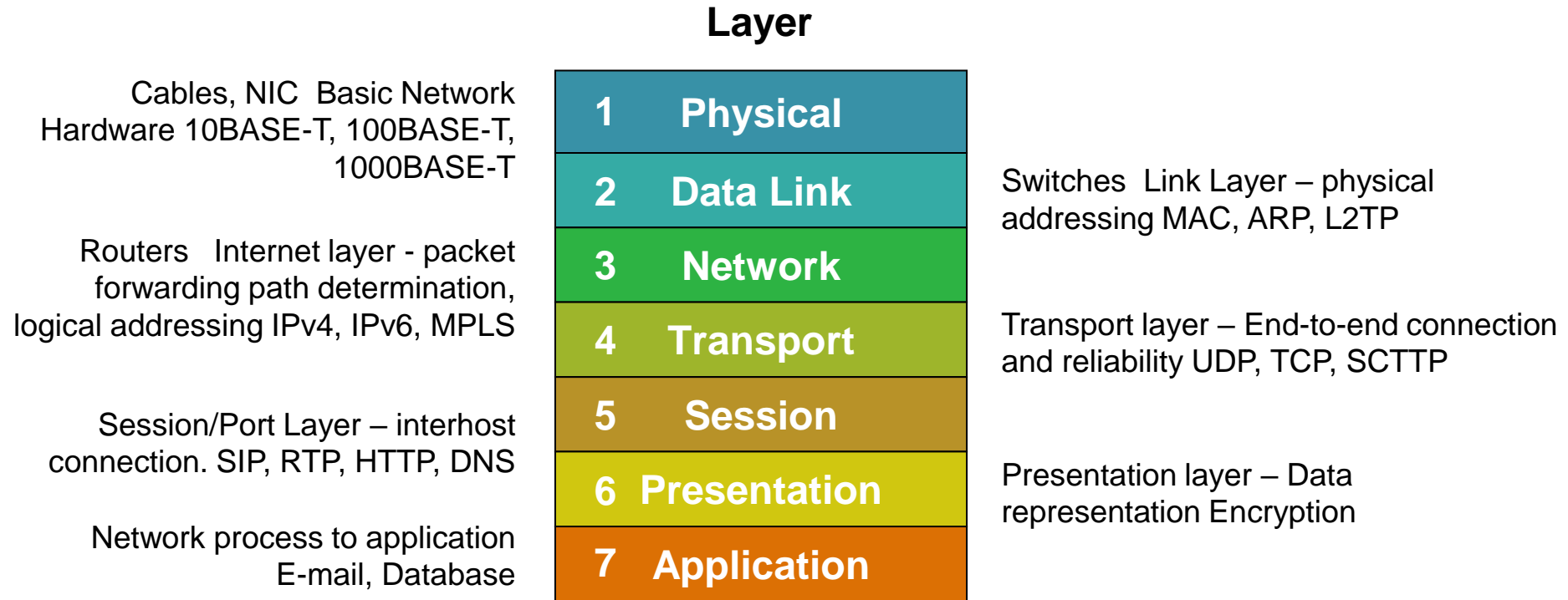
RTP Version

SIP Port 5060

TLS 5061

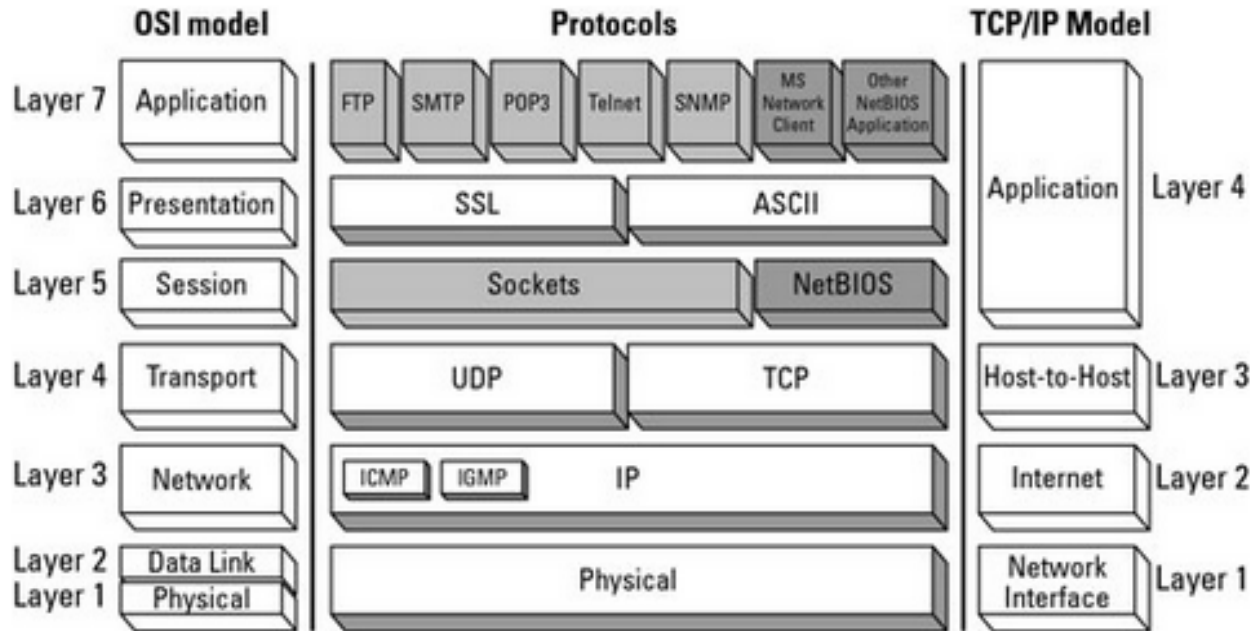


Open System Interconnection



OSI TCP Model

The Transmission Control Protocol/Internet Protocol (TCP/IP) suite was created by the U.S. Department of Defense (DoD) to ensure that communications could survive any conditions and that data integrity wouldn't be compromised under malicious attacks.



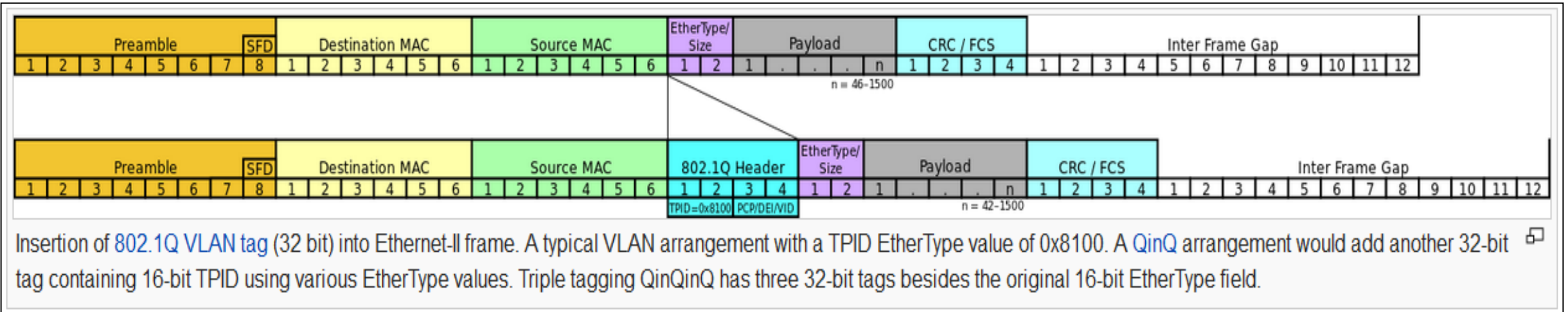
Application (layer 4): Acts as final endpoints at either end of a communication session between two network hosts

Host-to-host (layer 3): Manages the flow of traffic between two hosts or devices, ensuring that data arrives at the application on the host for which it is targeted

Internet (layer 2): Contains all functionality that manages the movement of data between two network devices over a routed network

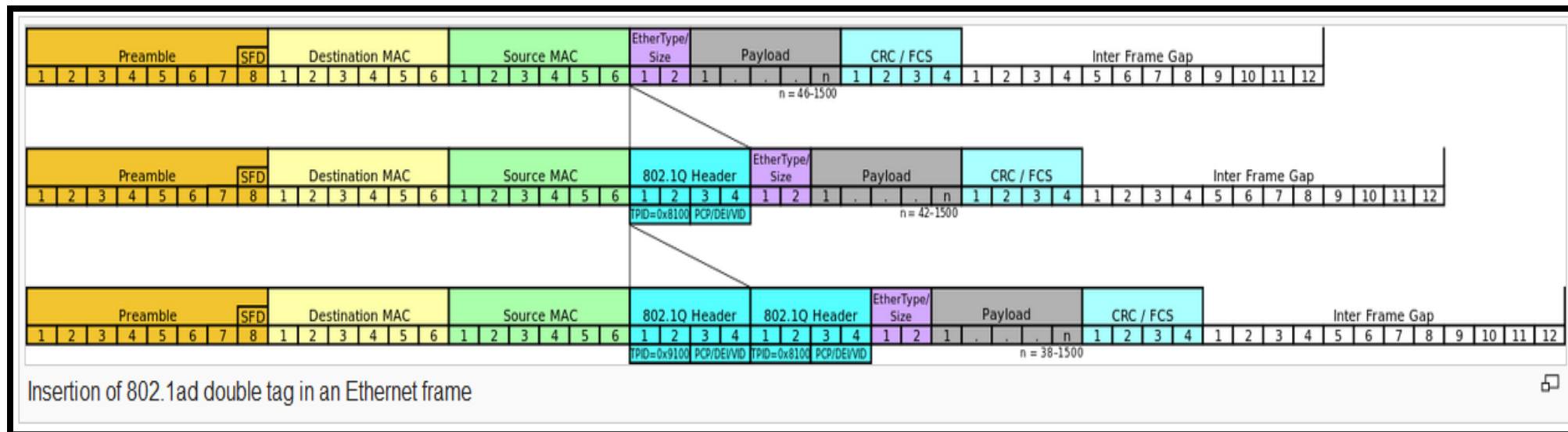
Network interface (layer 1): Deals with all physical components of network connectivity between the network and the IP protocol

Ethernet Frame (FCS)



- Frame Check Sequence (FCS)
 - The FCS field contains a number that is calculated by the source node based on the data in the frame
 - TRUE/FALSE

Ethernet Frame (VLANs)



- IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network

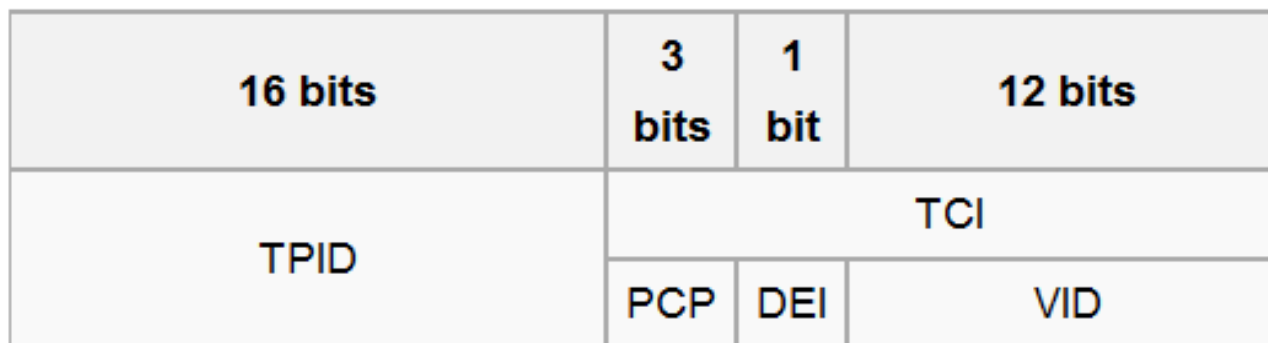
Tag Protocol Identifier (TPID)

Tag Control Information (TCI)

The TCI field is further divided into
Priority code point (PCP)

Drop eligible indicator (DEI)

VLAN identifier (VID)



Internet Protocol IPv4

Offsets	Octet	Internet Header Length		Differentiated Services Code Point				IPv4 Header Format								Explicit Congestion Notification															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	0	Version			IHL				DSCP				ECN				Total Length														
4	32	Identification										Flags				Fragment Offset															
8	64	Time To Live				Protocol				Header Checksum																					
12	96	Source IP Address																													
16	128	Destination IP Address																													
20	160	Options (if IHL > 5)																													

Protocol Number	Protocol Name	Abbreviation
1	Internet Control Message Protocol	ICMP
2	Internet Group Management Protocol	IGMP
6	Transmission Control Protocol	TCP
17	User Datagram Protocol	UDP
41	IPv6 encapsulation	ENCAP
89	Open Shortest Path First	OSPF
132	Stream Control Transmission Protocol	SCTP

Identification – Used for uniquely identifying the group of fragments of a single IP datagram.

Flags – Used to control or identify fragments.

Fragment Offset – 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram.

UDP Frame

UDP Port

FTP – 20 Data Transfer

FTP – 21 FTP Control

SSH – 22

Telnet – 23

SMTP – 25 E-Mail

HTTP – 80

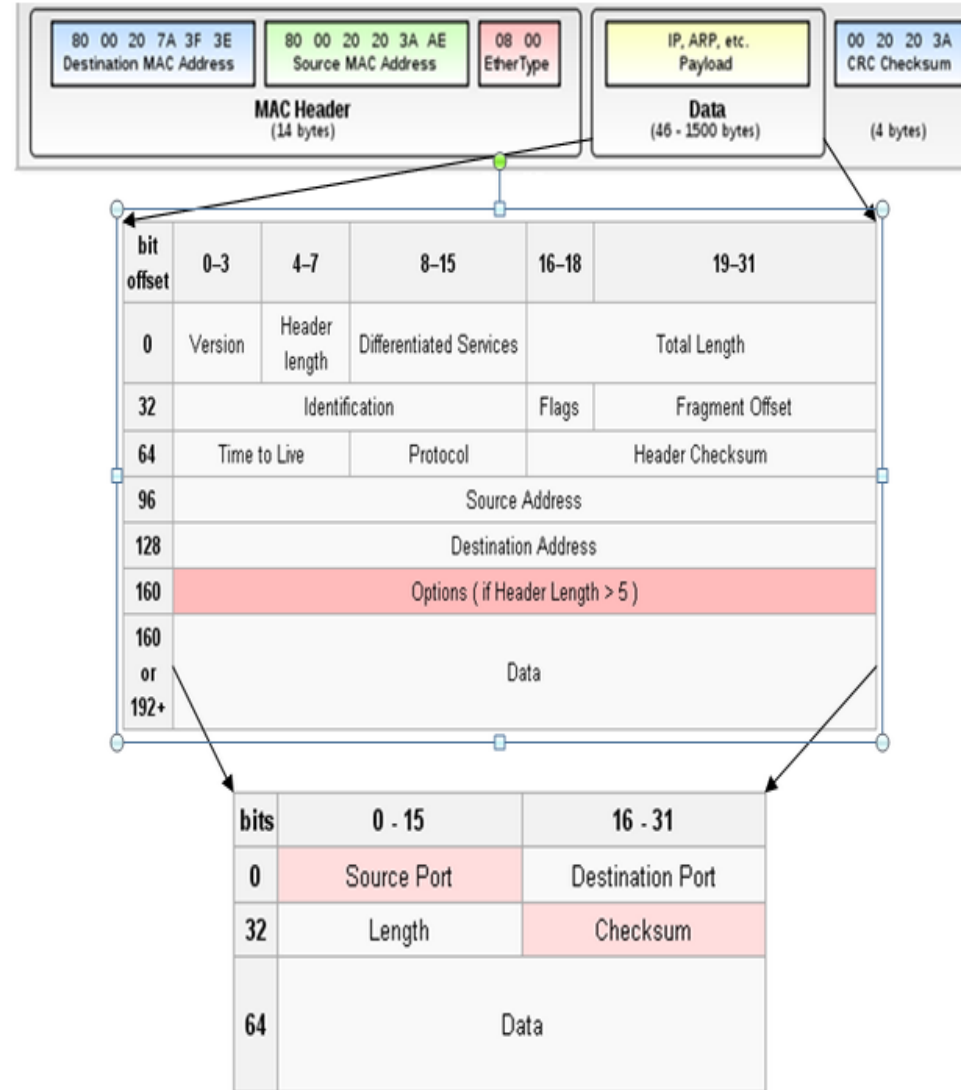
HTTPS – 443

RTP – even 1024 - 65535

RTCP – odd

SIP – 5060 (Destination Port)

SIP over TLS – 5061



Real-time Analysis

The screenshot displays the PacketScan (IpProt) HD 64-bit interface with the following panes:

- Summary View:** A table showing captured packets with columns for Device, Frame#, TIME (Relative), Length (Bytes), Error, Packet Type, Source IP Address, Destination IP Address, Source Address IPv6, Destination Address IPv6, Source Port UDP, Destination Port UDP, Source Port TCP, and Destination Port TCP.
- Detail View:** Ethernet Frame Data for Device2 Frame=0 at 00:00:00.000000000 OK Len=836. It shows MAC Layer and IP Layer details.
- Hex Dump View:** Hex Dump of the Frame Data showing hexadecimal values and their corresponding ASCII characters.
- Statistics View:** A summary table of captured packets, including columns for Device #, Error Code, Length, Protocol Flag, Time Stamp, Destination Address, and Source Address.
- Call Detail Records View:** A table showing call information with columns for Call ID, Call Status, Protocol, Call Originating (Number / Address), Call Destination (Number / Address), Call Start Date & Time, Call Duration, and Protocol Specific Info.

→ Summary View

→ Detail View

→ Hex Dump View

→ Statistics View

→ Call Detail Records View

- Default panes - summary, detail, and hex dump of the frame data views
- Optional panes – statistics and call trace views

TCP Frame

The screenshot shows the 'Add Filter' dialog box in Wireshark. The 'Filter Type' is set to 'Advanced'. The dialog is divided into several sections:

- Field List:** A tree view showing protocol fields. The 'TCP' section is expanded, and 'Destination Port' is selected.
- Operators:** A list of operators including '==' and '!='.
- Value (Decimal Value):** A text input field containing '80,443', which is highlighted with a red box.
- Examples:** A list of example values: 'Ex1: 6000', 'Ex2: 5060,2000,4235', and 'Ex3: 1024-2000'.
- Predefined Values:** A list of predefined values including 'FTP_Data', 'FTP_Control', 'Telnet', 'SMTP', 'DNS', 'HTTP', 'SNMP', 'SNMPTRAP', 'HTTPS', and 'POP3'.

In the background, the 'Add' button is highlighted with a red box, and a red arrow points from it to the 'Add Filter' dialog. The 'Clear All Filters' button is visible at the bottom left of the main window.

Filtering HTTP Traffic

Capture Filters Hardware Filters

Filter Type **Advanced**

Packet Slicing
Length

Filters

- HTTP
- Filter - 2
- Filter - 3
- Filter - 4
- Filter - 5
- Filter - 6
- Filter - 7
- Filter - 8
- Filter - 9
- Filter - 10

Field ID	Protocol	Field Name	Operator	Value	Condition
F1	TCP	Source Port	==	80	
F2	TCP	Destination Port	==	80	

Operators

- ==
- !=

Value (Decimal Value)

Examples :

- Ex1: 6000
- Ex2: 5060,2000,4235
- Ex3: 1024-2000

Predefined Values

- FTP_Data
- FTP_Control
- Telnet
- SMTP
- DNS
- HTTP

Add Insert Delete Clear All Update

Custom Expression

Validate & Update

Selected Filter Expression

Final Configured Expressions | Final Applied Expressions

Clear All Filters

Hardware Filters for Ethernet Fields

Capture Filters Hardware Filters

Filter Type **Advanced**

Packet Slicing
Length

Filters

- GENERAL
- MAC**
- VLANO
- VLAN1
- VLAN2
- IPv4
- IPv6
- ARP
- TCP
- UDP
- SIP
- RTP

Field ID	Protocol	Field Name	Operator	Value	Condition
F1	MAC	Ether Type	==	0800	

MAC (Ether Type)

802.1Q (VLANs)

IPv4

IPv6

Operators

- ==
- !=

Value (Hex Value)

0800

Examples :

Note: Supports single & multiple value only
Ex1: 0809
Ex2: 8100,9000,AF02

Predefined Values

- AARP (0x80F3)
- AppleTalk (0x809B)
- ARP (0x0806)
- ATA over Ethernet(0x88A2)
- Audio Video Transport Protocol (0x22f0)
- CFM Protocol / OAM (0x8902)

Add Insert Delete Clear All Update

Custom Expression

Validate & Update

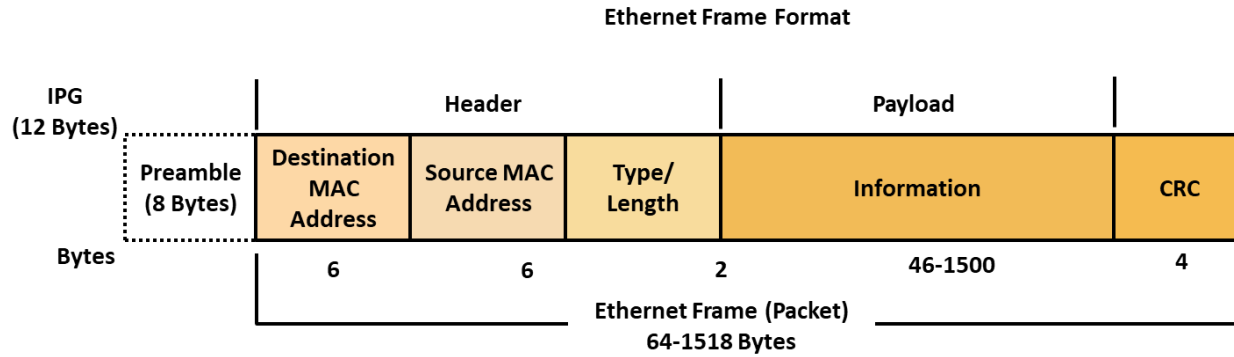
Selected Filter Expression

```
Assign[StreamId = 10] == (mMacTypeLength == 0x0800)
```

Final Configured Expressions Final Applied Expressions

Clear All Filters

Ethernet Frame Structure



Filtering using fields in IP frame

MAC: Media Access Control
 IPG: Inter Packet Gap
 CRC: Cyclic Redundancy Check

802.3 Ethernet packet and frame structure

Layer	Preamble	Start of frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46(42) ^[b] –1500 octets	4 octets	12 octets
Layer 2 Ethernet frame	← 64–1518(1522) octets →								
Layer 1 Ethernet packet	← 72–1526(1530) octets →								

Filtering SIP and RTP Traffic

Capture Filters Hardware Filters

Filter Type **Advanced**

Packet Slicing
Length

Filters

- SIP RTP
- Filter - 2
- Filter - 3
- Filter - 4
- Filter - 5
- Filter - 6
- Filter - 7
- Filter - 8
- Filter - 9
- Filter - 10

Field ID	Protocol	Field Name	Operator	Value	Condition
F1	SIP	SIP Port	==	5060	
F2	RTP	RTP Packets	==	TRUE	

Custom Expression

Selected Filter Expression

```
HashMask[mHashMaskSrcPort = 0xFFFE; mHashMaskDstPort = 0xFFFE] = Hash5Tuple  
Assign[StreamId = 10] = (((Layer4Protocol == UDP)) AND (mSrcPort == 5060 OR mDestPort == 5060)) OR ((mUdpSrcPort != (0..1023)) AND (mRtpVersion == 2))
```

Final Configured Expressions | Final Applied Expressions

```
HashMask[mHashMaskSrcPort = 0xFFFE; mHashMaskDstPort = 0xFFFE] = Hash5Tuple  
Assign[StreamId = 10] = (((Layer4Protocol == UDP)) AND (mSrcPort == 5060 OR mDestPort == 5060)) OR ((mUdpSrcPort != (0..1023)) AND (mRtpVersion == 2))
```

Layer4 Protocol

- UDP
- TCP
- SCTP

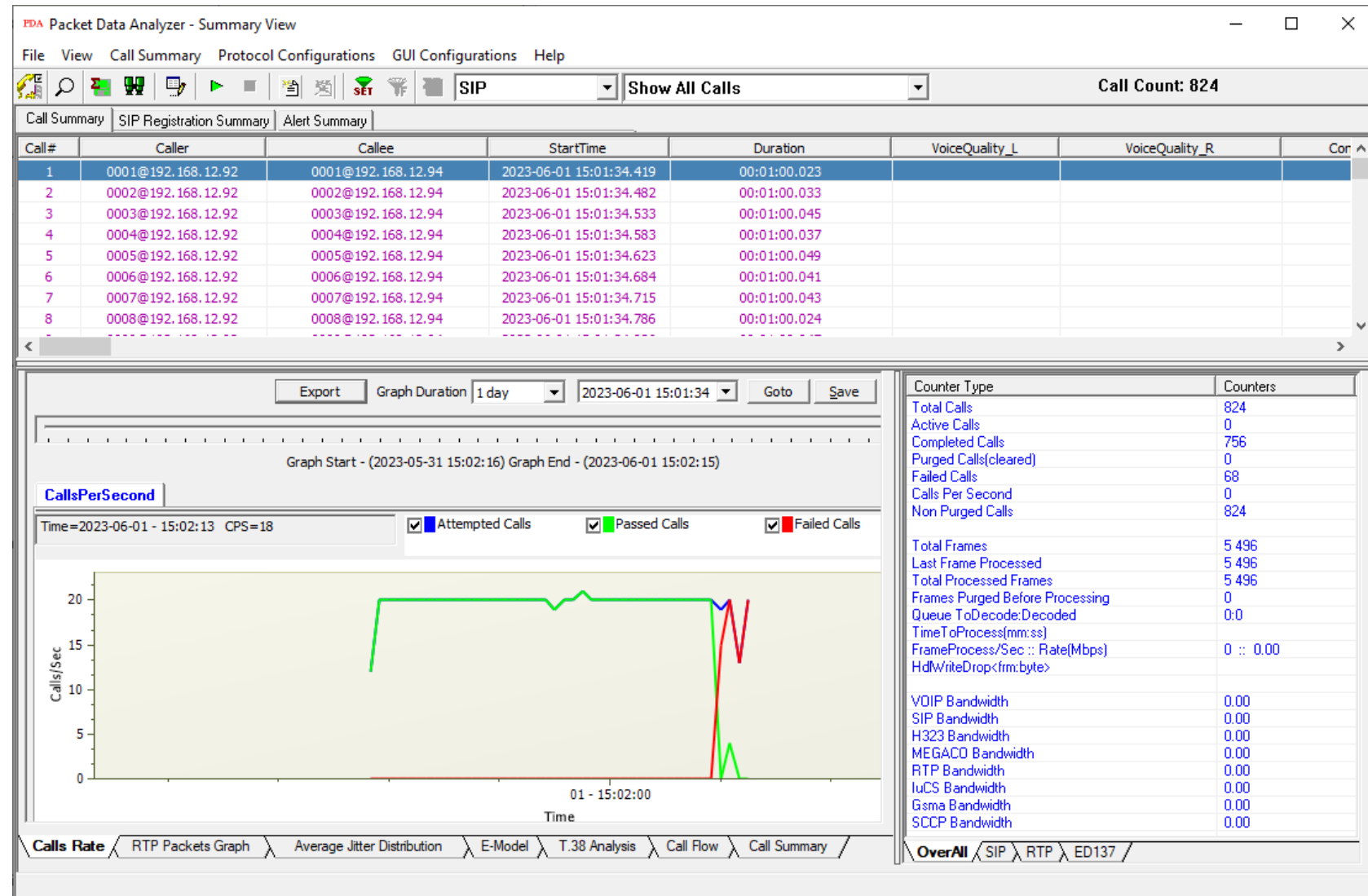
Value (Decimal Value)

Examples :

- Ex1: 5060
- Ex2: 5060,2000,4235
- Ex3: 5060-5070

Packet Data Analyzer (PDA) Summary View

- Summary View displays -
 - Summary of data transmission in each direction including calling number, called number, call id, start time, duration, missing packets, etc.
 - Includes separate statistical counts on total packets, calls, failed calls, captured frames, etc., for SIP, H323, MEGACO, and RTP based calls
 - Provides various graphs to view active calls, average jitter distribution, E-model based measurements for R-factor / MOS/ Packet discarded, RTP packets, T.38 fax analysis, and call signaling, Gap, Jitter, Gap/Jitter Distribution, Wave and Spectral Display for media stream analysis, VoIP calls and more



Displaying Filtered Calls using Expressions

- Filter CDRs (Call Detail Records) based on parameters such as caller, time, message count, etc.
- The expression supports the following mathematical operators: ==, <=, >=, !=, <, >, &&, ||
- For example, the filter expression "Error Code==400||Error Code>600" will display calls with Error Code equal to 400 and calls with Error Code greater than 600

PDA Packet Data Analyzer - Summary View

File View Call Summary Protocol Configurations GUI Configurations Help

SIP Show Filtered Calls Call Count: 6

ErrorCode==400 || ErrorCode>600

Call Summary SIP Registration Summary Alert Summary

Payload_R	ErrorCode	FailureCause	CallID	EndTime	PostDialDelay	SessionDisconnectDe
	400	5	GL-MAPS-2654-766727097-26124-3688@192.168.12.92	2023-06-01 15:02:12.275	9	0
	603	4	GL-MAPS-2679-766728649-26314-14696@192.168.12.92	2023-06-01 15:02:13.828	9	0
	604	4	GL-MAPS-2677-766728698-26320-13540@192.168.12.92	2023-06-01 15:02:13.879	19	0
	606	4	GL-MAPS-2677-766728748-26326-14572@192.168.12.92	2023-06-01 15:02:13.919	9	0
	400	5	GL-MAPS-2685-766728798-26332-6156@fe80::3f20:7953:f2df:f26a	2023-06-01 15:02:13.973	18	0
	606	4	GL-MAPS-2709-766730449-26530-14696@fe80::3f20:7953:f2df:f26a	2023-06-01 15:02:15.632	9	0

Save Call in *.hdl, *.pcap, and *.pcapng Formats

The screenshot displays the Packet Data Analyzer (PDA) interface in Summary View. The main window shows a table of call records. A context menu is open over the third call record, with the 'Save Call' option selected. A dialog box titled 'PDA Save Call - CallNum_3' is displayed, allowing the user to choose the file format (HDL File, PCAP File, and PCAPNG are checked) and the save path. Below the table, a 'Calls Per Second' graph shows the call rate over time. The bottom of the interface features a navigation bar with various analysis tabs.

Call #	Caller	Callee	StartTime	Duration	VoiceQuality_L	VoiceQuality_R	Cor
1	0001@192.168.12.92	0001@192.168.12.94	2023-06-01 15:01:34.419	00:01:00.023			
2	0002@192.168.12.92	0002@192.168.12.94	2023-06-01 15:01:34.482	00:01:00.033			
3	0003@192.168.12.92	0003@192.168.12.94	2023-06-01 15:01:34.533				
4	0004@192.168.12.92	0004@192.168.12.94	2023-06-01 15:01:34.583				
5	0005@192.168.12.92	0005@192.168.12.94	2023-06-01 15:01:34.623				
6	0006@192.168.12.92	0006@192.168.12.94	2023-06-01 15:01:34.684	00:01:00.041			
7	0007@192.168.12.92	0007@192.168.12.94	2023-06-01 15:01:34.715	00:01:00.043			
8	0008@192.168.12.92	0008@192.168.12.94					
9	0009@192.168.12.92	0009@192.168.12.94					

PDA Save Call - CallNum_3

File Type: HDL File PCAP File PCAPNG Link Type: 0

Path: C:\Program Files\GL Communications Inc\PacketScan\

Overwrite Files

Counters	Value
Total Calls	824
Failed Calls	0
Aborted Calls	756
Unanswered Calls	0
Unanswered Calls	68
Unanswered Calls	0
Unanswered Calls	824
Unanswered Calls	5 496
Unanswered Calls	5 496
Unanswered Calls	5 496
Unanswered Calls	0
Unanswered Calls	0:0
Unanswered Calls	0 :: 0.00
Unanswered Calls	
Unanswered Calls	0.00
Unanswered Calls	0.00
Unanswered Calls	0.00
Unanswered Calls	0.00
Unanswered Calls	0.00
Unanswered Calls	0.00
Unanswered Calls	0.00

Copy Cell Value to Clipboard

The screenshot displays the 'Packet Data Analyzer - Summary View' interface. At the top, a menu bar includes 'File', 'View', 'Call Summary', 'Protocol Configurations', 'GUI Configurations', and 'Help'. Below the menu is a toolbar with various icons and a 'SIP' dropdown menu. The main area features a 'Call Summary' tab with a table of call records. The table has columns for 'Call #', 'Caller', 'Callee', 'StartTime', 'Duration', 'VoiceQuality_L', 'VoiceQuality_R', and 'Cor'. Call #3 is selected, and a context menu is open over it, showing 'Save Call' and 'Copy Cell Value' options. A red arrow points from the 'Copy Cell Value' option to a Notepad window titled '*Untitled - Notepad'. The Notepad window contains the text: '2023-06-01 15:01:34.533', '00:01:00.045', and '0003@192.168.12.92'. Below the table is a 'Graph Duration' section with '5 days' selected and a 'Goto' button. The graph area shows 'Calls Per Second' with a line chart for 'Attempted Calls', 'Passed Calls', and 'Failed Calls'. The y-axis is 'Calls/Sec' (0-20) and the x-axis is 'Time' (01 - 15:02:00). A statistics panel on the right lists various metrics like 'Active Calls', 'Completed Calls', and 'Total Frames'. The bottom status bar shows 'Calls Rate', 'RTP Packets Graph', 'Average Jitter Distribution', 'E-Model', 'T.38 Analysis', 'Call Flow', 'Call Summary', and 'OverAll SIP RTP ED137'.

Call #	Caller	Callee	StartTime	Duration	VoiceQuality_L	VoiceQuality_R	Cor
1	0001@192.168.12.92	0001@192.168.12.94	2023-06-01 15:01:34.419	00:01:00.023			
2	0002@192.168.12.92	0002@192.168.12.94	2023-06-01 15:01:34.482	00:01:00.033			
3	0003@192.168.12.92	0003@192.168.12.94	2023-06-01 15:01:34.533	00:01:00.045			
4	0004@192.168.12.92	0004@192.168.12.94	2023-06-01 15:01:34.588	00:01:00.041			
5	0005@192.168.12.92	0005@192.168.12.94	2023-06-01 15:01:34.612	00:01:00.043			
6	0006@192.168.12.92	0006@192.168.12.94	2023-06-01 15:01:34.684	00:01:00.024			
7	0007@192.168.12.92	0007@192.168.12.94	2023-06-01 15:01:34.715	00:01:00.024			
8	0008@192.168.12.92	0008@192.168.12.94	2023-06-01 15:01:34.786	00:01:00.047			

Statistics Panel:

Active Calls	0
Completed Calls	756
Purged Calls(cleared)	0
Failed Calls	68
Calls Per Second	0
Non Purged Calls	824
Total Frames	5 496
Last Frame Processed	5 496
Total Processed Frames	5 496
Frames Purged Before Processing	0
Queue ToDecode:Decoded	0:0
TimeToProcess(mm:ss)	
FrameProcess/Sec :: Rate(Mbps)	0 :: 0.00
HdWriteDrop<frm:byte>	
VOIP Bandwidth	0.00
SIP Bandwidth	0.00
H323 Bandwidth	0.00
MEGACO Bandwidth	0.00
RTP Bandwidth	0.00
IuCS Bandwidth	0.00
Gsma Bandwidth	0.00
SCCP Bandwidth	0.00

Packet Data Analysis (PDA) Call Graph – SIP Call

- Displays the message sequences of captured VoIP calls
- Decodes of the selected SIP message is displayed on the right pane

The screenshot displays the PDA Packet Data Analyzer interface. The top section shows a 'Call Summary' table with columns for Call#, Caller, Callee, StartTime, Duration, VoiceQuality_L, VoiceQuality_R, Payload_L, Payload_R, Result, and ErrorCode. A red box highlights the first row of the table, which corresponds to the selected call.

Call#	Caller	Callee	StartTime	Duration	VoiceQuality_L	VoiceQuality_R	Payload_L	Payload_R	Result	ErrorCode
1	0001@192.168.12.92	0001@192.168.12.94	2023-06-01 15:01:34.419	00:01:00.023			PCMU/8000	PCMU/8000	Pass	0
2	0002@192.168.12.92	0002@192.168.12.94	2023-06-01 15:01:34.482	00:01:00.033			MuLAW_2/8000	MuLAW_2/8000	Pass	0
3	0003@192.168.12.92	0003@192.168.12.94	2023-06-01 15:01:34.533	00:01:00.045			PCMA/8000	PCMA/8000	Pass	0
4	0004@192.168.12.92	0004@192.168.12.94	2023-06-01 15:01:34.583	00:01:00.037			ALAW_2/8000	ALAW_2/8000	Pass	0
5	0005@192.168.12.92	0005@192.168.12.94	2023-06-01 15:01:34.623	00:01:00.049			G729/8000	G729/8000	Pass	0
6	0006@192.168.12.92	0006@192.168.12.94	2023-06-01 15:01:34.684	00:01:00.041			G729B/8000	G729B/8000	Pass	0
7	0007@192.168.12.92	0007@192.168.12.94	2023-06-01 15:01:34.715	00:01:00.043			GSM/8000	GSM/8000	Pass	0

Below the table is a 'Call Graph' showing a sequence of SIP messages between 192.168.12.92 and 192.168.12.94. The messages are: INVITE (00:00.000), SIP/2.0 100 Trying (00:00.020), SIP/2.0 180 Ringing (00:00.029), SIP/2.0 200 OK (00:00.153), ACK (00:00.163), BYE (01:00.177), and SIP/2.0 200 OK (01:00.187). A red arrow points from the first row of the table to the INVITE message in the graph.

The right pane shows the decoded SIP message details for the selected INVITE. A red box highlights the 'Find' field with the option 'Complete Stack' checked. A red arrow points from the 'SIP/2.0 200 OK' message in the graph to the decoded message details.

```
===== MAC Layer =====
Destination Address      = x6C626D3EEB30
Source Address          = x54BEF737BC79
Length/Protocol Type    = x0800 Internet IP(IPv4)
===== IPv4 Layer =====
Version                 = 0100.... (4)
Internet Header Length (In 32 bit words) = ....0101 (5)
Differentiated Services Field
Differentiated Services Codepoint = 000000.. Default
Explicit Congestion Notification = .....00 Not-ECT (Not ECN-...)
IP Hdr No TCP SegmentationOffload =
Total Length            = 761 (x02F9)
Identification         = 15592 (x3CE8)
Reserved Bit           = 0..... Not Set
Don't fragment         = .0..... Not Set
More fragments        = ..0.... Not Set
Fragment Offset        = 0 (...000000 00000000)
Time To Live           = 128 (x80)
Protocol               = 00010001 UDP
Header Check Sum       = x0000
Source IP Address      = 192.168.12.92 (xC0A80C5C)
Destination IP Address = 192.168.12.94 (xC0A80C5E)
```

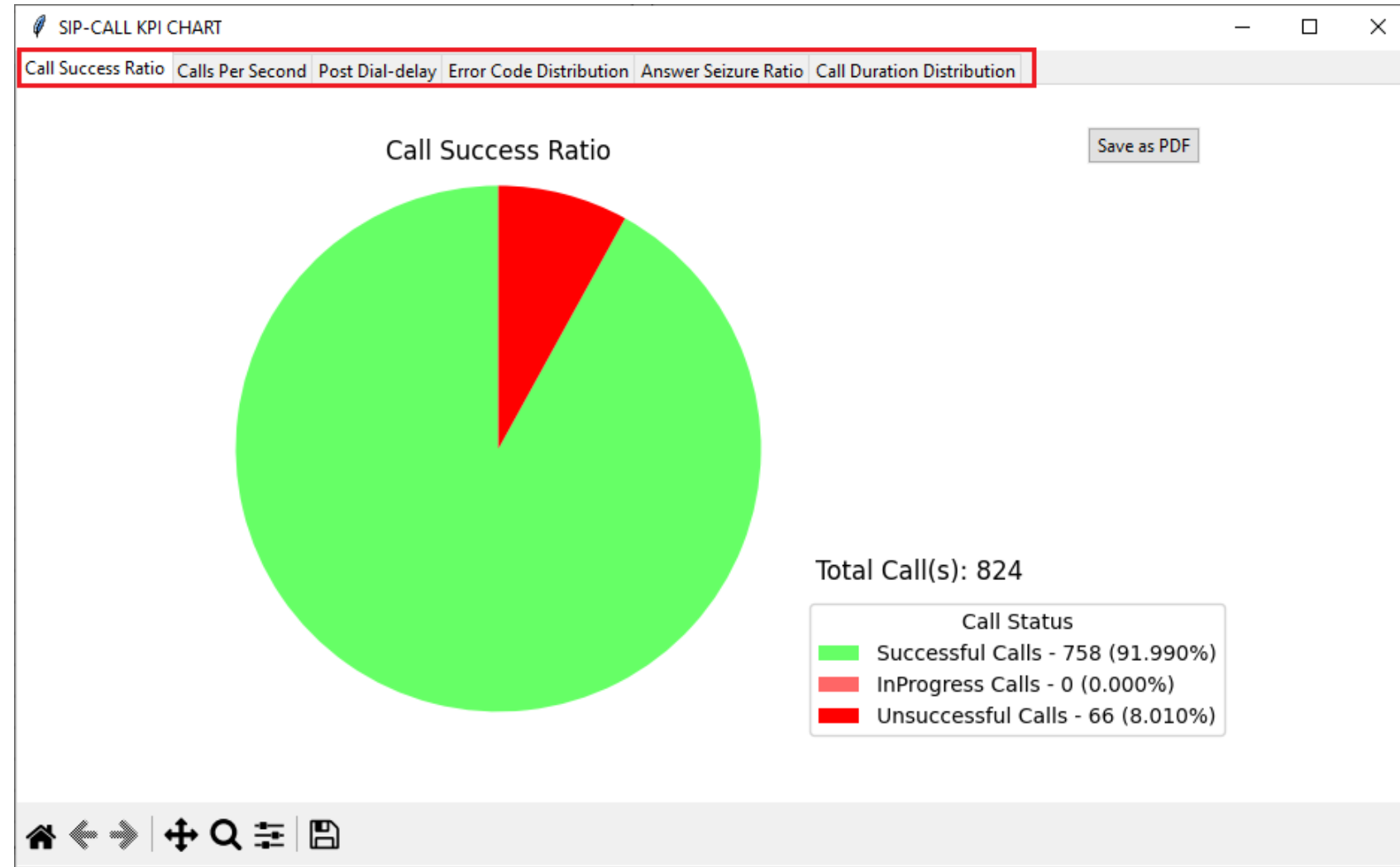
Displays decoded information of the selected SIP message

Key Performance Indicators (KPIs) Report for SIP Calls

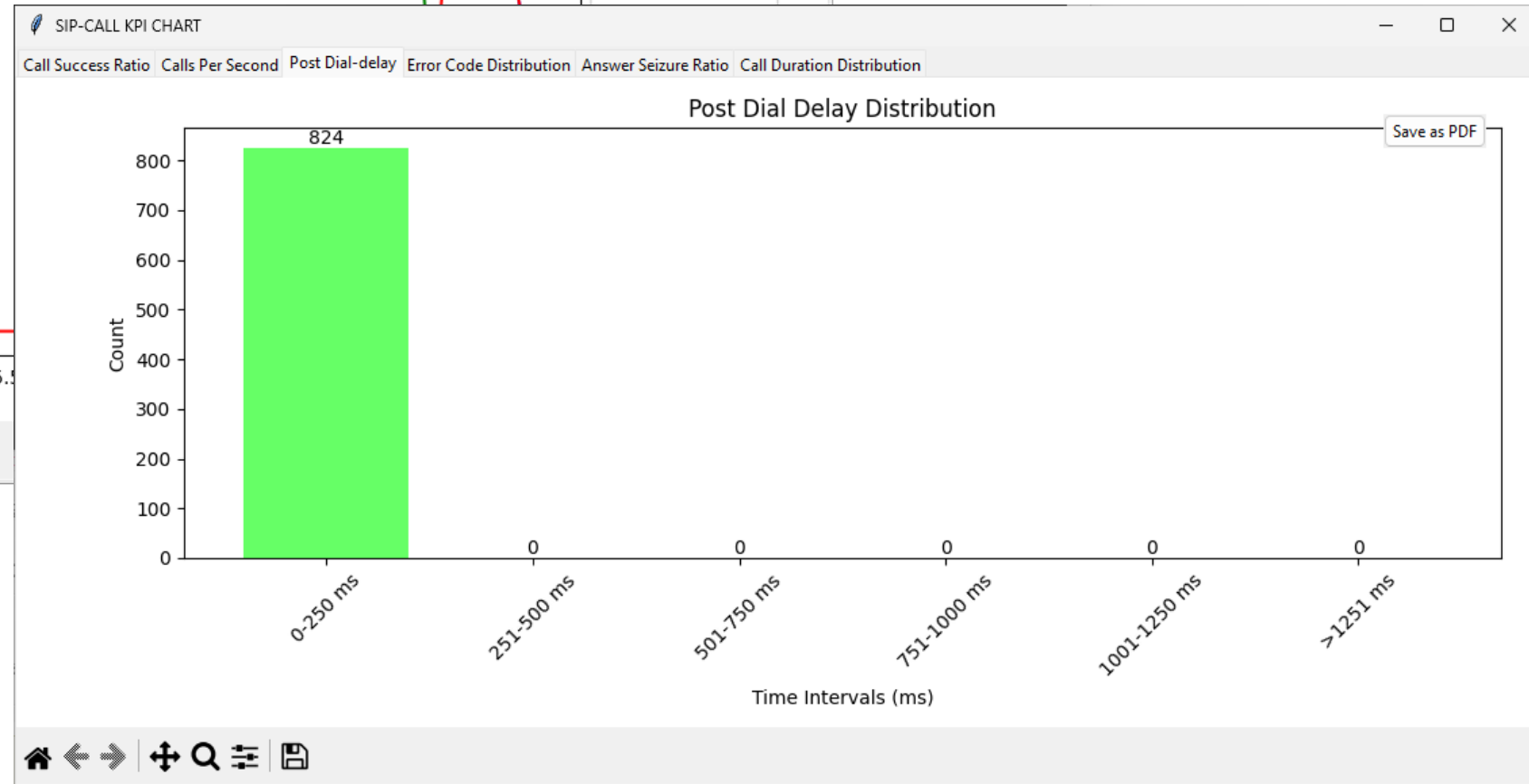
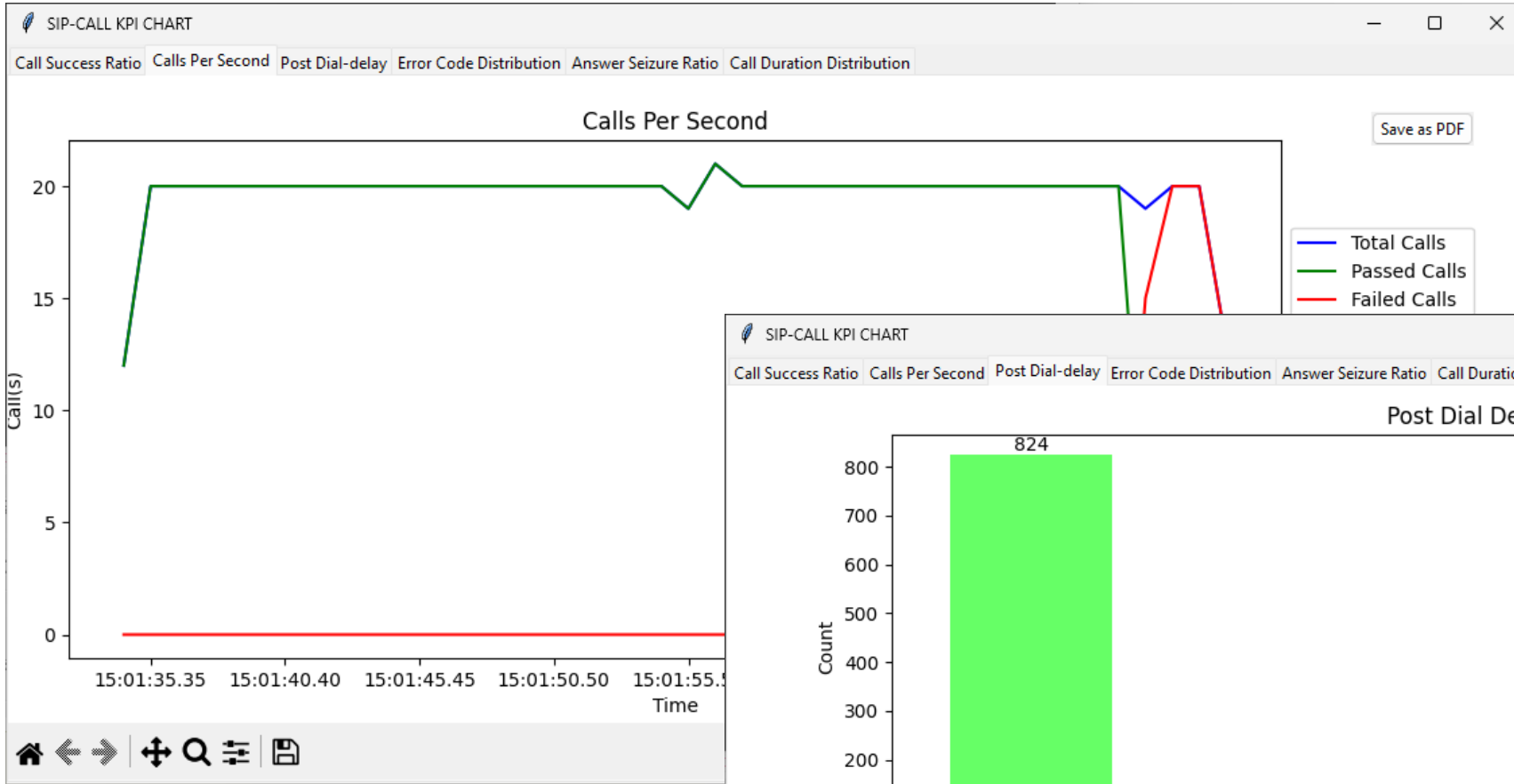
Call Success Ratio KPI

The **SIP Call Summary KPI** chart includes KPIs for the following:

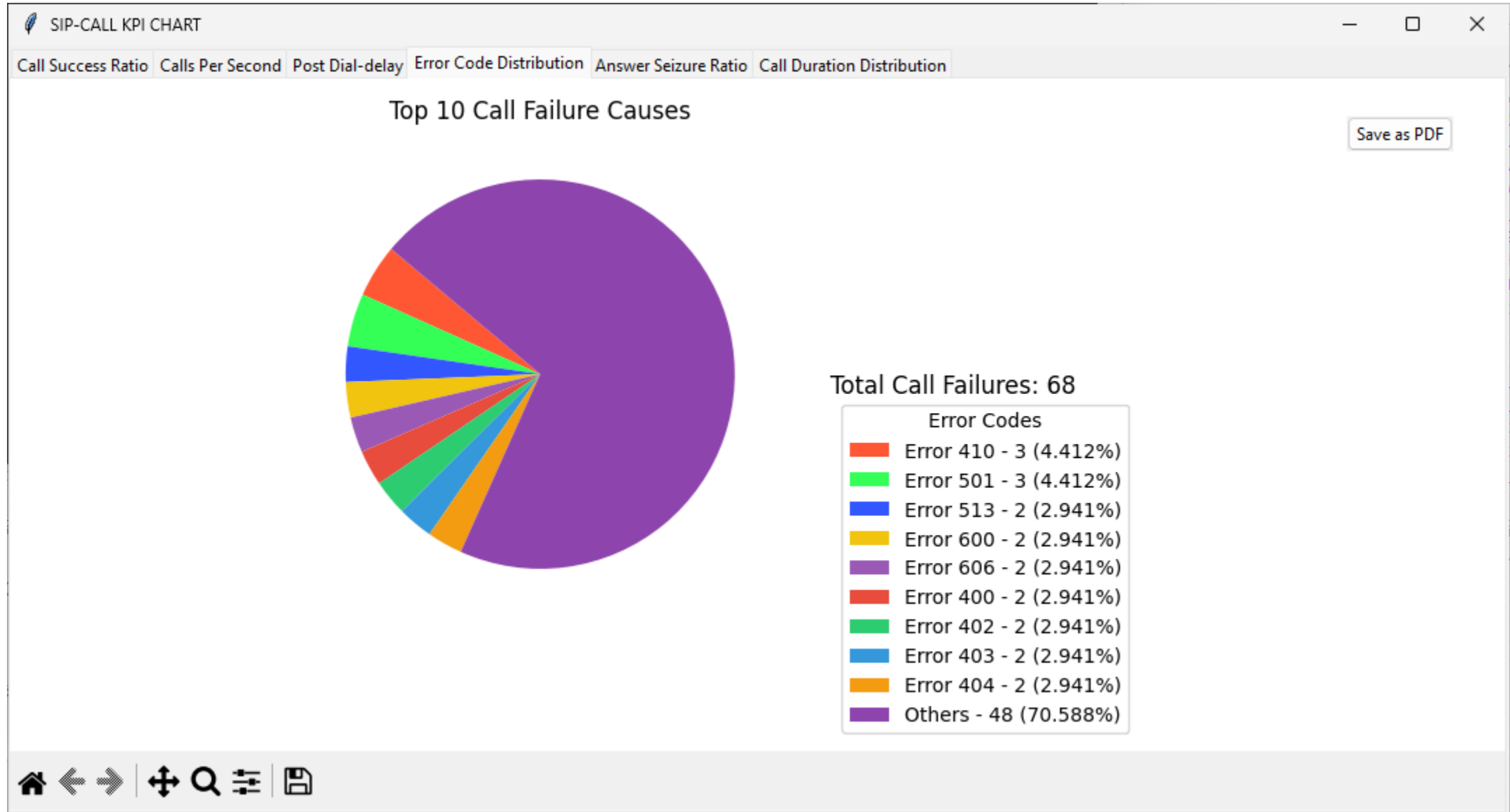
- **Call Success Ratio:** Displays graph for "Successful" and "Unsuccessful Calls," including counts and percentages (%)
- **Calls Per Second:** Shows graph "Total," "Passed," and "Failed Calls per second."
- **Post Dial Delay:** Shows delay counts in milliseconds (0-250ms, 251-500ms, etc.)
- **Error Code Distribution:** Lists Top 10 Call Failure Causes with counts and percentages (%)
- **Answer Seizure Ratio:** Shows "Answered" and "Unanswered Calls," with counts and percentages (%)
- **Call Duration Distribution:** Provides call counts for different durations (0-1 sec, 1-10 sec, etc.)



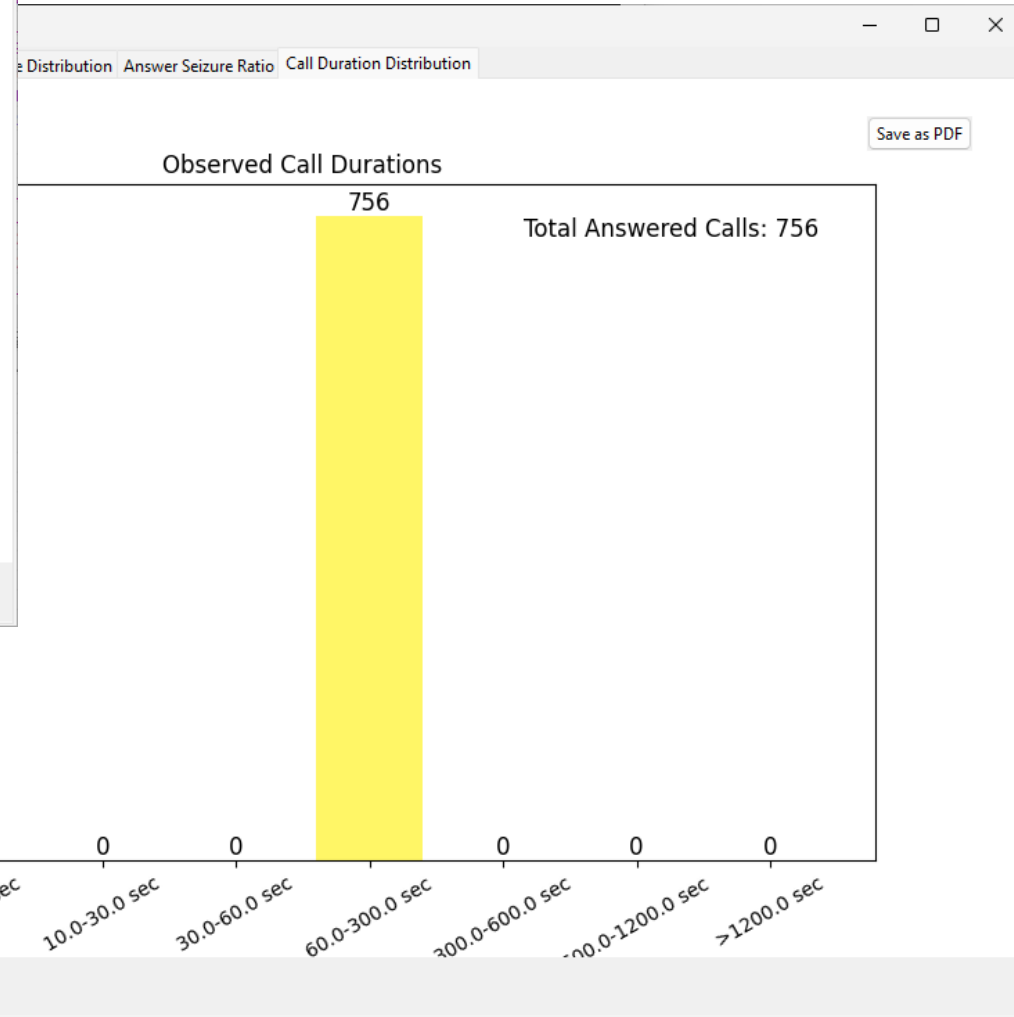
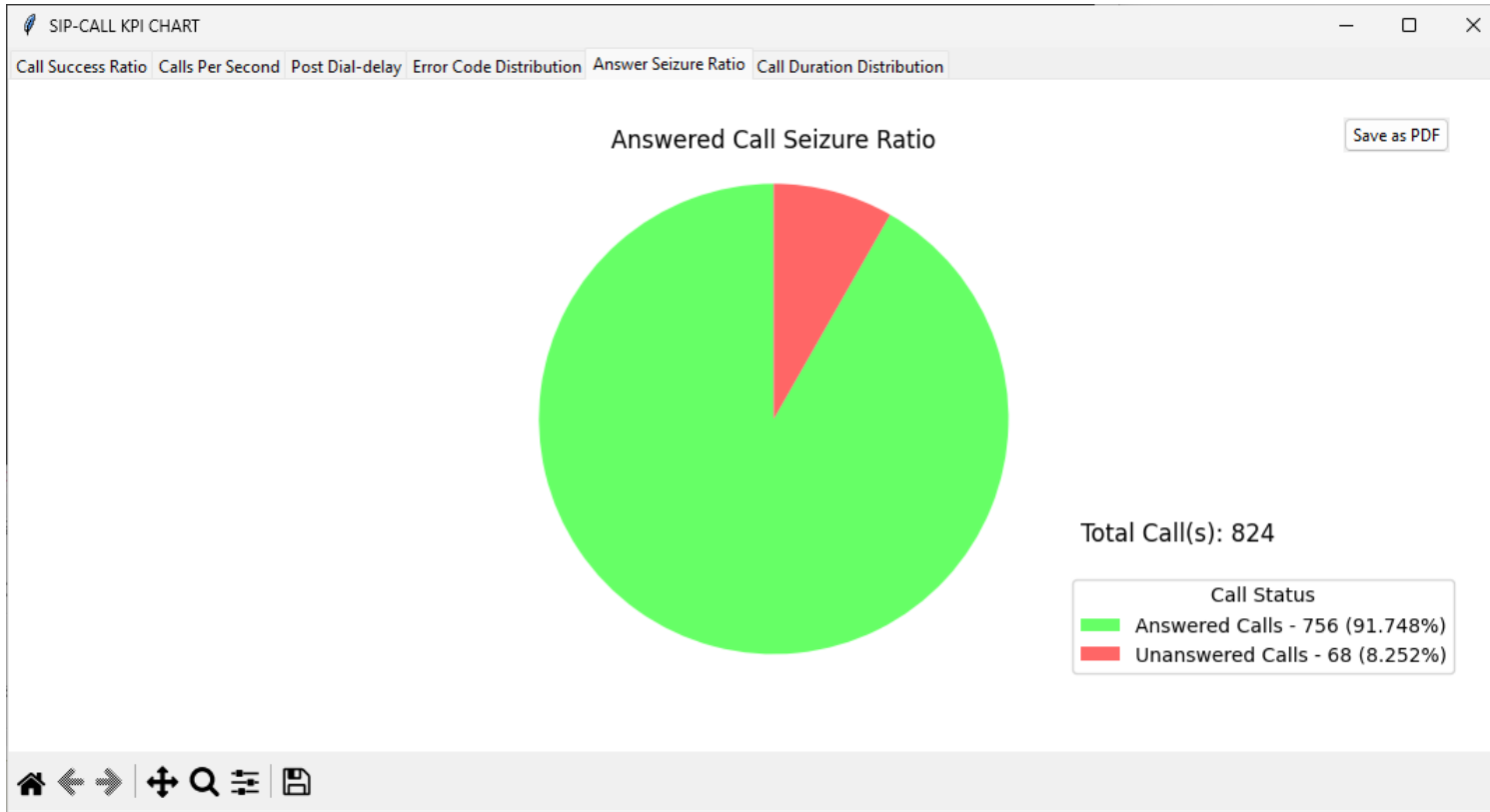
Calls Per Second and Post Delay KPIs



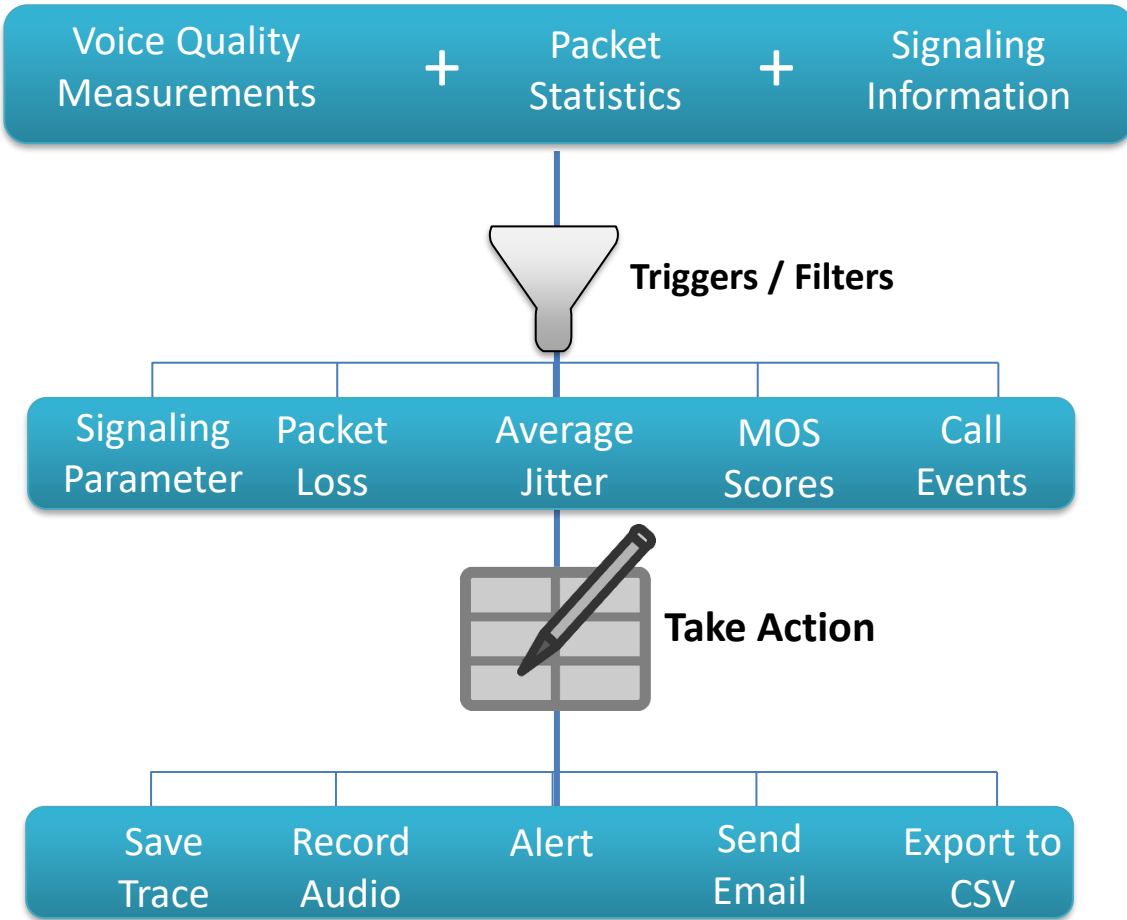
Error Code Distribution KPI



Answer Seizure Ratio and Call Duration Distribution KPIs



Triggers and Actions



- Triggers can be:
 - Calling/Called Number, Pass/Fail Calls, Voice/SMS/Fax Calls, Call Duration, MOS, SIP Error Code
- Follow on actions can be performed:
 - Saves call in HDL or Wireshark file format
 - Export selected call detail records to CSV file
 - Record audio to file and send email alerts
 - Extracts fax image in the TIFF format from the selected fax call

Voice Quality Metrics (Sample based)

- MOS is calculated periodically throughout the call which can help to mark the calls with Good, Average and Poor voice quality

Voice Quality Settings

File

Codec based MOS Distribution

Codec	Poor MOS Value	Average MOS Value	Good MOS Value
PCMA	0.00-3.00	3.00-4.00	4.00-4.50
PCMU	0.00-3.00	3.00-4.00	4.00-4.50
G726-40	0.00-2.60	2.60-3.90	3.90-4.18
G726-32	0.00-2.40	2.40-3.70	3.70-4.09
G726-24	0.00-2.00	2.00-3.10	3.10-3.44
G726-16	0.00-1.50	1.50-2.60	2.60-2.92
G729	0.00-2.40	2.40-3.70	3.70-4.01
G729B	0.00-2.40	2.40-3.70	3.70-4.01
GSM	0.00-2.20	2.20-3.30	3.30-3.68
GSM-EFR	0.00-2.60	2.60-3.90	3.90-4.16
AMR	0.00-2.20	2.20-3.30	3.30-4.16
GSM-HR	0.00-2.20	2.20-3.30	3.30-3.53
EVRC	0.00-2.20	2.20-3.30	3.30-3.95
ILBC	0.00-2.40	2.40-3.70	3.70-4.01
SPEEX	0.00-1.80	1.80-2.90	2.90-4.14
ILBC-13-33	0.00-2.40	2.40-3.70	3.70-4.01
G722	0.00-2.40	2.40-3.70	3.70-3.91
SPEEX-WB	0.00-2.40	2.40-3.70	3.70-4.14
AMR-WB	0.00-2.00	2.00-3.10	3.10-4.18
EVRCB	0.00-2.20	2.20-3.30	3.30-3.95
EVS-NB	0.00-2.60	2.60-3.90	3.90-4.20
EVS-WB	0.00-2.60	2.60-3.90	3.90-4.20
EVS-SWB	0.00-2.60	2.60-3.90	3.90-4.20
EVS-FB	0.00-2.60	2.60-3.90	3.90-4.20
OPUS-NB	0.00-2.40	2.40-3.70	3.70-4.01

Voice Quality Settings

Sample MOS Every secs Voice Quality Range ?

Poor%::0-75
Average%::76-89
Good%::90-100

OK Default

PDA Packet Data Analyzer - Detail View

File View Detail View Protocol Configurations GUI Configurations Help

SIP Show All Calls

Call Summary Registrar Summary Alert Summary

Packet #	Sequ...	RTP Tim...	Payload ...	P	Packet Sequence	Gap(ms)	Gap A...	Packet #	Sequence #	RTP Tim...	Payload...	Pa...	Packet Sequ...	Gap(ms)	Gap A...
48269	42170	3682328...	PCMU/8...	1..	Jump Within Limit	55.05	60.00	48910	34420	3699202...	PCMU/...	160	In Sequence	20.01	20.00
48272	42172	3682329...	PCMU/8...	1..	Jump Within Limit	43.93	40.00	48911	34421	3699202...	PCMU/...	160	In Sequence	20.01	20.00
48277	42176	3682329...	PCMU/8...	1..	Jump Within Limit	76.96	80.00	48912	34422	3699202...	PCMU/...	160	In Sequence	19.93	20.00
48280	42178	3682330...	PCMU/8...	1..	Jump Within Limit	42.94	40.00	48913	34423	3699202...	PCMU/...	160	In Sequence	20.01	20.00

Mean Opinion Score (Mos) During Call

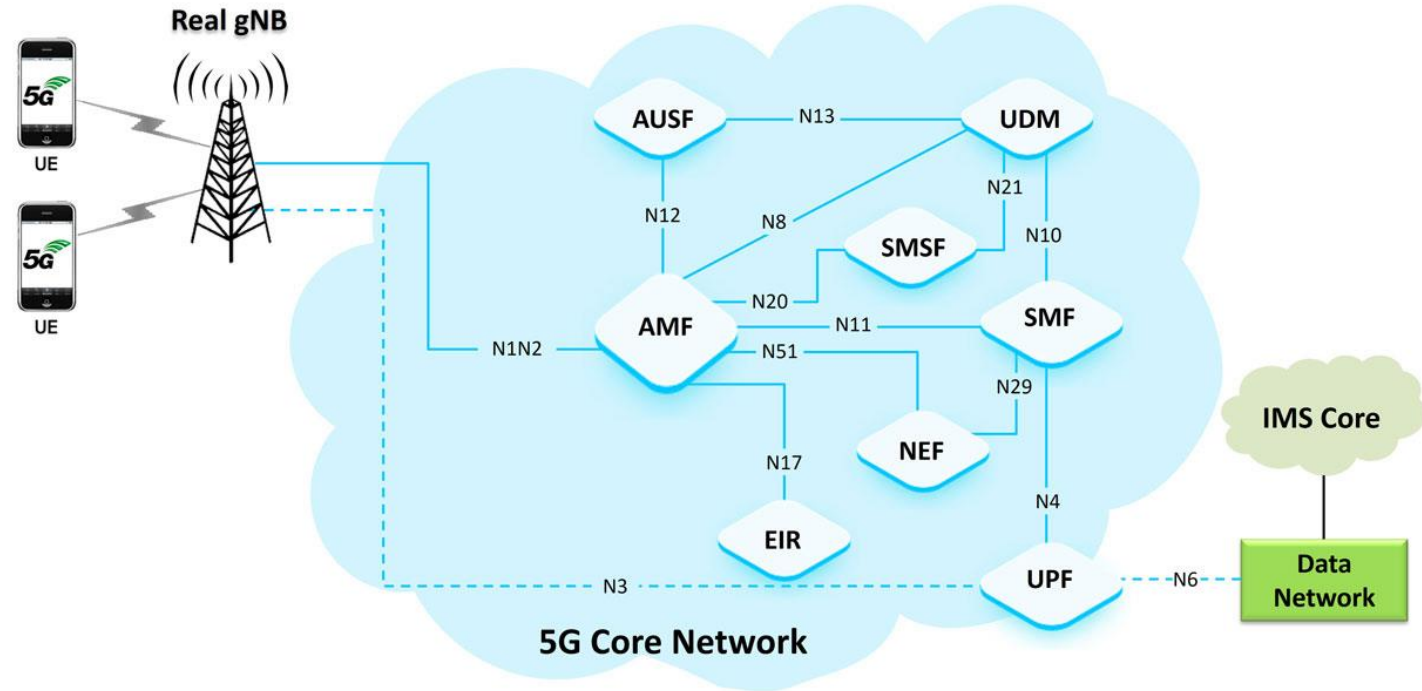
Time in Seconds

Left MOS Right MOS

Gap Graph Jitter Graph Gap Distribution Graph Jitter Distribution Graph MOS Graph Inband Events RTP Events Wave Graph Spectral Display R-Factor Statistics

5G Protocol Analyzer

- Capture, Decode, and Analysis of Calls in 5G Network
- Supported protocols - Non-Access Stratum (NAS), Next Generation Application Protocol (NGAP), Packet Forwarding Control Protocol (PFCP), XnAP, SCTP, UDP, TCP, and IP
- Following interfaces are supported in Packet Data Analyzer:
 - N1 N2, N4, N8, N10, N11, N12, and N13
 - Packet Data Analyzer feature in Packetscan™ HD provide a complete call flow of a 5G session



Decode View - 5G NGAP Layer

PacketScan 64-bit

File View Capture Statistics Database Call Detail Records Configure Help

2609 GoTo

Device	Frame#	TIME (Date)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IPv4	Destination IP Address IPv4	Source Address IPv6
✓	1	2609	2023-06-13 15:02:20.229319000		158	Internet IP[IPv4]	192.168.13.181	192.168.13.184	
✓	1	2610	2023-06-13 15:02:20.229391000		277	Internet IP[IPv4]	192.168.13.184	192.168.13.191	
✓	1	2611	2023-06-13 15:02:20.229391000		162	Internet IP[IPv4]	192.168.13.184	192.168.13.191	
✓	1	2612	2023-06-13 15:02:20.229391000		169	Internet IP[IPv4]	192.168.13.184	192.168.13.191	
✓	1	2613	2023-06-13 15:02:20.229496000		162	Internet IP[IPv4]	192.168.13.184	192.168.13.191	
✓	1	2614	2023-06-13 15:02:20.229601000		169	Internet IP[IPv4]	192.168.13.184	192.168.13.191	
✓	1	2615	2023-06-13 15:02:20.229706000		315	Internet IP[IPv4]	192.168.13.191	192.168.13.188	
✓	1	2616	2023-06-13 15:02:20.229706000		193	Internet IP[IPv4]	192.168.13.191	192.168.13.188	
✓	1	2617	2023-06-13 15:02:20.229706000		176	Internet IP[IPv4]	192.168.13.191	192.168.13.188	
✓	1	2618	2023-06-13 15:02:20.229812000		193	Internet IP[IPv4]	192.168.13.191	192.168.13.188	
✓	1	2619	2023-06-13 15:02:20.229917000		176	Internet IP[IPv4]	192.168.13.191	192.168.13.188	
✓	1	2620	2023-06-13 15:02:20.230022000		393	Internet IP[IPv4]	192.168.13.188	192.168.13.191	
✓	1	2621	2023-06-13 15:02:20.230022000		82	Internet IP[IPv4]	192.168.13.188	192.168.13.191	
✓	1	2622	2023-06-13 15:02:20.230022000		365	Internet IP[IPv4]	192.168.13.188	192.168.13.191	
✓	1	2623	2023-06-13 15:02:20.230127000		82	Internet IP[IPv4]	192.168.13.188	192.168.13.191	
✓	1	2624	2023-06-13 15:02:20.230232000		365	Internet IP[IPv4]	192.168.13.188	192.168.13.191	
✓	1	2625	2023-06-13 15:02:20.230336000		60	Internet IP[IPv4]	192.168.13.191	192.168.13.184	

003A Payload Protocol Identifier = x0000003C NGAP

==== NGAP Layer =====

```

NGAP-PDU = CHOICE
Extensibility Marker = 0
Choice Index = 0
InitiatingMessage = SEQUENCE
ProcedureCode = INTEGER
Contents = 15 id-InitialUEMessage
procedureCriticality = ENUMERATOR
Contents = 0 reject(0)
Value = Open Type
Length = 92
InitialUEMessage = SEQUENCE
Extensibility Marker = 0
ProtocolIE-Container = SEQUENCE OF
Iteration Count = 6
ProtocolIE-Container = Instance 0
ProtocolIE-Field = SEQUENCE
ProtocolIE-ID = INTEGER
Contents = 85 id-RAN-UE-NGAP-ID
procedureCriticality = ENUMERATOR
Contents = 0 reject(0)
Value = Open Type
Length = 2
RAN-UE-NGAP-ID = INTEGER
Length Determinant = 1
Contents = 2
ProtocolIE-Container = Instance 1
ProtocolIE-Field = SEQUENCE
ProtocolIE-ID = INTEGER
Contents = 38 id-NAS-PDU
procedureCriticality = ENUMERATOR
Contents = 0 reject(0)
Value = Open Type
Length = 44
NAS-PDU = OCTET STRING
Length Determinant = 43
NAS PDU Dump = x7E004171000D0100F1100000000003214062231001002E02C0E02F0201015200F110000001180100530101
ProtocolIE-Container = Instance 2
ProtocolIE-Field = SEQUENCE
ProtocolIE-ID = INTEGER
  
```

Capture Rate : 0.15 Mbps | C:\Program Files\GL Communications Inc\PacketScan\temp.h\Captured 47 036 frames | Missed Frames : 0

Call Graph – 5G N1N2

Packet Data Analyzer - Summary View

File View Call Summary Protocol Configurations GUI Configurations Help

5G N1N2 Interface Show All Calls

Call Summary Registraton Summary Alert Summary

Call #	StartTime	AmfUeNgapId	RrcEstablishmentCause	NrCellIdentity	Tac	AmfSetID	AmfRegionID
1	2023-07-03 15:13:10.834	2	mo-Signalling	1	1	1	2

Column Width Absolute Timing Show Latest

Time	Frame#	192.168.13.181	192.168.13.184	192.168.13.191	192.168.13.191
00.00.000	28968	38412	InitialUEMessage - Registration Request	38412	
00.00.743	29024		33231 POST /naus-auth/v1/ue-authentications	6668	
00.00.758	29029			6669	POST /nudm-ueau/v1/suci-0-001-01-000
00.00.778	29034			6669	200
00.00.803	29040		33231 201		
00.00.867	29050	38412	DownlinkNASTransport - Authentication R...		
00.00.870	29051	38412	UplinkNASTransport - Authentication Res	38412	
00.00.948	29061		33231 PUT /naus-auth/v1/ue-authentications/A	6668	
00.00.974	29067		33231 200		6668
00.00.985	29072			6669	POST /nudm-ueau/v1/msi-00101301204
00.00.989	29077			6669	201
00.01.053	29083	38412	DownlinkNASTransport - Security Mode C...	38412	
00.01.074	29087	38412	UplinkNASTransport - Security Mode Com	38412	
00.01.151	29092		33233 PUT /nudm-uecm/v1/msi-001013012042632/registrations/amf-3gpp-access		
00.01.178	29105		33233 201		
00.01.189	29109		33233 GET /nudm-sdm/v2/msi-001013012042632/nssai		
00.01.199	29112		33233 200		
00.01.218	29115		33233 GET /nudm-sdm/v2/msi-001013012042632?dataset-names=AM_SMF_SEL_SMS_SUB		
00.01.225	29118		33233 200		
00.01.358	29171		33233 POST /nudm-sdm/v2/msi-001013012042632/sdm-subscriptions		
00.01.372	29176		33233 201		
00.01.441	29184	38412	InitialContextSetupRequest - Registration ...	38412	

Find Complete Stack

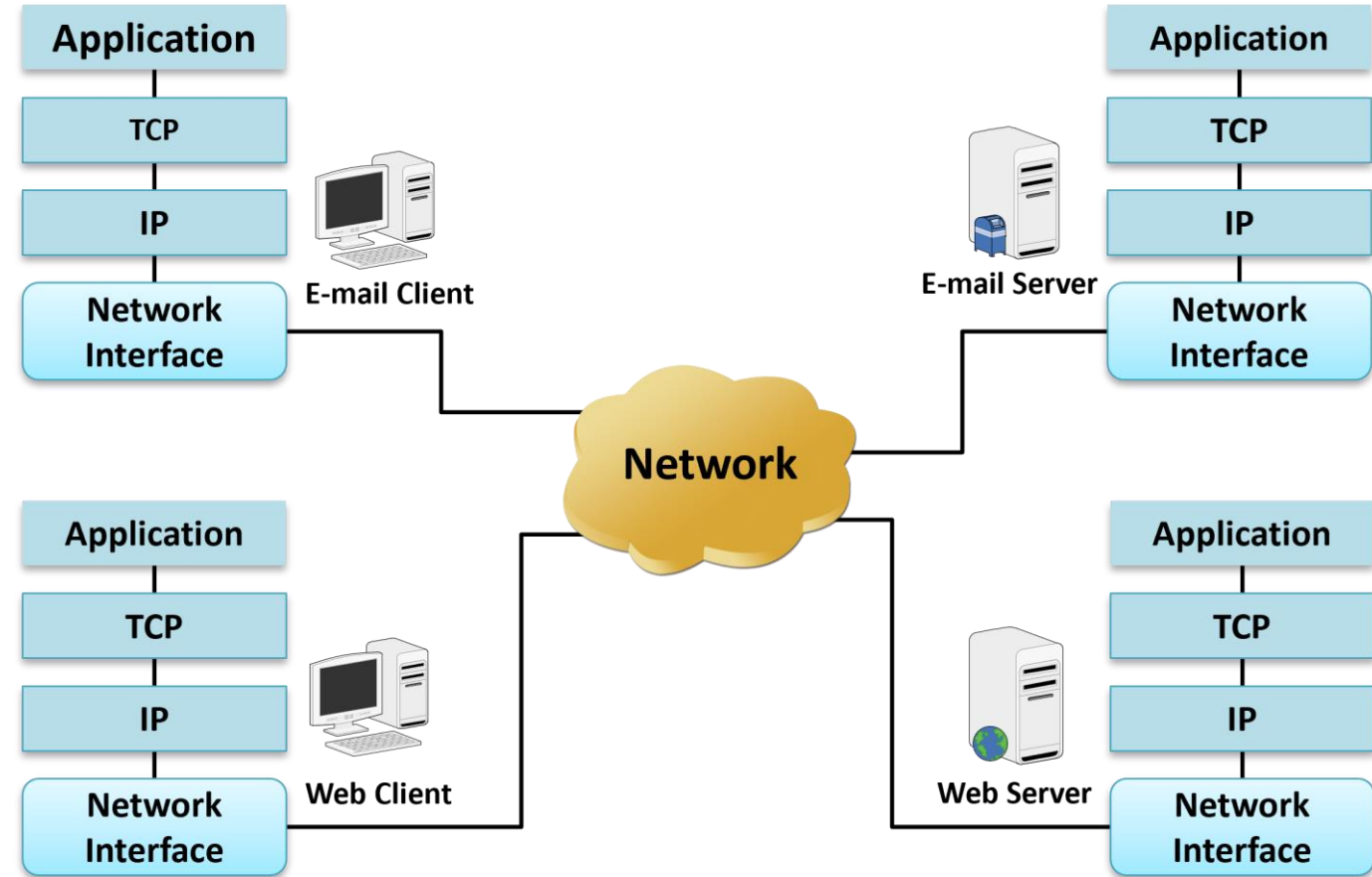
```

----- NGAP Layer -----
NGAP-PDU
Extensibility Marker
Choice Index
InitiatingMessage
ProcedureCode
Contents
procedureCriticality
Contents
Value
Length
InitialUEMessage
Extensibility Marker
ProtocolIE-Container
Iteration Count
ProtocolIE-Container
ProtocolIE-Field
ProtocolIE-ID
Contents
procedureCriticality
Contents
Value
Length
RAN-UE-NGAP-ID
Length Determinant
Contents
ProtocolIE-Container
ProtocolIE-Field
ProtocolIE-ID
Contents
procedureCriticality
Contents
Value
Length
NAS-PDU
Length Determinant
NAS PDU Dump
ProtocolIE-Container
ProtocolIE-Field
ProtocolIE-ID
Contents
procedureCriticality
Contents
Value
Length
UserLocationInformation
Choice Index
userLocationInformationNR
Extensibility Marker
    
```

Active Calls Graph Call Graph Call Summary

TCP Analytics Network

- Analyze TCP connections between internal company LAN connected computers and outside computers on the WAN
- Analyze TCP connections of a particular client server pair
- Analyze TCP connections on a subset of a LAN
- Display top level statistics
- Communicate with PacketScan™ to display packets that belong to a selected TCP connection
- Export information to CSV files for subsequent Excel or a database import
- Sort tabular information by column values



TCP Data Processing in PacketScan™ Application

PacketScan (IpProt) 64-bit [off-line]

File View Capture Statistics Database Call Detail Records Configure Help

0 GoTo

Device	Frame#	TIME (Date)	Length (Bytes)	Error	Destination Port UDP	FIN Finish Data Flag TCP	Protocol IP	RST Reset Connection Flag TCP	Sequence Number TCP	Source IP Address IP	Source Port TCP	Source Port UDP	SYN Synchron
✓ 1	144	2022-07-29 17:33:24.556410000	54			- more data from sender	TCP	- do not reset connection	2753544325	192.168.12.92	54791		- not set
✓ 1	145	2022-07-29 17:33:24.728730000	86										
✓ 1	146	2022-07-29 17:33:24.812591000	60										
✓ 1	147	2022-07-29 17:33:25.045551000	105			- more data from sender	TCP	- do not reset connection	2510704147	192.168.30.155	3389		- not set
✓ 1	148	2022-07-29 17:33:25.056367000								192.168.30.155		3389	
✓ 1	149	2022-07-29 17:33:25.056368000								192.168.30.155		3389	
✓ 1	150	2022-07-29 17:33:25.056552000								192.168.12.92		54511	
✓ 1	151	2022-07-29 17:33:25.058647000								192.168.30.155		3389	
✓ 1	152	2022-07-29 17:33:25.077041000								192.168.30.155		3389	
✓ 1	153	2022-07-29 17:33:25.077213000	54		3389		UDP			192.168.12.92		54511	
✓ 1	154	2022-07-29 17:33:25.094835000	54			- more data from sender	TCP	- do not reset connection	1890036032	192.168.12.92	57522		- not set
✓ 1	155	2022-07-29 17:33:25.095795000	60										
✓ 1	156	2022-07-29 17:33:25.141599000	137		3389		UDP			192.168.12.92		54511	
✓ 1	157	2022-07-29 17:33:25.186258000	60										
✓ 1	158	2022-07-29 17:33:25.479651000	105			- more data from sender	TCP	- do not reset connection	2131187858	192.168.30.146	3389		- not set
✓ 1	159	2022-07-29 17:33:25.508338000	105			- more data from sender	TCP	- do not reset connection	3823082860	192.168.30.104	3389		- not set
✓ 1	160	2022-07-29 17:33:25.521455000	60		54511		UDP			192.168.30.155		3389	
✓ 1	161	2022-07-29 17:33:25.526595000	54			- more data from sender	TCP	- do not reset connection	3047300261	192.168.12.92	54789		- not set
✓ 1	162	2022-07-29 17:33:25.557192000	54			- more data from sender	TCP	- do not reset connection	1417555879	192.168.12.92	56829		- not set
✓ 1	163	2022-07-29 17:33:25.723157000	86										
✓ 1	164	2022-07-29 17:33:25.868552000	126			- more data from sender	TCP	- do not reset connection	267330076	192.168.12.92	49292		- not set
✓ 1	165	2022-07-29 17:33:25.869198000	126			- more data from sender	TCP	- do not reset connection	544278709	192.168.1.3	445		- not set
✓ 1	166	2022-07-29 17:33:25.869293000	126			- more data from sender	TCP	- do not reset connection	267330148	192.168.12.92	49292		- not set
✓ 1	167	2022-07-29 17:33:25.869893000	126			- more data from sender	TCP	- do not reset connection	544278781	192.168.1.3	445		- not set
✓ 1	168	2022-07-29 17:33:25.870038000	54			- more data from sender	TCP	RST	267330220	192.168.12.92	49292		- not set
✓ 1	169	2022-07-29 17:33:26.056672000	60										

Processed 20 000 000

Progress indicator. Click cancel to stop the process.

Cancel

Device# Frame=144 at 2022-07-29 17:33:24.556410000 OK Len=54

Ethernet Frame Data

```

***** MAC Layer *****
0000 Destination Address      = xCOEAE484BA92
0006 Source Address          = x54BEF737BC79
000C Length/Protocol Type    = x0800 Internet IP(IPv4)
***** IP Layer *****
000E Version                  = 0100.... (4)
000E Internet Header Length (In 32 bit words) = ....0101 (5)
Differentiated Services Field =
000F Differentiated Services Codepoint = 000000.. Default
000F Explicit Congestion Notification = .....00 Not-ECT (Not ECN-Capable Transport)
IP Hdr No TCP SegmentationOffload =
0010 Total Length             = 40 (x0028)
0012 Identification          = 52172 (xCBCC)
0014 Reserved Bit            = 0..... Not Set
0014 Don't fragment          = .1..... Set
0014 More fragments          = ..0..... Not Set
0014 Fragment Offset         = 0 (.....00000000)
    
```

Off-line Viewing. E:\GL People\Sunil\TCP Analytics\Trace\20220801.hdl 24 704 523 Frames

PacketScan™ with ESP Deciphering Feature

- ESP deciphered packets as shown

The screenshot displays the PacketScan 64-bit application window. The top menu bar includes File, View, Capture, Statistics, Database, Call Detail Records, Configure, and Help. Below the menu is a toolbar with various icons and a 'GoTo' field. The main window is divided into two sections. The upper section is a table listing captured packets with columns for Device, Frame#, TIME (Relative), Length (Bytes), Error, Length/Protocol Type MAC, Packet Type MAC, Source IP Address IPv4, Destination IP Address IPv4, and Source Address IPv6. The lower section shows a detailed view of a packet, with the 'SIP Layer' section highlighted by a red box. The SIP layer details include headers (HDR) and body (BODY) information, such as 'INVITE sip:0001@192.168.12.45 SIP/2.0' and various parameters like 'Via', 'Max-Forwards', 'From', 'To', 'Call-ID', 'CSeq', 'Contact', 'Content-Type', and 'Content-Length'.

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IPv4	Destination IP Address IPv4	Source Address IPv6
✓ 1	0	00:00:00.000000000	769		Internet IP(IPv4)	SIP	192.168.12.86	192.168.12.45	
✓ 1	1	00:00:00.515721000	769		Internet IP(IPv4)	SIP	192.168.12.86	192.168.12.45	
✓ 1	2	00:00:01.537143000	769		Internet IP(IPv4)	SIP	192.168.12.86	192.168.12.45	
✓ 1	3	00:00:03.558945000	769		Internet IP(IPv4)	SIP	192.168.12.86	192.168.12.45	
✓ 1	4	00:00:04.626310000	764		Internet IP(IPv4)	SIP	192.168.12.90	192.168.12.45	

```
0018 Header Check Sum = x2403
001A Source IP Address = 192.168.12.86 (xC0A80C56)
001E Destination IP Address = 192.168.12.45 (xC0A80C2D)
===== UDP Layer =====
0022 Source Port = 5060 (x13C4)
0024 Destination Port = 5060 (x13C4)
0026 Length (Header + Data) = 735 (x02DF)
0028 Checksum = x16FB
===== SIP Layer =====
HDR
HDR = INVITE sip:0001@192.168.12.45 SIP/2.0
HDR = Via: SIP/2.0/UDP 192.168.12.86:5060;branch=z9hG4bK-29-103772070-10509-4472
HDR = Max-Forwards: 70
HDR = Allow: INVITE, BYE, CANCEL, ACK, INFO, OPTIONS, SUBSCRIBE, NOTIFY, REFER, REGISTER, UPDATE
HDR = From: 0001 <sip:0001@192.168.12.86>;tag=FromTag-26-103772070-10506-4472
HDR = To: 0001 <sip:0001@192.168.12.45>
HDR = Call-ID: GL-MAPS-28-103772070-10508-4472@192.168.12.86
HDR = CSeq: 1 INVITE
HDR = Contact: 0001 <sip:0001@192.168.12.86>
HDR = Content-Type: application/sdp
HDR = Content-Length: 238
BODY
BODY = v=0
BODY = o=0001 31062954 1 IN IP4 192.168.12.90
BODY = s=SIP Call
BODY = c=IN IP4 192.168.12.90
BODY = t=0 0
BODY = m=audio 1034 RTP/AVP 0 8 101
BODY = a=rtpmap:0 PCMU/8000
BODY = a=rtpmap:8 PCMA/8000
BODY = a=rtpmap:101 telephone-event/8000
BODY = a=fmtp:101 0-15
BODY = aptime:20
BODY = a=sendrecv
```

Comparison of Before and After Deciphering

PacketScan 64-bit

File View Capture Statistics Database Call Detail Records Configure Help

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IPv4	Destination IP Address IPv4	Source Address IPv6
✓	1	0	00:00:00.000000000		822	Internet IP(IPv4)	192.168.12.86	192.168.12.45	
✓	1	1	00:00:00.515721000		822	Internet IP(IPv4)	192.168.12.86	192.168.12.45	
✓	1	2	00:00:01.537143000		822	Internet IP(IPv4)	192.168.12.86	192.168.12.45	
✓	1	3	00:00:03.558945000		822	Internet IP(IPv4)	192.168.12.86	192.168.12.45	
✓	1	4	00:00:04.626310000		806	Internet IP(IPv4)	192.168.12.90	192.168.12.45	
✓	1	5	00:00:05.143077000		806	Internet IP(IPv4)	192.168.12.90	192.168.12.45	
✓	1	6	00:00:06.165570000		806	Internet IP(IPv4)	192.168.12.90	192.168.12.45	

Device1 Frame=0 at 00:00:00.000000000 OK Len=822

Ethernet Frame Data

```

***** MAC Layer *****
0000 Destination Address      = xE0D55EADFBFD
0006 Source Address          = xFCAA1492AB2F
000C Length/Protocol Type    = x0800 Internet IP(IPv4)
***** IPv4 Layer *****
000E Version                  = 0100... (4)
000E Internet Header Length (In 32 bit words) = ...0101 (5)
000F Differentiated Services Field = 000000... Default
000F Explicit Congestion Notification = .....00 Not-ECT (Not ECN-Capable Transport)
IP Hdr No TCP SegmentationOffload =
0010 Total Length             = 808 (x0328)
0012 Identification           = 31181 (x79CD)
0014 Reserved Bit             = 0..... Not Set
0014 Don't fragment           = 0..... Not Set
0014 More fragments           = 0..... Not Set
0014 Fragment Offset          = 0 (...00000 00000000)
0016 Time To Live             = 128 (x80)
0017 Protocol                  = 00110010 Encap Security Payload
0018 Header Check Sum         = x2403
001A Source IP Address        = 192.168.12.86 (xC0A80C56)
001E Destination IP Address   = 192.168.12.45 (xC0A80C2D)
***** Encapsulating Security Payload Protocol Layer *****
0022 Security Parameter Index = 97709536 (x05D2EDE0)
0026 Sequence Number         = 1 (x00000001)
ESP Payload Data              = x49F74319A723AF44...BFA3074B9C6D5534 (Len=
  
```

*** Right click to SHOW/HIDE layer details or copy ***

Before Deciphering

PacketScan 64-bit

File View Capture Statistics Database Call Detail Records Configure Help

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IPv4	Destination IP Address IPv4	Source Address IPv6
✓	1	0	00:00:00.000000000		763	Internet IP(IPv4)	192.168.12.86	192.168.12.45	
✓	1	1	00:00:00.515721000		769	Internet IP(IPv4)	192.168.12.86	192.168.12.45	
✓	1	2	00:00:01.537143000		769	Internet IP(IPv4)	192.168.12.86	192.168.12.45	
✓	1	3	00:00:03.558945000		769	Internet IP(IPv4)	192.168.12.86	192.168.12.45	
✓	1	4	00:00:04.626310000		764	Internet IP(IPv4)	192.168.12.90	192.168.12.45	

```

0018 Header Check Sum         = x2403
001A Source IP Address        = 192.168.12.86 (xC0A80C56)
001E Destination IP Address   = 192.168.12.45 (xC0A80C2D)
***** UDP Layer *****
0022 Source Port              = 5060 (x13C4)
0024 Destination Port        = 5060 (x13C4)
0026 Length (Header + Data)   = 735 (x02DF)
0028 Checksum                  = x16FB
***** SIP Layer *****
HDR
HDR = INVITE sip:0001@192.168.12.45 SIP/2.0
HDR = Via: SIP/2.0/UDP 192.168.12.86:5060;branch=z9hG4bK-29-103772070-10509-4472
HDR = Max-Forwards: 70
HDR = Allow: INVITE, BYE, CANCEL, ACK, INFO, OPTIONS, SUBSCRIBE, NOTIFY, REFER, REGISTER, UPDATE
HDR = From: 0001 <sip:0001@192.168.12.86>;tag=FromTag-26-103772070-10506-4472
HDR = To: 0001 <sip:0001@192.168.12.45>
HDR = Call-ID: GL-MAPS-28-103772070-10508-4472@192.168.12.86
HDR = CSeq: 1 INVITE
HDR = Contact: 0001 <sip:0001@192.168.12.86>
HDR = Content-Type: application/sdp
HDR = Content-Length: 238
HDR =
BODY
BODY = v=0
BODY = o=0001 31062954 1 IN IP4 192.168.12.90
BODY = s=SIP Call
BODY = c=IN IP4 192.168.12.90
BODY = t=0 0
BODY = m=audio 1034 RTP/AVP 0 8 101
BODY = a=rtptime:0 PCMU/8000
BODY = a=rtptime:8 PCMA/8000
BODY = a=rtptime:101 telephone-event/8000
BODY = a=fmtp:101 0-15
BODY = a=ptime:20
BODY = a=sendrecv
  
```

Off-line Viewing. [C:\Users\Suni\Desktop\FastRecorderAndPacketExtractor_56 Frames]

After Deciphering

Analysis of eCPRI Decodes in Offline PacketScan™ HD

Over UDP

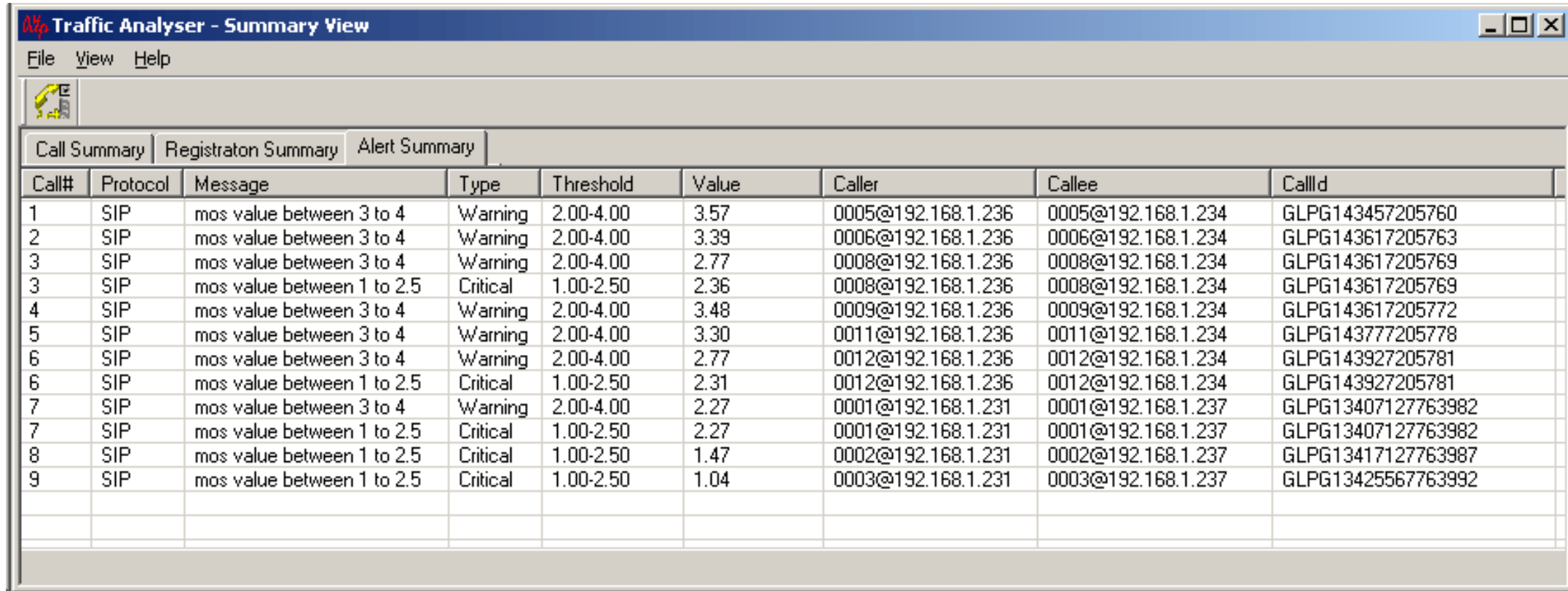
```
Device0 Frame=6 at 2022-06-09 06:07:36.711206000 OK Len=112 *** Right d
Ethernet Frame Data
----- MAC Layer -----
0000 Destination Address      = xFCAA149225C4
0006 Source Address          = x54BEF737CB9A
000C Length/Protocol Type    = x86DD IPv6
----- IPv6 Layer -----
000E Protocol Version        = 0110.... (6)
000E Traffic Class           = 0 (...0000 0000....)
000F Flow Label              = 834513 (...1100 10111011 11010001)
0012 Payload Length          = 58 (x003A)
0014 Next Header              = 00010001 User Datagram Protocol (UDP)
0015 Hop Limit                = 64 (x40)
0016 Source Address           = fe80::64f2:5e84:f1db:502
0026 Destination Address     = fe80::589e:b2d5:9074:2bec
----- UDP Layer -----
0036 Source Port              = 64000 (xFA00)
0038 Destination Port        = 64000 (xFA00)
003A Length (Header + Data)   = 58 (x003A)
003C Checksum                 = x7F76
----- eCPRI Layer -----
003E C                         = .....0 eCPRI message is the last one inside the eCPRI PDU
003E eCPRI Protocol Revision  = 0001.... (1)
003F eCPRI Message Type       = 00000100 Remote Memory Access
0040 eCPRI Payload Size       = 28 (x001C)
0042 Remote Memory Access ID  = 17 (x11)
0043 Req/Resp                  = ....0010 Failure
0043 Read/Write                = 0010.... Write_No_Resp
0044 Element ID               = 8755 (x2233)
0046 Address                   = x050403020100
004C Length                    = 16 (x0010)
    User Data                   = xFFEEDDCCBBAA99887766554433221100
```

Analysis of eCPRI Decodes in Offline PacketScan™ HD (Contd.)

Over MAC

```
Device0 Frame=0 at 2019-02-13 11:36:46.000000000 OK Len=64 *** Right
Ethernet Frame Data
===== MAC Layer =====
0000 Destination Address = x008016000000
0006 Source Address = x008016884EFF
000C Length/Protocol Type = xAEFE eCPRI
===== eCPRI Layer =====
000E C = .....0 eCPRI message is the last one inside the eCPRI PDU
000E eCPRI Protocol Revision = 0001.... (1)
000F eCPRI Message Type = 00000000 IQ Data
0010 eCPRI Payload Size = 20 (x0014)
eCPRI Payload = x123487650F0E0D0C0B0A09080706050403020100
===== O-RAN Fronthaul CUS Layer =====
ecpriPcid =
0012 BandSector_ID = ..010010 (18)
0012 DU_Port_ID = 00..... (0)
0013 RU_Port_ID = ....0100 (4)
0013 CC_ID = 0011.... (3)
ecpriSeqid =
0014 Sequence ID = 135 (x87)
0015 Subsequence ID = .1100101 (101)
0015 E bit = 0..... More fragments follow
0016 FilterIndex = ....1111 Reserved
0016 payloadVersion = .000.... (0)
0016 dataDirection = 0..... Uplink
0017 frameId = 14 (x0E)
0018 subframeId = 0000.... (0)
0018 slotId = 52 (....1101 00.....)
0019 startSymbolId = ..001100 (12)
001A sectionId = 176 (00001011 0000....)
001B symInc = ....0.. use the current symbol number
001B rb = ....1... every other RB used
001B startPrbu = 521 (.....10 00001001)
001D numPrbu = 8 (x08)
udCompHdr =
001E udCompMeth = ....0111 Reserved
001E udIqWidth = 0000.... I and Q are each 16 bit wide
Dump = x050403020100
```


PDA - Alert Summary



The screenshot shows a software window titled "Traffic Analyser - Summary View". It has a menu bar with "File", "View", and "Help". Below the menu bar is a toolbar with a small icon. The main area contains a tabbed interface with three tabs: "Call Summary", "Registraton Summary", and "Alert Summary". The "Alert Summary" tab is active, displaying a table with the following columns: Call#, Protocol, Message, Type, Threshold, Value, Caller, Callee, and CallId. The table contains 9 rows of alert data.

Call#	Protocol	Message	Type	Threshold	Value	Caller	Callee	CallId
1	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.57	0005@192.168.1.236	0005@192.168.1.234	GLPG143457205760
2	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.39	0006@192.168.1.236	0006@192.168.1.234	GLPG143617205763
3	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.77	0008@192.168.1.236	0008@192.168.1.234	GLPG143617205769
3	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.36	0008@192.168.1.236	0008@192.168.1.234	GLPG143617205769
4	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.48	0009@192.168.1.236	0009@192.168.1.234	GLPG143617205772
5	SIP	mos value between 3 to 4	Warning	2.00-4.00	3.30	0011@192.168.1.236	0011@192.168.1.234	GLPG143777205778
6	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.77	0012@192.168.1.236	0012@192.168.1.234	GLPG143927205781
6	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.31	0012@192.168.1.236	0012@192.168.1.234	GLPG143927205781
7	SIP	mos value between 3 to 4	Warning	2.00-4.00	2.27	0001@192.168.1.231	0001@192.168.1.237	GLPG13407127763982
7	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	2.27	0001@192.168.1.231	0001@192.168.1.237	GLPG13407127763982
8	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	1.47	0002@192.168.1.231	0002@192.168.1.237	GLPG13417127763987
9	SIP	mos value between 1 to 2.5	Critical	1.00-2.50	1.04	0003@192.168.1.231	0003@192.168.1.237	GLPG13425567763992

- Generates alerts when vital parameters go beyond a specified value
- Provides an active list of the alerts for the events in a tabular column
- Displays the summary of call#, user-defined message, threshold value, actual value for which the alert occurred, callee, caller, and callid

Registration Summary

The screenshot displays the 'Packet Data Analyzer - Summary View' interface. At the top, there is a menu bar with 'File', 'View', 'Call Summary', and 'Help'. Below the menu is a toolbar with icons for various functions and a dropdown menu set to 'Show All Registrations' with a 'Total : 15' indicator. The main area is divided into three tabs: 'Call Summary', 'SIP Registration Summary', and 'Alert Summary'. The 'SIP Registration Summary' tab is active, showing a table of registration events.

Call #	Method	Register Request Ti...	User Agent	Registrar	Result	Status	ErrorCode	Call ID	Registered Time
0	Register	2023-11-15 11:18:1...	0001@192.168.12.112	192.168.12.112	Passed	Registered	0	GL-MAPS-16-33884...	2023-11-15 11:18:1...
1	DeRegister	2023-11-15 11:18:2...	0001@192.168.12.112	192.168.12.112	Passed	De-Registered	0	GL-MAPS-16-33884...	
2	Register	2023-11-15 11:19:1...	0001@192.168.12.112	192.168.12.112	Failed	Failed	404	GL-MAPS-23-33937...	
3	Register	2023-11-15 11:19:2...	0001@192.168.12.112	192.168.12.112	Failed	Failed	403	GL-MAPS-28-33949...	
4	Register	2023-11-15 11:19:4...	0001@192.168.12.112	192.168.12.112	Failed	Failed	423	GL-MAPS-33-33971...	
5	Register	2023-11-15 11:20:0...	0001@192.168.12.112	192.168.12.112	Failed	Failed	480	GL-MAPS-38-33995...	
6	Register	2023-11-15 11:20:2...	0001@192.168.12.112	192.168.12.112	Failed	Failed	482	GL-MAPS-43-34015...	
7	Register	2023-11-15 11:20:5...	0001@192.168.12.112	192.168.12.112	Failed	Failed	400	GL-MAPS-48-34043...	

Below the table, there is a 'Registration Type' dropdown set to 'Registration', an 'Export' button, a 'Graph Duration' dropdown set to '7 days', and a date/time selector set to '2023-11-15 11:18:18'. There are also 'Goto', 'Save', and 'Update Graph' buttons. A graph titled 'Registration Per Second' is displayed, showing a bar chart of registration activity over time. The y-axis is labeled 'Registration/Sec' and ranges from 0 to 10. The x-axis is labeled 'Time' and shows intervals from 15-11:18:00 to 15-11:25:00. The graph shows several small bars representing individual registration attempts, with a legend indicating 'Attempted' (blue), 'Successful' (green), and 'Unsuccessful' (red). Below the graph, there are tabs for 'Registration Graph' and 'Registration Trace'. To the right of the graph is a 'Registration Statistics' table.

Registration Statistics	Count
Total Registrations	15
Active Registrations	0
Completed Registrations	5
Failed Registrations	10
Timed Out Registrations	0
InProgress Registrations	0
Registration Sessions	13
De-Registration Sessions	2
Registration Messages	13
De-Registration Messa...	2
Failed Registration Cat...	
Client Failures	
403 Forbidden	1
404 Not Found	1
423 Interval Too Brief	1
480 Temporarily Un...	1
482 Loop Detected	1
4xx Other Client Failure	1
Server Failures	
500 Server Internal ...	1
5xx Other Server Fail...	1
Global Failures	
603 Decline	1
6xx Other Global Fail...	1

- Displays the SIP registration information in a tabular format which includes user agent, registrar, registered time, status, and so on for each user agent
- Displays the active registration graph of the entire registration summary
- Provides the trace display of each registration

Registration Trace

Traffic Analyzer - Summary View

File View Help

Show All Registrations

Call Summary Registraton Summary Alert Summary

Call #	User Agent	Registrar	Status	Registered Time	TTL (secs)	Expiry Time	Remaining Time	RRD (msecs)	Registration...
0	0001@192.168.1.115	192.168.1.190	Registered	2011-01-03 18:31:09	120	2011-01-03 18:33:09		0	1
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		246162	2
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		0	1
3	0001@192.168.1.115	192.168.1.190	Registered	2011-01-03 18:33:59	120	2011-01-03 18:35:59		1	1

192.168.1.115 192.168.1.190

54098 REGISTER 5060

5060 SIP/2.0 407 Proxy Authentication Required 54098

54098 REGISTER 5060

5060 SIP/2.0 200 OK 54098

```
REGISTER sip:192.168.1.190 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.115:5060;branch=z9hG4bK3372630384-4779
Max-Forwards: 70
Allow: INVITE,BYE,CANCEL,ACK,INFO,PRACK,COMET,OPTIONS,SUBSCRIBE,NOTI
From: 0001 <sip:0001@192.168.1.115>;tag=GLPG_3372630384-4780
To: sip:0001@192.168.1.115
Call-ID: GLPG-9223369124778
CSeq: 1 REGISTER
Expires: 120
Contact: 0001 <sip:0001@192.168.1.115>
Content-Length: 0
```

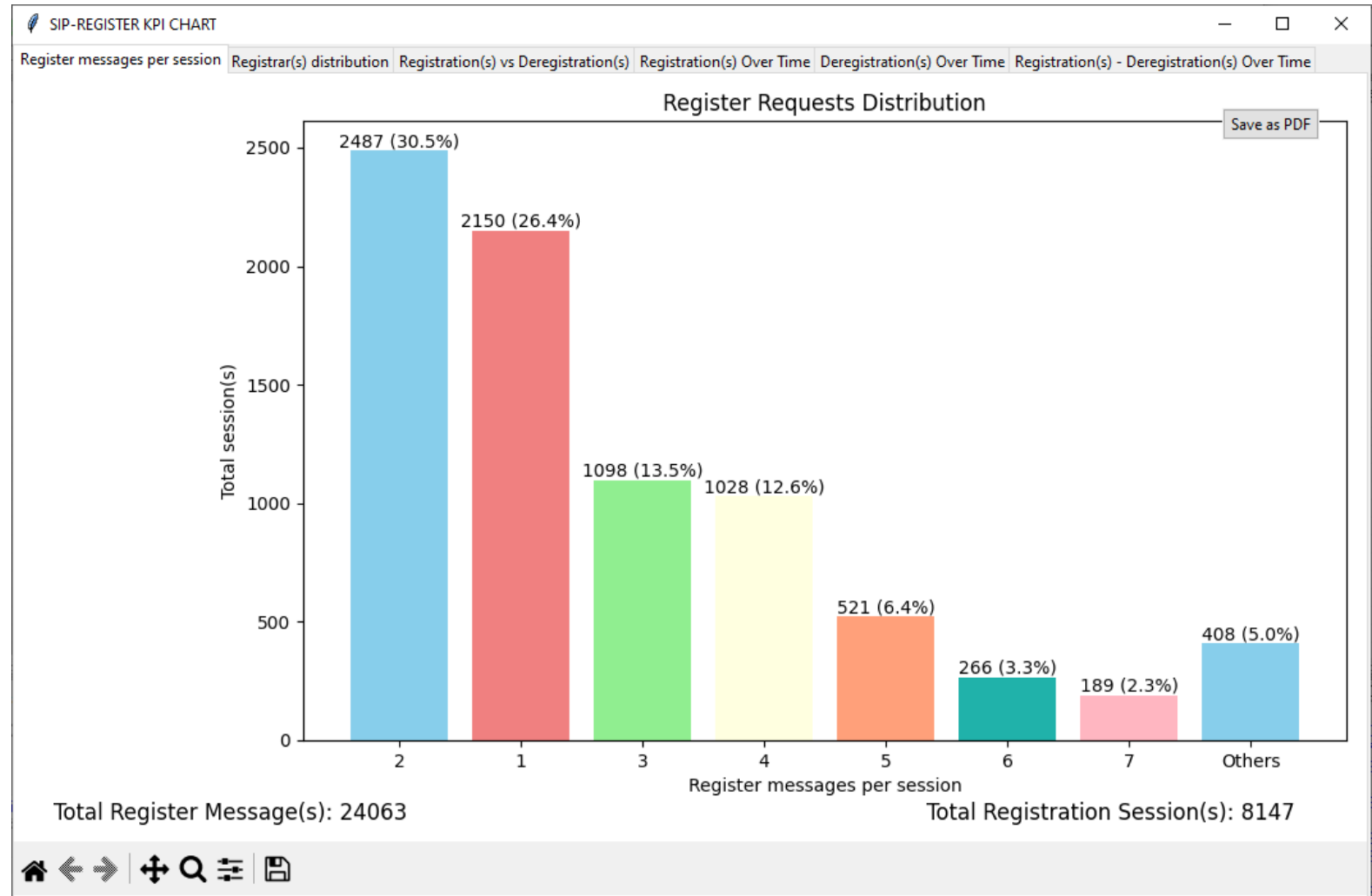
Active Registration Graph Registration Trace

- 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

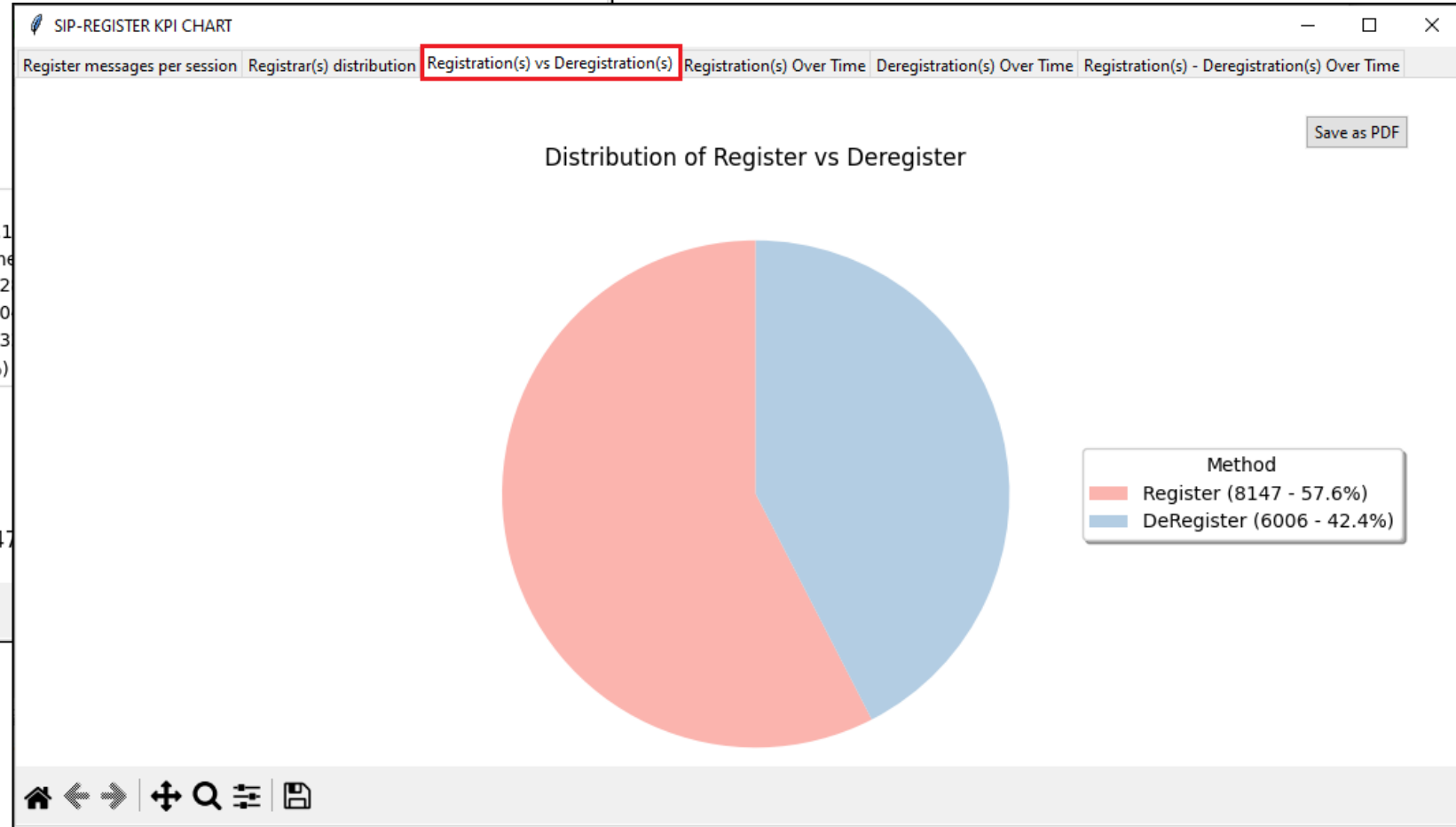
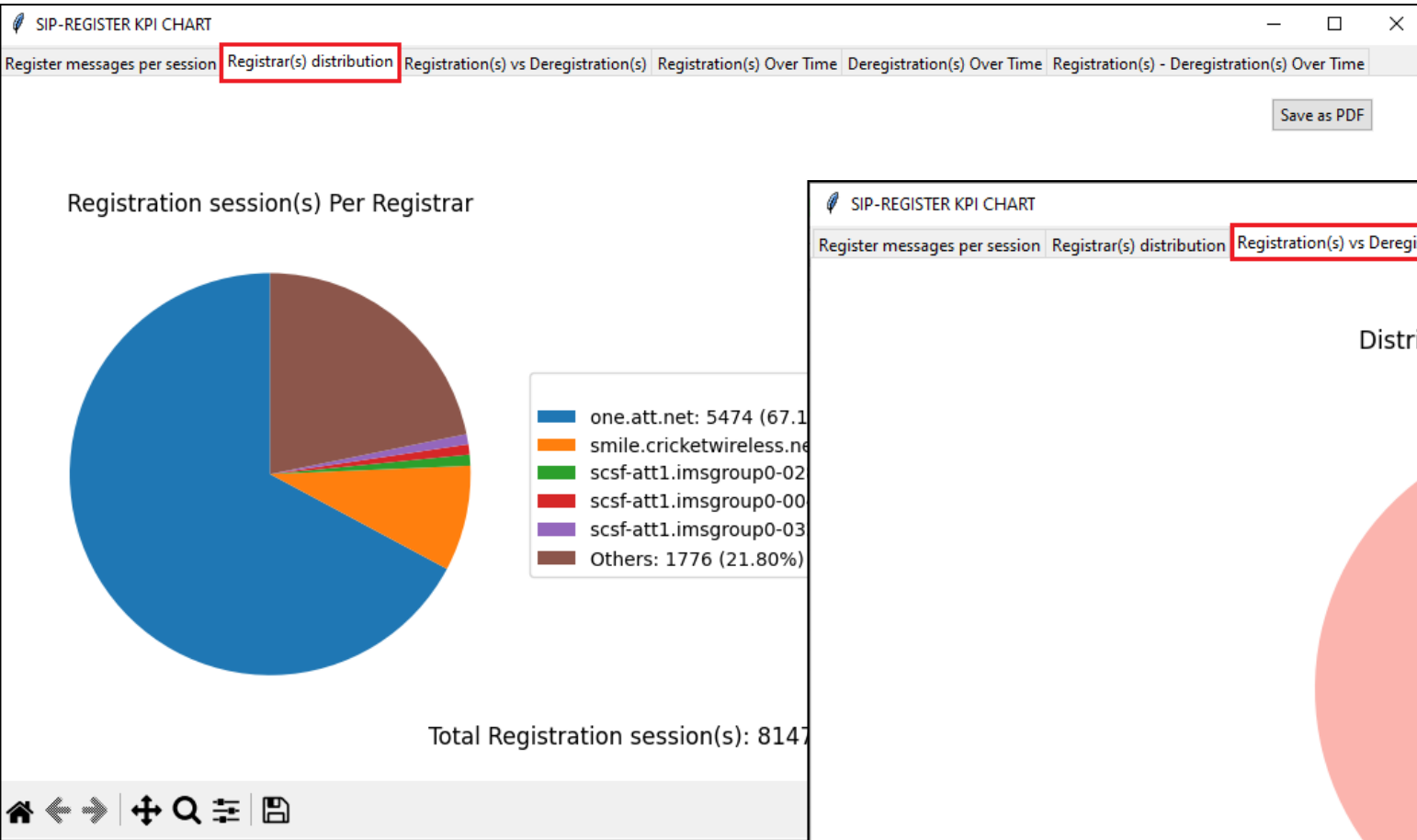
KPI Report (Registration)

The SIP Registration Summary KPI Report includes KPIs for the following:

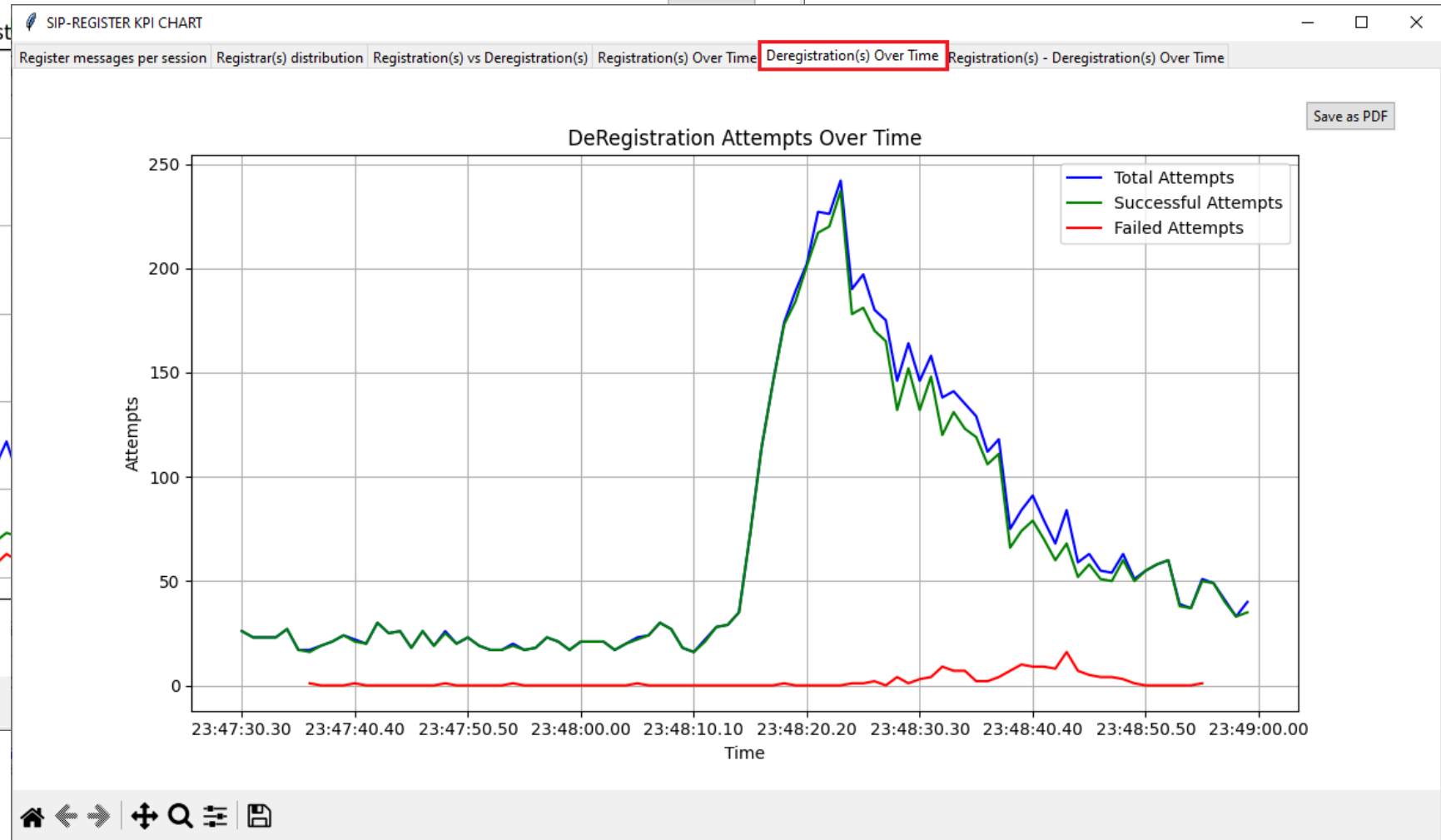
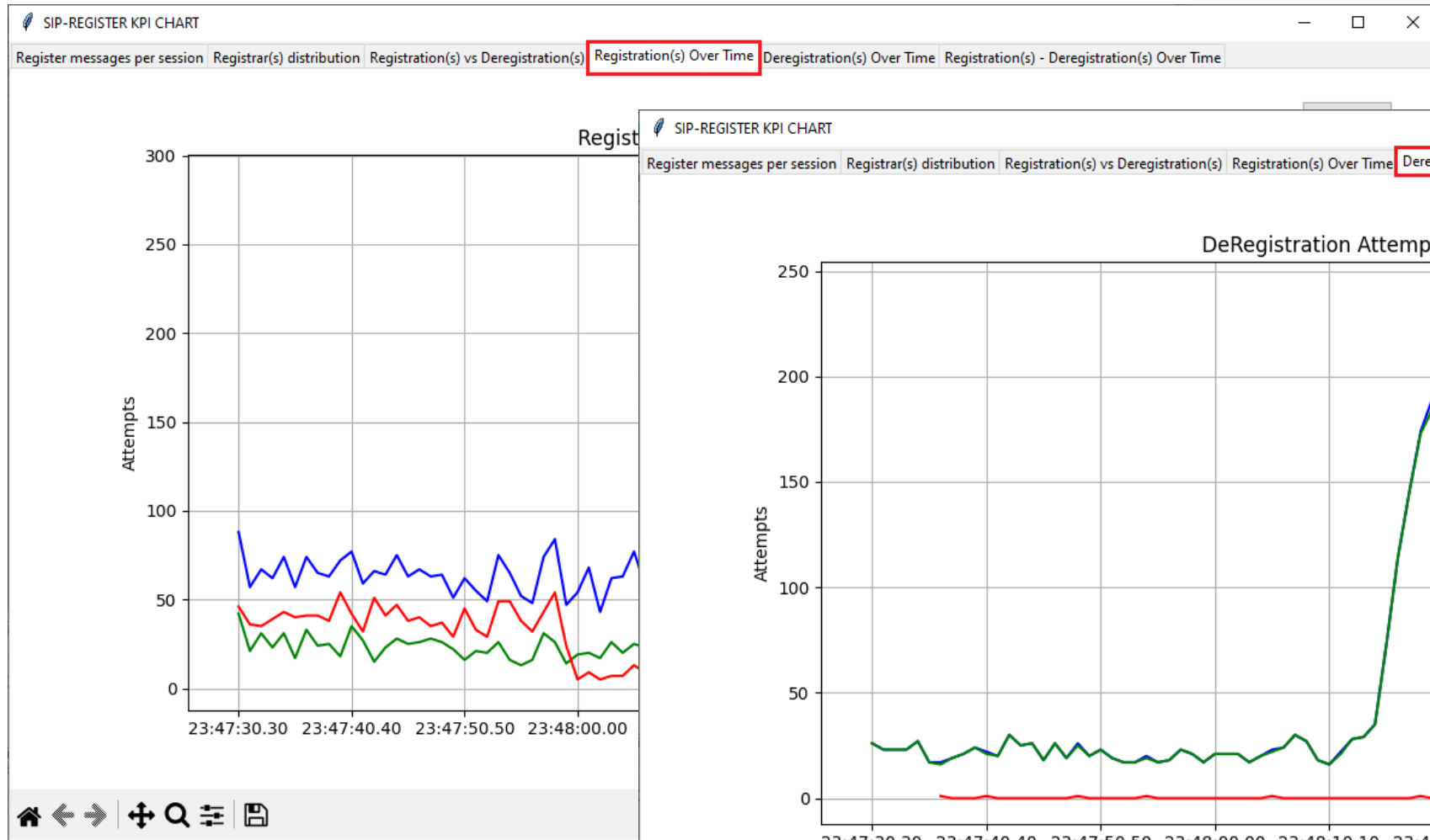
- **Register Messages per Session:** Shows a graph for the distribution of Register Requests
- **Registrar(s) Distribution:** Displays a graph for the number of Registration sessions per Registrar
- **Registration(s) vs Deregistration(s):** Illustrates a graph comparing the distribution of Register and Deregister counts with percentages (%)
- **Registration(s) Over Time:** Show the graphs for "Successful," "Failed," and "Total Attempts" per second
- **Deregistration(s) Over Time:** Displays a graph for "Successful" and "Total Attempts" per second
- **Registration(s) - Deregistration(s) Over Time:** Shows a graph for overall "Register & Deregister attempts," "Register & Deregister passed," and "Register & Deregister failed" attempts per second



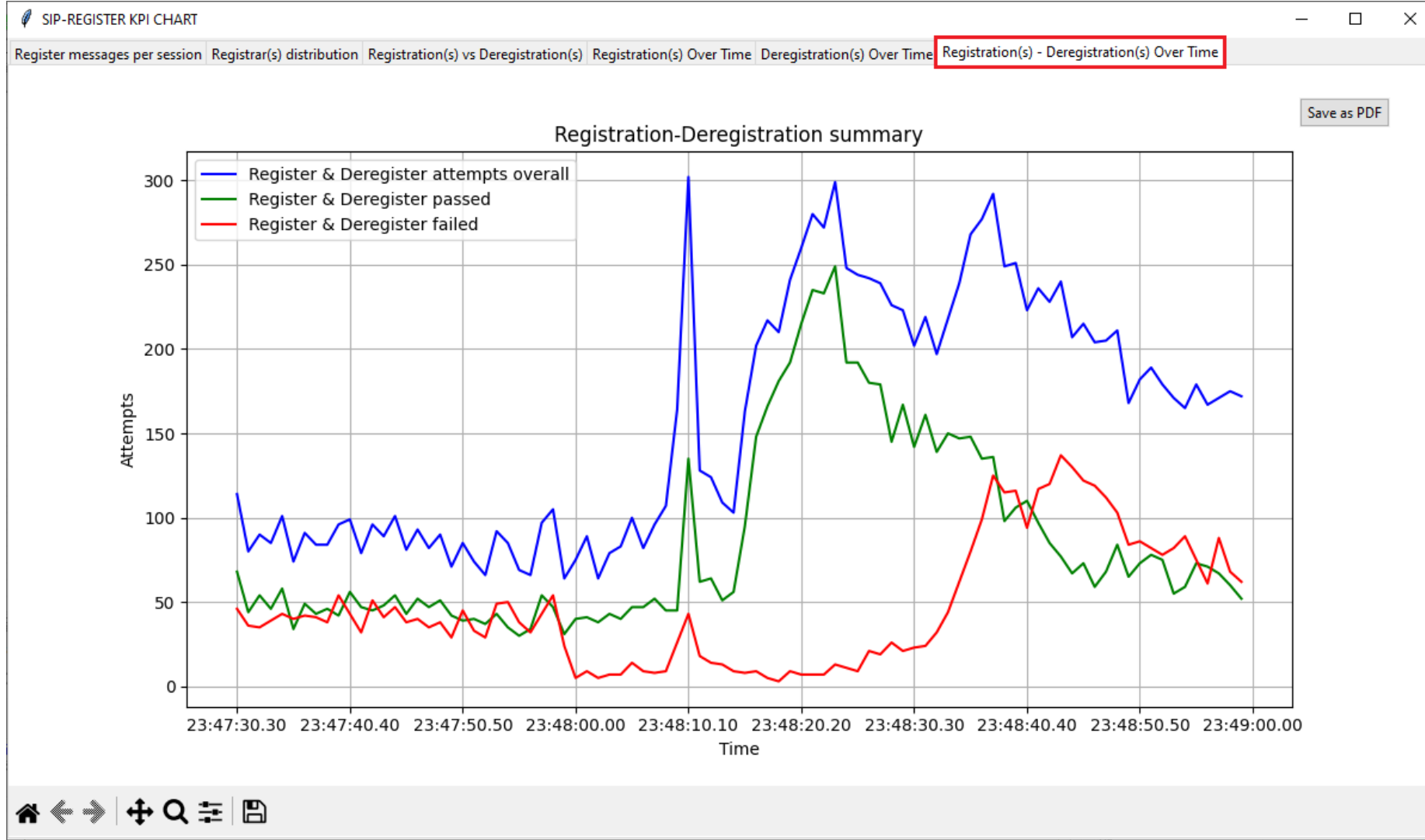
Registrar(s) Distribution, Registration vs Deregistration KPIs



Registration(s) over Time, Deregistration over Time KPIs



Registration(s)-Deregistration(s) over Time KPI



Thank you