

---

---

# PacketScan Web™

## All-IP Signaling and Traffic Analysis

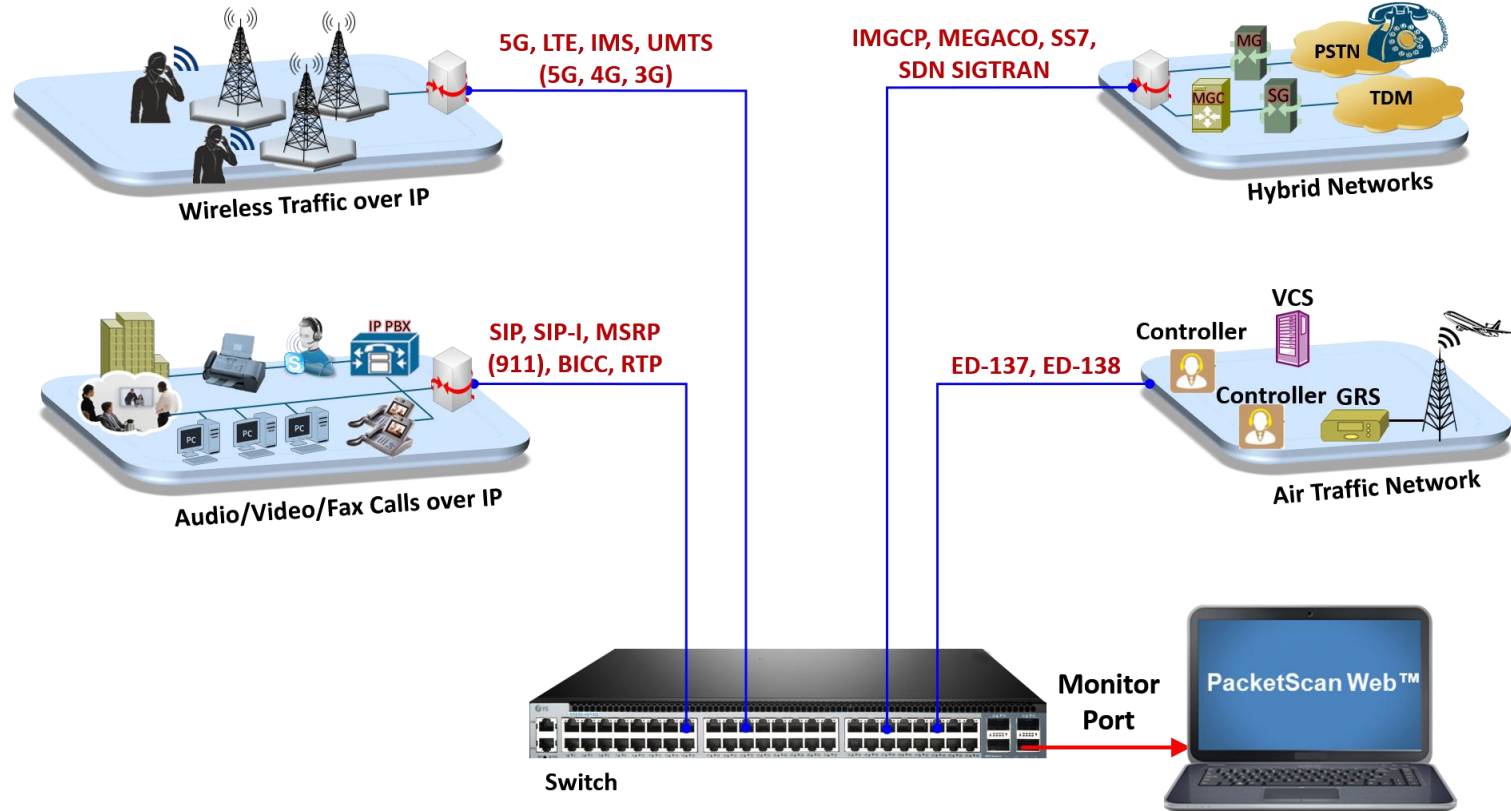
---

---



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

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



# Overview

- **Extends PacketScan capabilities** beyond a single desktop to enterprise-wide environments
- **Intuitive web-based interface** for simplified access, monitoring, and management
- **Supports Linux-based server deployments** for high-performance, scalable operation
- **Enables secure multi-user collaboration**, allowing concurrent access and analysis
- **Offers open REST APIs** for automated capture, analysis, and integration with third-party tools

# What's New in PacketScan Web™

- **PacketScan™ on Linux**
  - Deploy PacketScan™ directly on Linux servers where your workloads reside
  - Supports both real-time and offline (PCAP/NG) capture and analysis
  - Runs in headless mode — lightweight, efficient, and ideal for server environments
  - Offers the same decode and analysis capabilities as the standalone Windows version
- **Network-Wide Analysis from a Single Web UI**
  - Centrally manage and monitor multiple probes from one intuitive dashboard
  - Add and register probes across labs and remote locations
  - Start/stop captures, configure ring buffers, and apply filters across all probes
  - Call Summary– Call Success Rate, Setup Time, RTP Loss, Jitter, MOS, and Errors
  - Merge and correlate traces from multiple capture points for complete visibility

# What's New in PacketScan Web™ (Contd.)

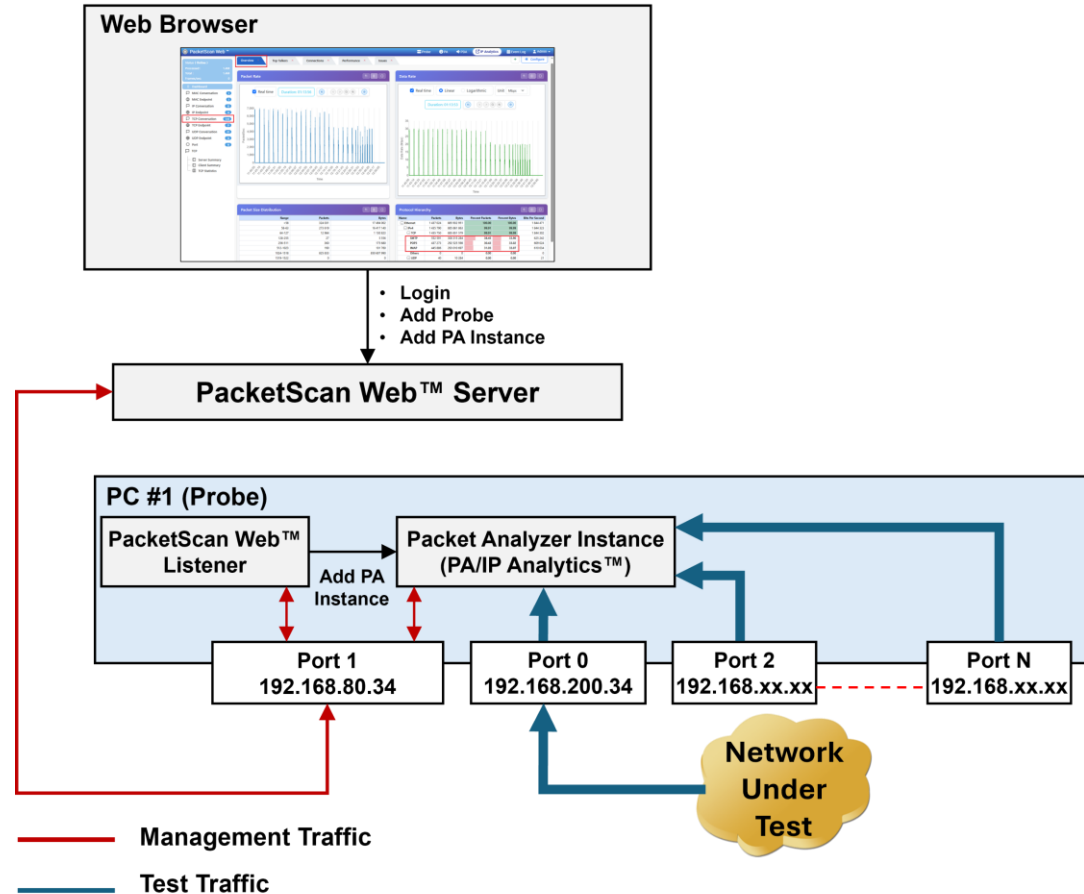
- **REST APIs for Automation**
- Integrate PacketScan Web™ seamlessly into your automation or CI/CD workflows
- Key API Endpoints:
  - **/probes** – Manage and monitor probe status
  - **/capture** – Control capture sessions and buffer size
  - **/filters** – Upload or apply custom filter templates
  - **/kpis** – Retrieve real-time performance metrics
  - **/pcaps** – Export specific PCAP slices for analysis
- **Enhanced Capture Filters**
  - Choose from built-in protocol filters or define custom expressions
  - Apply filters pre-capture or post-capture for flexible control
  - Supports IP groups, subnets, and range-based filtering
  - Save and reuse filters across sessions or probes for consistent workflows

# Key Features

- Browser-based packet capture, protocol analysis, Packet Data Analysis (PDA), and IP Analytics™
- Supports both Windows® and Linux® deployments
- Centralized Web UI for managing multiple PacketScan™ Probes
- Multi-user client-server architecture for distributed monitoring
- Real-time and offline analysis of HDL, PCAP, and PCAPNG trace files
- Advanced filtering, search, and pre-capture traffic filtering
- Integrated Packet Data Analysis (PDA) with call flows, CDRs, and ladder diagrams
- Built-in IP Analytics™ for endpoint, conversation, and TCP/UDP performance analysis
- Rich dashboards with call Summary and traffic statistics
- Merge and correlate traces from multiple capture points for end-to-end visibility
- Download trace, configuration, and log files from remote PacketScan Web™ Probes for offline analysis and archival
- REST API support for automation and third-party integration
- Comprehensive support for 5G, LTE, IMS, VoIP, SIGTRAN, GSM, UMTS, Diameter, RTP, and other IP protocols

# PacketScan Web™ Architecture

- **PacketScan Web™** uses a centralized control and distributed capture architecture
- **PacketScan Web™ server** acts as the central management and orchestration component of the system
- **PacketScan Web™ probes** are distributed PCs on which traffic capture happen
- **PacketScan Web™ Listener** is a lightweight application that creates Packet Analyzer instances on command from PacketScan Web™ Server
- **Packet Analyzer** performs high-performance Ethernet traffic capture, analysis (including IP Analytics™) on a single or multiple ports



# Packet Analyzer (PA)

- Analyzer opens with Summary, Detail and Hex Dump as default panes

The screenshot displays the PacketScan Web interface. At the top, there is a navigation bar with 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin' buttons. Below this is a toolbar with various icons and a search bar. The main area is divided into three panes:

- Summary View:** A table listing captured packets. The table has columns for 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, and Destination Address\_IPv6. The table shows 17 packets, all from device 3, with various lengths and protocols (Internet IP(IPv4) and SIP).
- Detailed View:** A pane showing the structure of the selected packet (Frame#0). It lists fields such as Ethernet Frame Data, MAC Layer, Destination Address, Source Address, Length/Protocol Type, IP Version, Internet Header Length, Differentiated Services Field, Differentiated Services Codepoint, Explicit Congestion Notification, IP Hdr No TCP SegmentationOffload, Total Length, Identification, Reserved Bit, Don't fragment, More fragments, Fragment Offset, Time To Live, and Protocol. Each field is followed by its value and a brief description.
- Hex Dump View:** A pane showing the raw hexadecimal data of the selected packet. It includes a hex dump of the frame data and a corresponding ASCII dump. The hex dump shows the raw bytes of the packet, and the ASCII dump shows the human-readable text extracted from the packet.

Red arrows point from the text labels to the corresponding panes in the interface.

# Define Summary Columns

- The **Define Summary Columns** window allows users to customize the Packet Analyzer summary view by selecting protocol fields
- Click a protocol in the protocol hierarchy and expand it to view all fields associated with the selected protocol
- The **Search Protocol** option allows users to quickly locate specific protocols and fields within the hierarchy
- Select the required protocol fields and click **Define** to add them to the summary configuration

The screenshot shows the PacketScan Web interface. The top navigation bar includes 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin'. Below the navigation bar, there are buttons for 'Save', 'Load', and 'Default'. The main content area is titled 'Define Summary Columns'. On the left side, there is a sidebar with several options: 'Select Summary Columns', 'Time Display Format', 'Define Summary Columns' (highlighted in blue), 'Define Alias Columns', 'View Filter', 'Search Filter', 'Capture Options', 'Capture Filter', and 'Config File Editor'. The main area contains a search bar for protocols, a list of protocols (INAP, IP Mobility, IPA, IPv4), and a search bar for protocol fields. The 'IPv4' protocol is expanded, and its fields are listed. The 'Destination IP Address' and 'Source IP Address' fields are checked, and their respective checkboxes are highlighted with red boxes. A 'Define' button is located at the top right of the main area.

# Select Summary Columns

- Navigate to **Select Summary Columns** to display and reorder summary fields
- Move the required fields from **Hidden Columns** to **Selected Columns**
- Click **Select All** to add all fields, or drag and drop individual fields as needed
- Click **Apply** to save the column configuration
- A confirmation message appears indicating the configuration has been saved successfully
- Click **OK** to continue

PacketScan Web™

Probe PA PDA IP Analytics Event Log Admin

Save Load Default

### Select Summary Columns

Select Summary Columns To Display

**Selection Methods:** Single click selects a single item, Ctrl + Click enables multiple selections, and Shift + Click selects a range of items between the last selected and the current click.  
**Rearrangement Methods:** Drag and drop allows reordering items within a list and moving items between the list boxes.

**Selected Columns**

- Time
- Length (Bytes)
- Error
- Length/Protocol Type\_MAC
- Packet Type\_MAC
- Source Port\_UDP
- Destination Port\_UDP
- Source Port\_TCP
- SSRC identifier\_RTP
- Destination Port\_TCP
- Marker bit\_RTP
- SIP Method\_SIP

**Hidden Columns**

- Source IP Address\_IPv4
- Destination IP Address\_IPv4
- Source Address\_IPv6
- Destination Address\_IPv6

Sel Only Select All Restore Apply

# Summary View

- The selected fields are now displayed in the **Summary View**

PacketScan Web™

Probe PA PDA IP Analytics Event Log Admin

Enter Frame Probe Probe 1 PA Instance Test 1

Device	Frame#	Source IP Address_IPv4	Destination IP Address_IPv4	Source Address_IPv6	Destination Address_IPv6	TIME (Date)	Length (Bytes)	Error	Length/Protocol Type_MAC
0	0					2023-04-05 08:54:43.014648000	60		ARP
0	1					2023-04-05 08:54:43.822787000	60		ARP
0	2					2023-04-05 08:54:44.325731000	60		ARP
0	3					2023-04-05 08:54:44.812477000	60		ARP
0	4					2023-04-05 08:54:45.816035000	60		ARP
0	5					2023-04-05 08:54:47.176194000	60		ARP
0	6					2023-04-05 08:54:47.812530000	60		ARP
0	7					2023-04-05 08:54:48.820242000	60		ARP

# Time display Format

- Four- time formats are supported for both real-time and offline analysis

The screenshot displays the PacketScan Web interface. The top navigation bar includes 'PacketScan Web™', 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin'. Below the navigation bar, there are buttons for 'Save', 'Load', and 'Default'. The left sidebar contains several menu items: 'Select Summary Columns', 'Time Display Format' (highlighted in blue), 'Define Summary Columns', 'Define Alias Columns', 'View Filter', 'Search Filter', 'Capture Options', 'Capture Filter', and 'Config File Editor'. The main content area is titled 'Time Display Format Configuration' and features a section 'Select Time display format' with four radio button options: 'System Time (HH:MM:SS.uSec)', 'Relative to the frame 0 (HH:MM:SS.uSec)', 'Date and Time (YYYY:MM:DD HH:MM:SS.uSec)' (which is selected and has a checkmark), and 'Time Difference between frames (HH:MM:SS.uSec)'. A green 'Apply' button is located at the bottom of the configuration area.

# Define Alias

The **Define Alias Columns** option allows to assign custom alias names to protocol fields, making filter expressions easier to create and read

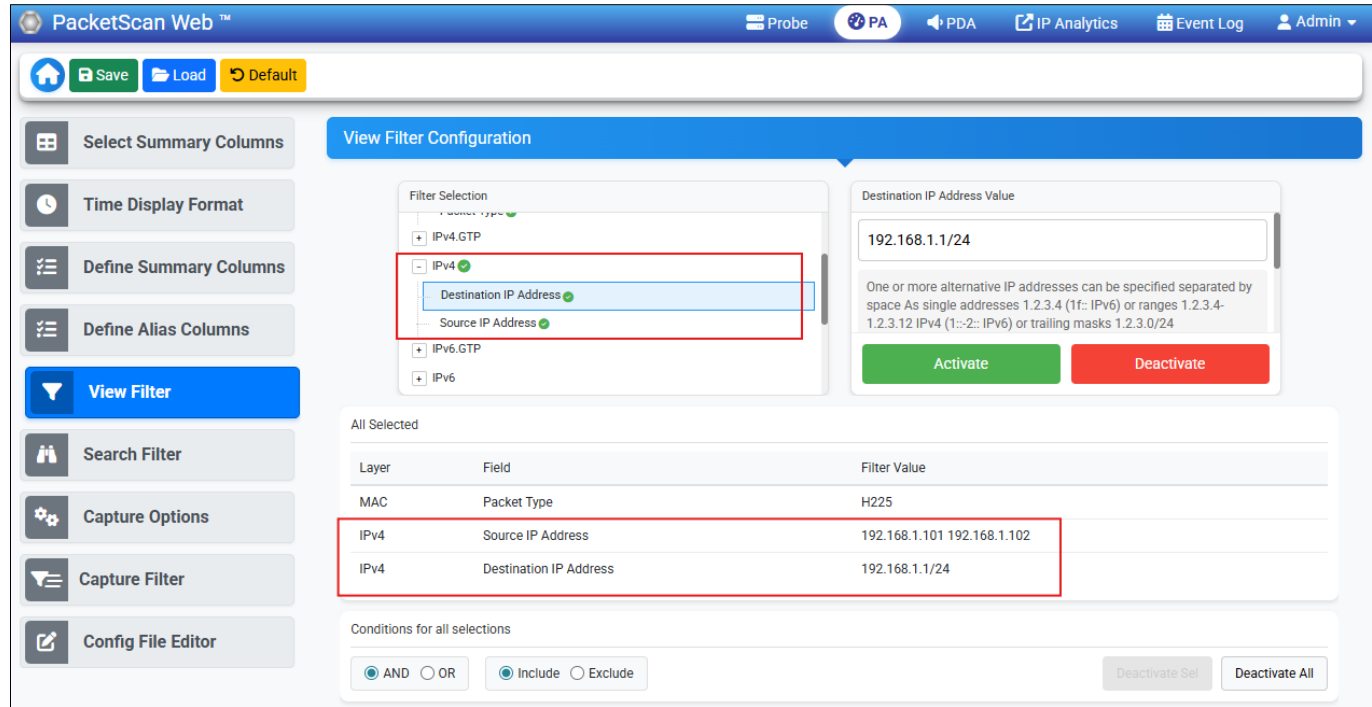
- Enter the required protocol name or keyword in the Search Protocols field (for example, IP)
- Expand the required protocol (for example, IPv4) and select the desired protocol field
- Enter a custom alias name in the corresponding Alias field (for example, ip.dst for Destination IP Address)
- Click Define Alias to save and apply the alias configuration
- Use the defined alias in filter expressions to quickly filter and analyze matching packets

The screenshot displays the 'Define Alias Columns' configuration page in the PacketScan Web interface. The interface includes a top navigation bar with 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin' options. Below the navigation bar are buttons for 'Save', 'Load', and 'Default'. The main content area is titled 'Define Alias Columns' and features a search bar with 'ip' entered and a 'Define Alias' button. A tree view on the left shows the protocol hierarchy: 'PacketScan' > 'IP Mobility' > 'IPA' > 'IPv4'. The 'IPv4' protocol is expanded, showing a list of fields. The 'Destination IP Address' field is selected, and its corresponding alias 'ip.dst' is entered in the 'Alias' field. Other fields listed include '<SrcDestIpAddr', 'Compartments', 'Copled Flag', 'Differentiated Services Codepoint', 'Don't fragment', 'Explicit Congestion Notification', 'Flag', 'Fragment Offset', 'Fragmented Ip Payload Data', 'Function', 'Handling Restrictions', and 'Header Check Sum'.

# Filter Configuration

The View Filter option filters captured packets based on selected protocol fields and values

- Select the required protocol and field
- Enter the filter value and click Activate
- Choose Include or Exclude to control the displayed packets
- Combine multiple conditions using AND or OR operators.



The screenshot shows the PacketScan Web interface for configuring a filter. The top navigation bar includes 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin'. The main area is titled 'View Filter Configuration'. On the left, a sidebar contains options: 'Select Summary Columns', 'Time Display Format', 'Define Summary Columns', 'Define Alias Columns', 'View Filter' (highlighted in blue), 'Search Filter', 'Capture Options', 'Capture Filter', and 'Config File Editor'. The main configuration area shows a 'Filter Selection' list with 'IPv4.GTP' expanded to show 'Destination IP Address' and 'Source IP Address' fields. The 'Destination IP Address Value' field is set to '192.168.1.1/24'. Below this is a table of 'All Selected' conditions:

Layer	Field	Filter Value
MAC	Packet Type	H225
IPv4	Source IP Address	192.168.1.101 192.168.1.102
IPv4	Destination IP Address	192.168.1.1/24

At the bottom, there are radio buttons for 'AND' and 'OR' (selected), and 'Include' and 'Exclude' (selected). There are also 'Deactivate Sel.' and 'Deactivate All' buttons.

# Capture Options

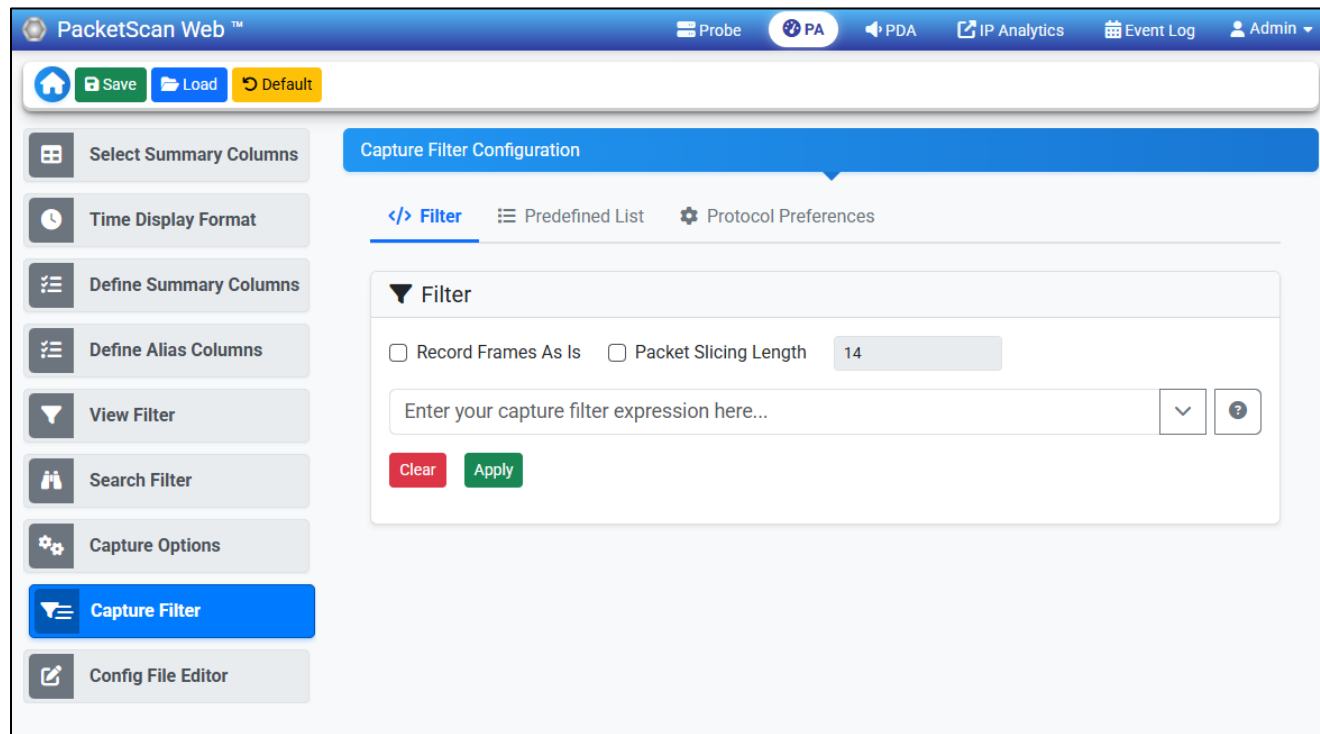
The screenshot shows the PacketScan Web interface with the 'Capture Options Configuration' panel active. The interface includes a top navigation bar with 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin' menus. A secondary bar contains 'Home', 'Save', 'Load', and 'Default' buttons. A left sidebar lists various configuration options, with 'Capture Options' highlighted in blue. The main configuration area is titled 'Capture Options Configuration' and contains the following sections:

- Interface Selection:** A scrollable list of Ethernet Boards with checkboxes:
  - Intel(R) Ethernet Connection I217-V192.168.1.28
  - Realtek Ethernet Controller192.168.1.223
- Default Capture File Name and Maximum Size:**
  - Capture File:
  - Maximum Size in Bytes:
- Capture Limit Specified as Number of Frames or Elapse Time:**
  - Circular Capture Buffer
  - In Memory
  - Frames/Time Format:

A green 'Apply' button is located at the bottom of the configuration panel.

# Capture Filter

- Configure the **capture file location**, **maximum file size**, and **capture limit** based on file size, frame count, or time duration
- Enable **Circular Capture Buffer** for continuous packet capture by overwriting the oldest packets when the buffer is full
- Select the required **network interface(s)** and use **In-Memory Capture** to improve performance during high-speed traffic capture



The screenshot displays the PacketScan Web interface for configuring a capture filter. The top navigation bar includes 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin'. Below the navigation bar, there are buttons for 'Save', 'Load', and 'Default'. The main content area is titled 'Capture Filter Configuration' and features three tabs: '</> Filter' (selected), 'Predefined List', and 'Protocol Preferences'. Under the 'Filter' tab, there is a 'Filter' section with two checkboxes: 'Record Frames As Is' and 'Packet Slicing Length' (set to 14). Below this is a text input field with the placeholder 'Enter your capture filter expression here...' and a dropdown arrow. At the bottom of the input field are 'Clear' and 'Apply' buttons. The left sidebar contains various configuration options: 'Select Summary Columns', 'Time Display Format', 'Define Summary Columns', 'Define Alias Columns', 'View Filter', 'Search Filter', 'Capture Options', 'Capture Filter' (highlighted in blue), and 'Config File Editor'.

# Starting Real Time Capture

- Click the **Start Real-time** icon from the toolbar to start real time capture
- Observe that the packets are being captured and the status bar displays real-time capture information such as capture status, capture rate, active trace file, and captured frame statistics

**Note:** For View Filters and Filter Criteria Configuration, refer to the **Additional Operations** slides



The screenshot displays the PacketScan Web interface. The top part shows a table of captured packets with columns for Device, Frame#, TIME (Date), Length (Bytes), Error, Length/Protocol Type\_MAC, Packet Type\_MAC, Source IP Address\_IPv4, Destination IP Address\_IPv4, and Source Address\_IPv6. The table lists 21 frames, all with a length of 60 bytes and protocol type of IEEE802.3 Length Field. The first frame is selected, and its details are shown below.

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
0	0	2026-05-11 03:57:22.068852000	60		IEEE802.3 Length Field				
0	1	2026-05-11 03:57:23.108861000	60		IEEE802.3 Length Field				
0	2	2026-05-11 03:57:24.068825000	60		IEEE802.3 Length Field				
0	3	2026-05-11 03:57:25.108765000	60		IEEE802.3 Length Field				
0	4	2026-05-11 03:57:25.420064000	64		Internet IP(IPv4)		192.168.200.1	255.255.255.255	
0	5	2026-05-11 03:57:25.4200704000	71		Internet IP(IPv4)		192.168.200.1	255.255.255.255	
0	6	2026-05-11 03:57:26.069200000	60		IEEE802.3 Length Field				
0	7	2026-05-11 03:57:27.108679000	60		IEEE802.3 Length Field				
0	8	2026-05-11 03:57:28.068783000	60		IEEE802.3 Length Field				
0	9	2026-05-11 03:57:29.108761000	60		IEEE802.3 Length Field				
0	10	2026-05-11 03:57:30.068739000	60		IEEE802.3 Length Field				
0	11	2026-05-11 03:57:31.109028000	60		IEEE802.3 Length Field				
0	12	2026-05-11 03:57:32.068811000	60		IEEE802.3 Length Field				
0	13	2026-05-11 03:57:33.108801000	60		IEEE802.3 Length Field				
0	14	2026-05-11 03:57:34.068786000	60		IEEE802.3 Length Field				
0	15	2026-05-11 03:57:35.108892000	60		IEEE802.3 Length Field				
0	16	2026-05-11 03:57:35.429660000	64		Internet IP(IPv4)		192.168.200.1	255.255.255.255	
0	17	2026-05-11 03:57:35.430368000	71		Internet IP(IPv4)		192.168.200.1	255.255.255.255	
0	18	2026-05-11 03:57:35.766244000	66		Internet IP(IPv4)		192.168.200.111	192.168.100.111	
0	19	2026-05-11 03:57:35.766291000	66		Internet IP(IPv4)		192.168.200.111	192.168.100.111	
0	20	2026-05-11 03:57:35.766299000	66		Internet IP(IPv4)		192.168.200.111	192.168.100.111	
0	21	2026-05-11 03:57:35.766310000	66		Internet IP(IPv4)		192.168.200.111	192.168.100.111	

Device0 Frame=0 at 2026-05-11 03:57:22.068852000 OK Len=60

Ethernet Frame Data

```
===== MAC Layer =====
0000 Destination Address = x0180C2000000
0006 Source Address     = x144CFF0143FA
000C Length/Protocol Type = x0026 IEEE802.3 Length Field
===== LLC [MAC] Layer =====
000E Destination Address = 0100001. (33)
000E Individual/Group (I/G) = .....0 Individual DSAP
000F Source Address     = 0100001. (33)
000F Command/Response (C/R) = .....0 Command
0010 Control Field      = .....11 Unnumbered
0010 Modifier Function  = 000.00.. UI
0010 Poll/Final        = ...0.... (0)
===== STP Layer =====
```

Hex Dump of the Frame Data

```
-----+-----+-----+
01 80 C2 00 00 00 14 4C FF 01 43 FA 00 26 42 42 .....L...sBB
03 00 00 00 00 00 7F FF 14 4C FF 01 43 F7 00 00 .....L...C....
00 00 7F FF 14 4C FF 01 43 F7 80 04 00 00 0A 00 .....L...C.....
01 00 08 00 00 00 00 00 08 0D E6 72 ..... ..F
```

Online-Running | Capture Rate : 0.01 Mbps | ...Inc\PacketScanWebProbe\Users\Instance 1\Temp.hdl | Captured 2433 Frames | Missing Frames : 0



# LTE Protocol Analysis

- Captures and monitors real-time signaling and traffic on LTE networks
- The application segregates, monitors and collects statistics on all calls and can test eNodeB or UE over various interfaces, including S1, S3, S4, S5 (or S8), S6a, S10, S11, S13, and X2

The screenshot displays the PacketScan Web interface. At the top, there's a navigation bar with 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin' options. Below this is a toolbar with various icons for file operations and analysis. The main area is divided into two sections. The upper section is a table listing network traffic:

Device	Frame#	Source IP Address IPv4	TIME (Date)	Length (Bytes)	Error	Length/Protocol Type_MAC	Packet Type_MAC	Source Port_UDP	Destination Port_UDP	Source Port_TCP
2	61	192.168.12.26	2021-08-02 18:19:05.56383000	65		Internet IP(IPv4)		2123	2123	
2	62	192.168.12.111	2021-08-02 18:19:05.566871000	71		Internet IP(IPv4)		2124	2124	
2	63	192.168.12.112	2021-08-02 18:19:05.569585000	64		Internet IP(IPv4)		2124	2124	
2	64	192.168.12.111	2021-08-02 18:19:05.572667000	69		Internet IP(IPv4)		2123	2123	
2	65	192.168.12.26	2021-08-02 18:19:05.579289000	110		Internet IP(IPv4)				
2	66	192.168.12.27	2021-08-02 18:19:05.590383000	118		Internet IP(IPv4)				
2	67	192.168.12.27	2021-08-02 18:19:05.592325000	130		Internet IP(IPv4)				
2	68	192.168.12.26	2021-08-02 18:19:05.609378000	274		Internet IP(IPv4)				
2	69	192.168.12.110	2021-08-02 18:19:05.618459000	242		Internet IP(IPv4)				
2	70	192.168.12.26	2021-08-02 18:19:05.639061000	65		Internet IP(IPv4)		2123	2123	
2	71	192.168.12.111	2021-08-02 18:19:05.642740000	71		Internet IP(IPv4)		2124	2124	

The lower section shows a detailed protocol analysis of the selected frame (Frame 65). It lists various protocol fields and their values:

- 005D ProtocolIE-Container = Item 3
- 005D ProtocolIE-Field = SEQUENCE
- 005D ProtocolIE-ID = INTEGER
- 005D Contents = 26 id-NAS-PDU
- 005F Criticality = ENUMERATOR
- 005F Contents = 0 reject(0)
- 0060 Length = 11
- 0061 value = Open Type
- 0061 NAS PDU = SEQUENCE
- 0061 NAS-PDU = OCTET STRING
- 0061 Length Determinant = 10
- 0062 Contents = x273A7585DA0408F8ACE5

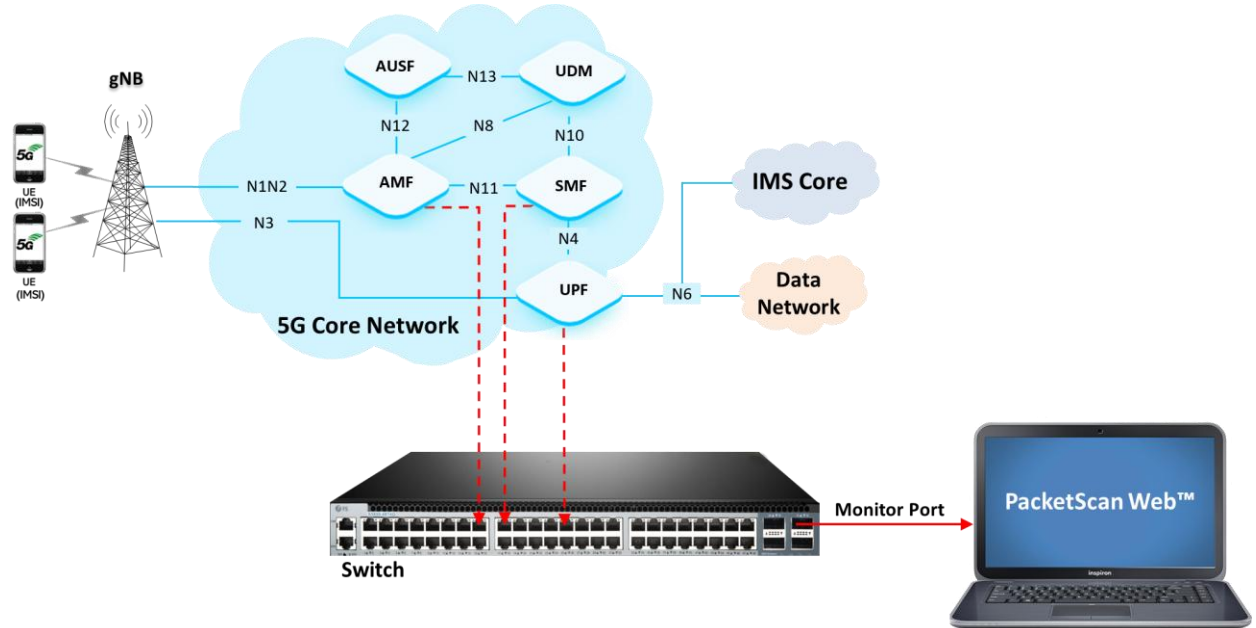
Below the list, there's a hex dump of the frame data:

```
Hex Dump of the Frame Data
+-----+-----+-----+-----+-----+-----+-----+-----+
00 24 1D 78 08 9C 00 24 1D 78 87 1C 08 00 45 00  .$.x...$.x...E.
00 60 4F 45 00 00 80 84 00 00 C0 A8 0C 1A C0 A8  .`OE.....
0C 1B 8E 3C 8E 3C 3C 1D EE 13 D1 44 AE B8 00 03  .>.<<<.D...
00 3E 00 00 00 26 00 01 00 25 00 00 00 12 00 07  .>...$.
00 2A 00 00 04 00 00 00 02 00 11 00 08 00 03 40  .*......@
27 16 00 21 00 07 00 00 23 00 02 0C 40 00 1A 00  .`!.....#...@...
0B 0A 27 3A 75 85 DA 04 08 F8 AC E5 00 00  .`:u... .....
```

The status bar at the bottom indicates the file path: 'Off-line ...\GL Communications Inc\PacketScanWebProbe\SampleTraces\LTE\LTE-EndToEnd-Call.hdl' and the frame number '87 Frames'.

# 5G Protocol Analysis

- Captures, segregates, monitors and collects statistics on all calls over N1N2, N4, N8, N10, N12 and N13 interfaces of the 5G network
- Provides VoNR call statistics such as caller, callee, MOS scores, discarded packets and voice storage



# Packet Data Analyzer (PDA)

- PacketScan Web™ includes Call Summary View and Registration Summary View interfaces under the PDA module for call-level signaling analysis and troubleshooting

The screenshot displays the PacketScan Web PDA interface. The top navigation bar includes 'PDA' and 'IP Analytics'. The main content area is split into two views:

- Call Summary View:** A table listing call details. A red box highlights the 'SIP Registration Summary' tab. A red arrow points to the 'Summary View' label.
- Registration Summary View:** A table showing registration events. A red box highlights the 'SIP Registration Summary' tab. A red arrow points to the 'Registration Summary View' label.

The Registration Summary table includes columns: Reg#, Method, RegisterRequestTime, UserAgent, Registrar, Result, Status, ErrorCode, CallID, RegisteredTime, Requests, Responses, and Expires. The Call Summary table includes columns: Call#, Caller, Callee, StartTime, Duration, VoiceQuality\_L, VoiceQuality\_R, Payload\_L, Payload\_R, Result, ErrorCode, FailureCause, and CallID.

The bottom section shows a packet capture view for the IP address 192.168.12.117, displaying SIP layer details for a REGISTER request and response.

# CDR Configuration

- **Customize** Call Detail Record (CDR) fields to display the most relevant call information
- **Configure** CDR parameters for on-screen analysis or database storage
- **Optimize** call monitoring and reporting with flexible column selection and layouts

PacketScan Web™

Probe PA PDA IP Analytics Event Log

CDR Configuration

Export to CSV

Whitelist Config

Criteria Based Recording

Other Option

CDR Configuration

Display Configuration

Database Configuration

Selection Methods: Single click selects a single item, Ctrl + Click enables multiple selections, and Shift + Click selects a range of items between the last selected and the current click.  
Rearrangement Methods: Drag and drop allows reordering items within a list and moving items between the list boxes.

Protocol

SIP

H323

RTP

MEGACO

GSM

luCS

SKINNY

CAMEL

ISUP

LTE

Selected Columns

WhiteList

HDLTraceFileName

Caller

Callee

CallID

StartTime

Duration

EndTime

CallSuccess

FailureCause

PostDialDelay

SessionDisconnectDelay

Hidden Columns

InBandDgt\_LL

InBandDgt\_LR

ISUPCalledNumber

ISUPCallingNumber

ISUPCalledNOA

ISUPCallingNOA

ISUPCalledPartyCategory

ISUPCallingPartyCategory

ISUPCallingPartyNPI

ISUPLocationValue

ISUPReleaseCause

SinalInFrameCount

Copy to Display Config

Select All Restore Apply

# Export to CSV

- **Export** Traffic Call Detail Records (CDRs) and Frame Summary for selected protocols to **CSV** files at the specified location

The screenshot displays the 'Export to CSV' configuration page in the PacketScan Web interface. The page is titled 'Export to CSV' and features a sidebar with navigation options: CDR Configuration, Export to CSV (highlighted), Whitelist Config, Criteria Based Recording, and Other Option. The main content area is divided into several sections:

- Selected Protocols:** A list of protocols with checkboxes. SIP is selected, while H323, RTP, MEGACO, GSMA, luCS, SKINNY, CAMEL, and ISUP are not.
- Probe Name:** A text input field containing 'VoIP'.
- Write Call Detail Record (CDR):** A checked checkbox.
- Append CDR Header Fields:** A checked checkbox.
- Active Call CDR:** An unchecked checkbox.
- Update Every (Sec):** A numeric input field set to '0'.
- Write frameSummary:** A checked checkbox.
- ED137 Events:** An unchecked checkbox.
- MSRP Frame Summary:** An unchecked checkbox.
- CSV File Configuration:**
  - Directory:** A text input field containing 'C:\Program Files\GL Communications Inc\PacketScanWebProbe\Users\Test 1\CSVFiles'.
  - File Name:** A text input field containing 'ProtocolName\_Test\_Year\_Month\_Date\_Hr\_Min'.
  - Create Protocol Sub-Folder:** A checked checkbox.
  - Create New File After:** A section with three radio buttons: 'File Size' (unchecked), 'Record Count' (unchecked), and 'Time Duration' (checked). The 'Time Duration' field is set to '60' seconds.
  - File Timeout (Sec):** A numeric input field set to '10'.

An 'Activate' button is located at the bottom of the configuration section.

# 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

The screenshot shows the PacketScan Web interface with the PDA (Packet Detail Analyzer) view selected. The top navigation bar includes 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin'. The main header displays 'SIP' and 'Show All Calls' with a 'Call Count : 824'. Below this is a table titled 'SIP Registration Summary' with columns for Call#, Caller, Callee, StartTime, Duration, VoiceQuality\_L, VoiceQuality\_R, Payload\_L, Payload\_R, Result, ErrorCode, FailureCause, and CallID. The table lists 12 call entries with various details.

Below the table, there are tabs for 'CallFlow' and 'Statistics'. The 'CallFlow' tab is active, showing a sequence of frames between two IP addresses: fe80::3f20:7953:f2df:f26a and fe80::6c2b:7326:94f6:2. The frames include INVITE, SIP/2.0 100 Trying, SIP/2.0 180 Ringing, SIP/2.0 200 OK, ACK, BYE, and another SIP/2.0 200 OK.

The 'Statistics' tab is also visible, showing a search bar and a 'Find Next' button. The 'Find' field contains 'SIP Layer' and the 'Complete Stack' checkbox is checked.

The detailed view shows the SIP layer analysis for the selected frame. The text includes:
 

```

    ===== SIP Layer =====
    INVITE sip:0722@[fe80::6c2b:7326:94f6:21e7]:transport=tcp SIP/2.0
    Via: SIP/2.0/UDP [fe80::3f20:7953:f2df:f26a]:5060;branch=z9hG4bK-2619-766725347-25880-14696
    Max-Forwards: 70
    Allow: INVITE, BYE, CANCEL, ACK, INFO, OPTIONS, SUBSCRIBE, NOTIFY, REFER, REGISTER, UPDATE
    From: 0722 <sip:0722@[fe80::3f20:7953:f2df:f26a]>;tag=FromTag-2616-766725347-25877-14696
    To: 0722 <sip:0722@[fe80::6c2b:7326:94f6:21e7]>
    Call-ID: GL-MAPS-2618-766725347-25879-14696@fe80::3f20:7953:f2df:f26a
    CSeq: 1 INVITE
    Contact: 0722 <sip:0722@[fe80::3f20:7953:f2df:f26a]:transport=tcp>
    Content-Type: application/sdp
    Content-Length: 385

    v=0
    o=0722 33142031 1 IN IP6 fe80::3f20:7953:f2df:f26a17
    s=SIP Call
    c=IN IP6 fe80::3f20:7953:f2df:f26a17
    t=0
    m=audio 3910 RTP/AVP 111 8 18 3 101
    a=rtptime:1111 SPEEX/8000
    a=fmtp:1111 ebw=8000;vbr=0;cong=off;penh=0
    
```

# Call Graph – SIP Call

- Displays the message sequences of captured VoIP calls
- Decodes the selected SIP message and displays it on the right pane
- The Complete Stack option enables the user to view the full call details for the selected message on the ladder diagram

The screenshot displays the PacketScan Web interface for a SIP call. 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, ErrorCode, FailureCause, CallID, and EndTime. A red arrow points from the 'CallID' column of the first row (0001) to the 'CallFlow' section.

The 'CallFlow' section shows a ladder diagram of the call sequence between 192.168.12.92 and 192.168.12.94. The sequence includes: INVITE (0.00.000), SIP/2.0 100 Trying (0.00.028), SIP/2.0 180 Ringing (0.00.029), SIP/2.0 200 OK (0.00.153), ACK (0.00.163), BYE (01.00.177), and SIP/2.0 200 OK (01.00.187).

The 'Find' section on the right shows the decoded SIP message for the selected INVITE. The 'Complete Stack' checkbox is checked. The decoded message details are as follows:

```
===== MAC Layer =====
Destination Address = xC624D3EEB30
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-Capable Transport)
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 (...00000 00000000)
Time To Live         = 128 (x80)
Protocol             = 00010001 UDP
Header Check Sum     = x0000
Source IP Address    = 192.168.12.92 (xCOA80C5C)
Destination IP Address = 192.168.12.94 (xCOA80C5E)
===== UDP Layer =====
Source Port          = 5060 (x13C4)
Destination Port     = 5060 (x13C4)
Length (Header + Data) = 741 (x02E5)
```

A red arrow points from the 'SIP/2.0 100 Trying' message in the ladder diagram to the 'Time To Live' field in the decoded message details.

Displays decoded information of selected SIP message

# Registration Summary

- Displays the SIP registration information in a tabular format which includes user agent, registrar, registered time, status, and so on for each user agent
- Provides the Call flow and statistics of each registration

The screenshot displays the PacketScan Web interface. At the top, there's a navigation bar with 'Probe', 'PA', 'PDA', 'IP Analytics', 'Event Log', and 'Admin'. Below this, a search bar contains 'Show All Registrations' and 'Call Count : 3'. There are dropdown menus for 'Probe' (Probe 1) and 'PA Instance' (Test 1). The main content area is divided into two sections: 'SIP Registration Summary' and 'CallFlow'.

**SIP Registration Summary Table:**

Reg#	Method	RegisterRequestTime	UserAgent	Registrar	Result	Status	ErrorCode	CallID	RegisteredTime	Requests	Responses
<input type="checkbox"/> 1	Register	2024-10-16 17:13:18.132	0001	192.168.12.117	Passed	Registered		GL-MAPS-1-667514568-2512-5580@192.168.12.117	2024-10-16 17:13:18.257	3	3
<input type="checkbox"/> 2	Register	2024-10-16 17:13:23.805	0001	192.168.12.95	Passed	Registered		GL-MAPS-1-667520231-14548-6976@192.168.12.95	2024-10-16 17:13:23.934	3	3
<input type="checkbox"/> 3	DeRegister	2024-10-16 17:13:51.769	0001	192.168.12.117	Passed	De-Registered		GL-MAPS-1-667514568-2512-5580@192.168.12.117		2	2

**CallFlow Section:**

Column Width: [Slider] Absolute Timing [ ] Show Latest [ ]

Find [ ] Find Next [ ] Complete Stack [ ]

Time Frame# 192.168.12.117 192.168.12.158

Time	Frame#	Source	Destination	Content
00:00:00.000	0	5060	5060	REGISTER
00:00:00.001	1	5060	5060	SIP/2.0 407 Proxy Authentication ...
00:00:00.011	2	5060	5060	REGISTER
00:00:00.013	3	5060	5060	REGISTER
00:00:00.124	4	5060	5060	SIP/2.0 200 OK
00:00:00.126	5	5060	5060	SIP/2.0 200 OK

**SIP Layer Details:**

```
===== SIP Layer =====
REGISTER sip:192.168.12.117 SIP/2.0
Via: SIP/2.0/UDP 192.168.12.117:5060;branch=z9hG4bK-4-667514590-2515-5580
Route: <sip:192.168.12.158:5060;lr>
Max-Forwards: 70
Allow: INVITE, BYE, CANCEL, ACK, INFO, PRACK, OPTIONS, SUBSCRIBE, NOTIFY, REFER, REGISTER, UPDATE
From: 0001 <sip:0001@192.168.12.117>;tag=FromTag-2-667514568-2513-5580
To: <sip:0001@192.168.12.117>
Call-ID: GL-MAPS-1-667514568-2512-5580@192.168.12.117
CSeq: 1 REGISTER
Expires: 3600
Contact: 0001 <sip:0001@192.168.12.117>
Content-Length: 0
```

# Registration Statistics

- Display the count of the registration details

CallFlow **Statistics**

**SIP Registration statistics**

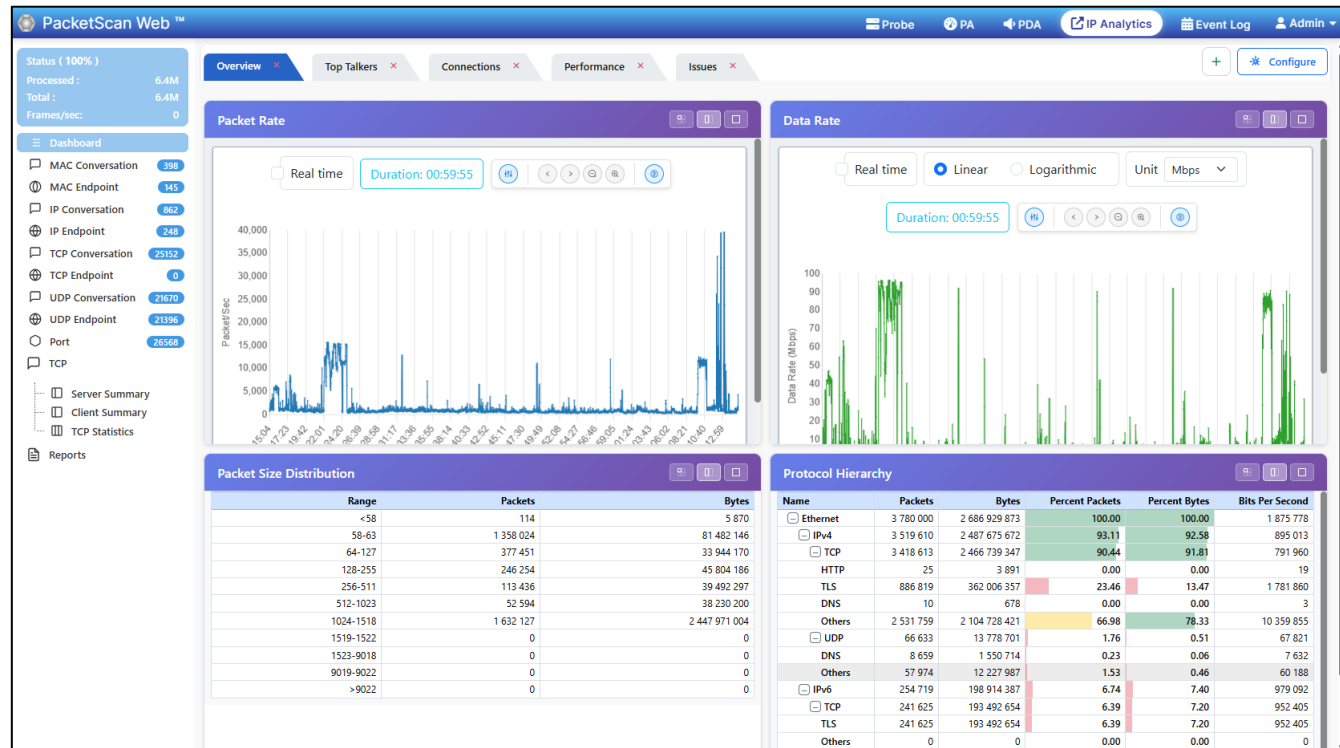
Registration Summary	
Total Registrations	3
Active Registrations	0
Completed Registrations	3
Failed Registrations	0
Timed Out Registrations	0
InProgress Registrations	0

Registration Sessions and Messages	
Registration Sessions	2
De-Registration Sessions	1
Registration Messages	6
De-Registration Messages	2

Global Failures	
403 Forbidden	0
404 Not Found	0
423 Interval Too Brief	0
480 Temporarily Unavailable	0
482 Loop Detected	0
4xx Other Client Failure	0
500 Server Internal Error	0
5xx Other Server Failure	0
603 Decline	0
6xx Other Global Failures	0

# IP Analytics

- IP Analytics™ in PacketScan Web™ provides session-level visibility into real-time and offline IP traffic through graphical dashboards and protocol-aware analytics
- The solution organizes traffic into IP, MAC, TCP, and UDP conversations and endpoints, enabling users to monitor packet rate, data rate, protocol hierarchy, throughput trends, retransmissions, congestion behavior, and session statistics



**Thank you**