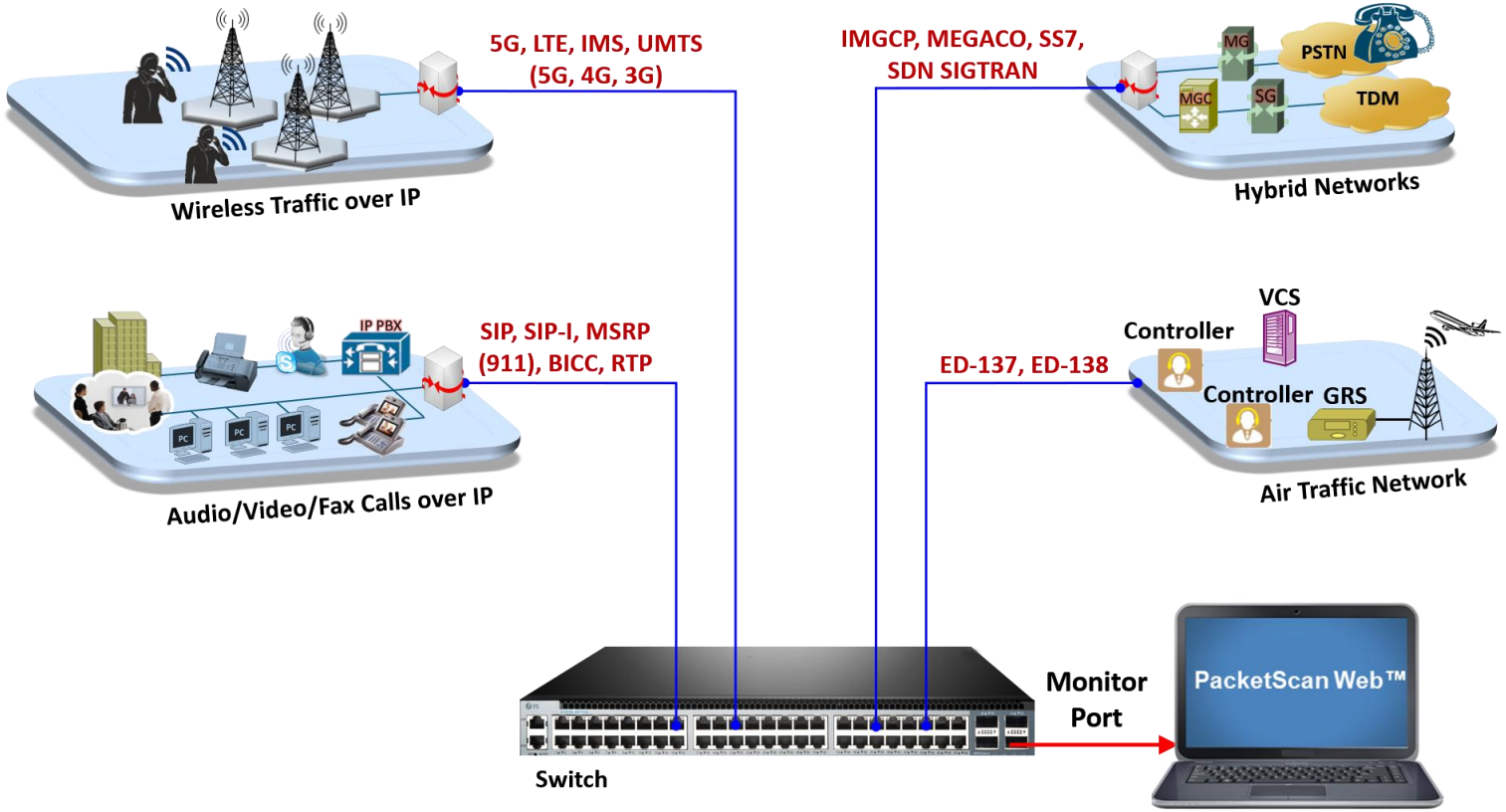
PacketScan Web™

All-IP Signaling and Traffic Analysis

GL Communications Inc.
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 Web™ All-IP Signaling and Traffic Analysis

(5G/4G/3G/2G/VoIP/RTP, RTCP/ Video Analysis)



GL Communications

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

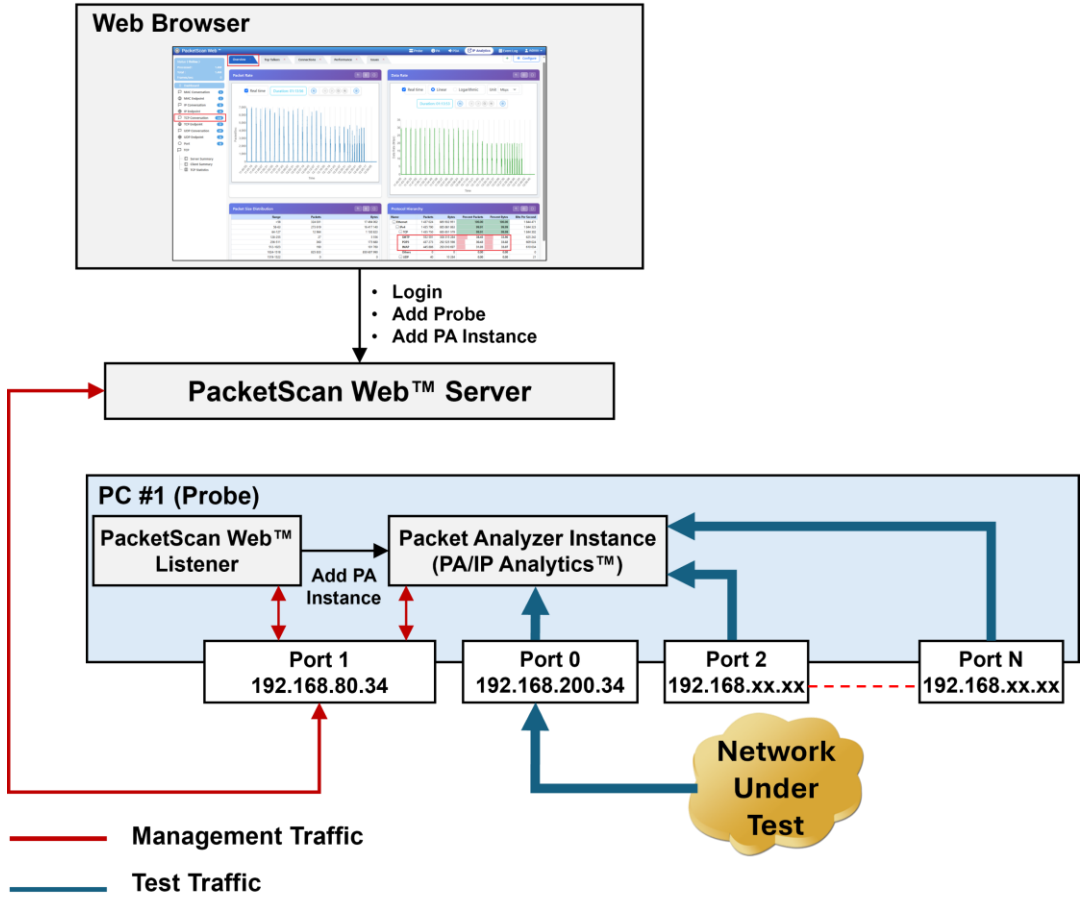
- **Enhanced Capture Filters**
  - Choose from built-in protocol filters or define custom expressions
  - Apply filters pre-capture or post-capture for flexible control
  - Supports IP groups, subnets, and range-based filtering
  - Save and reuse filters across sessions or probes for consistent workflows

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

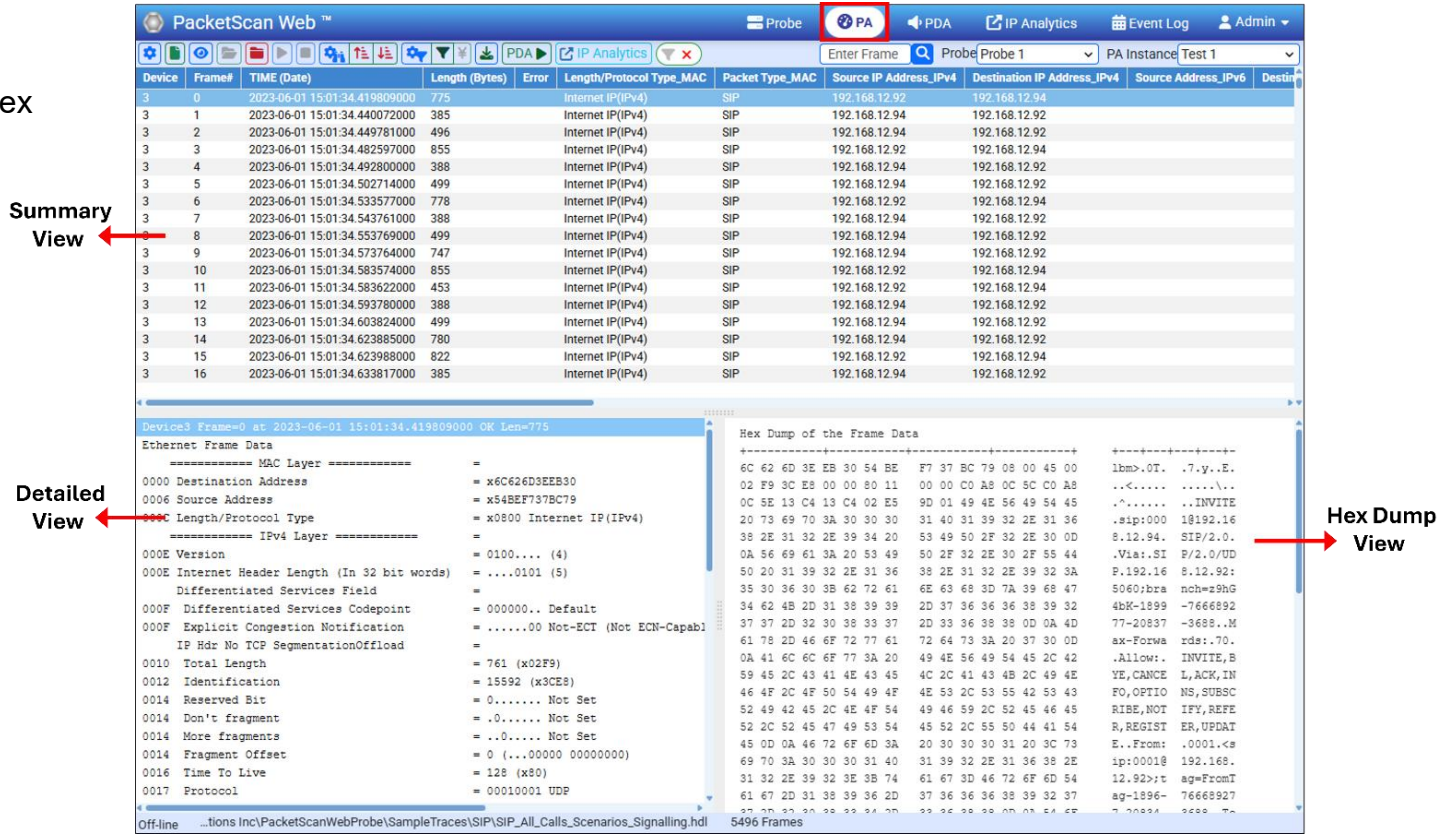
PacketScan Web™ Architecture

- **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



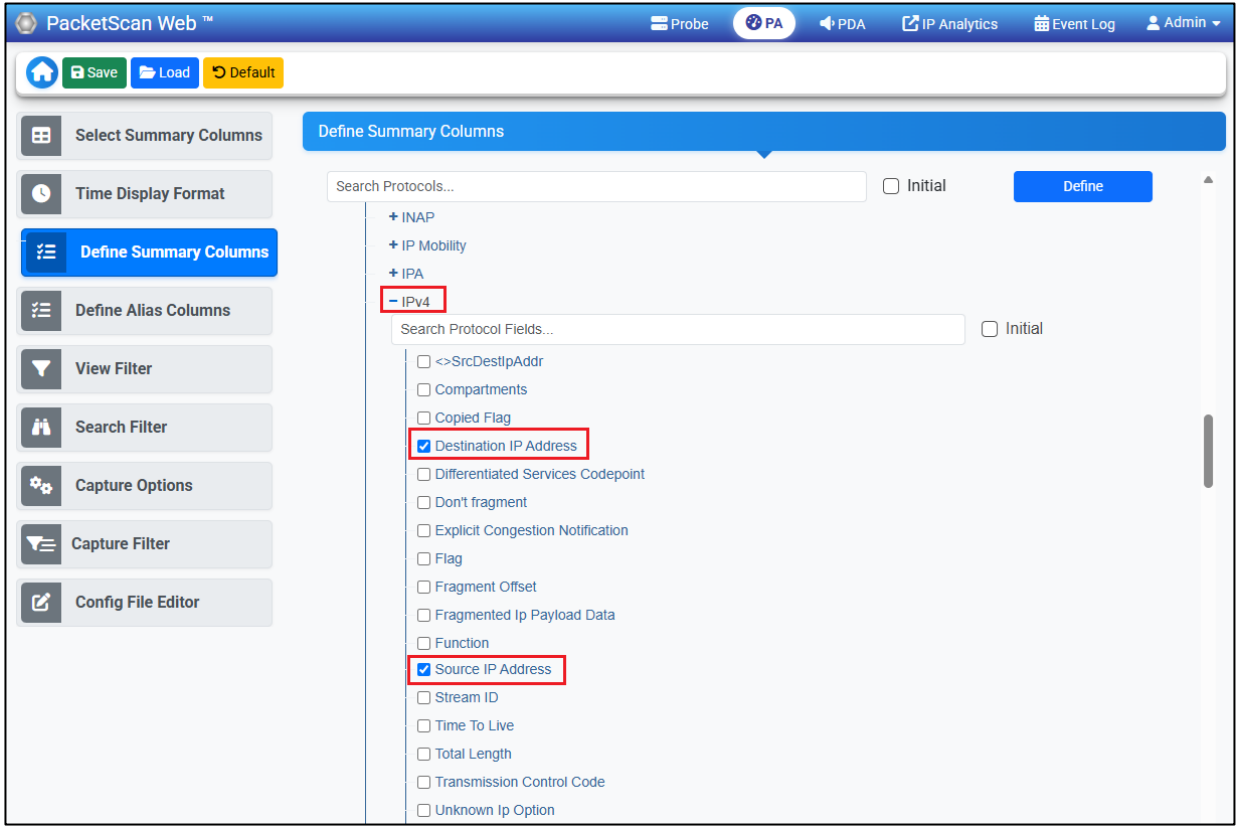
Packet Analyzer (PA)

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



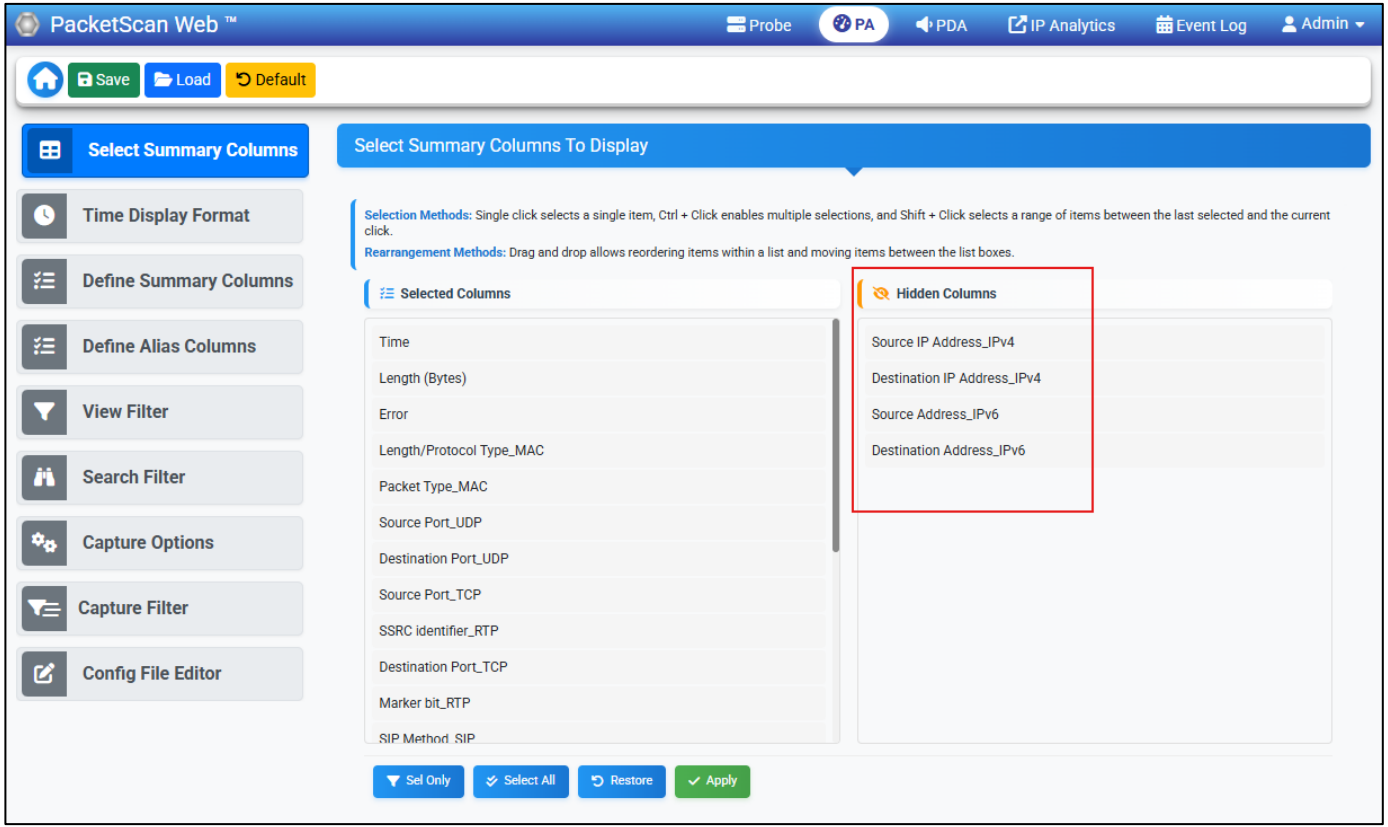
Define Summary Columns

- 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



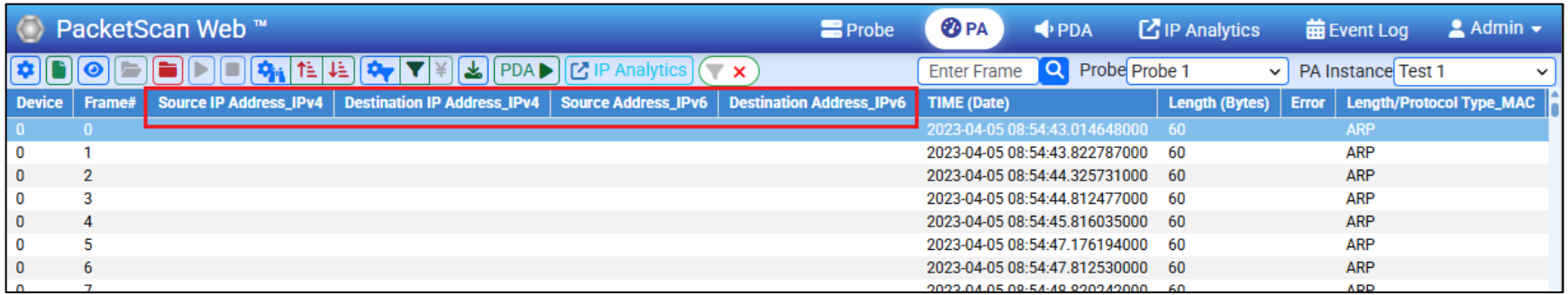
Select Summary Columns

- 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



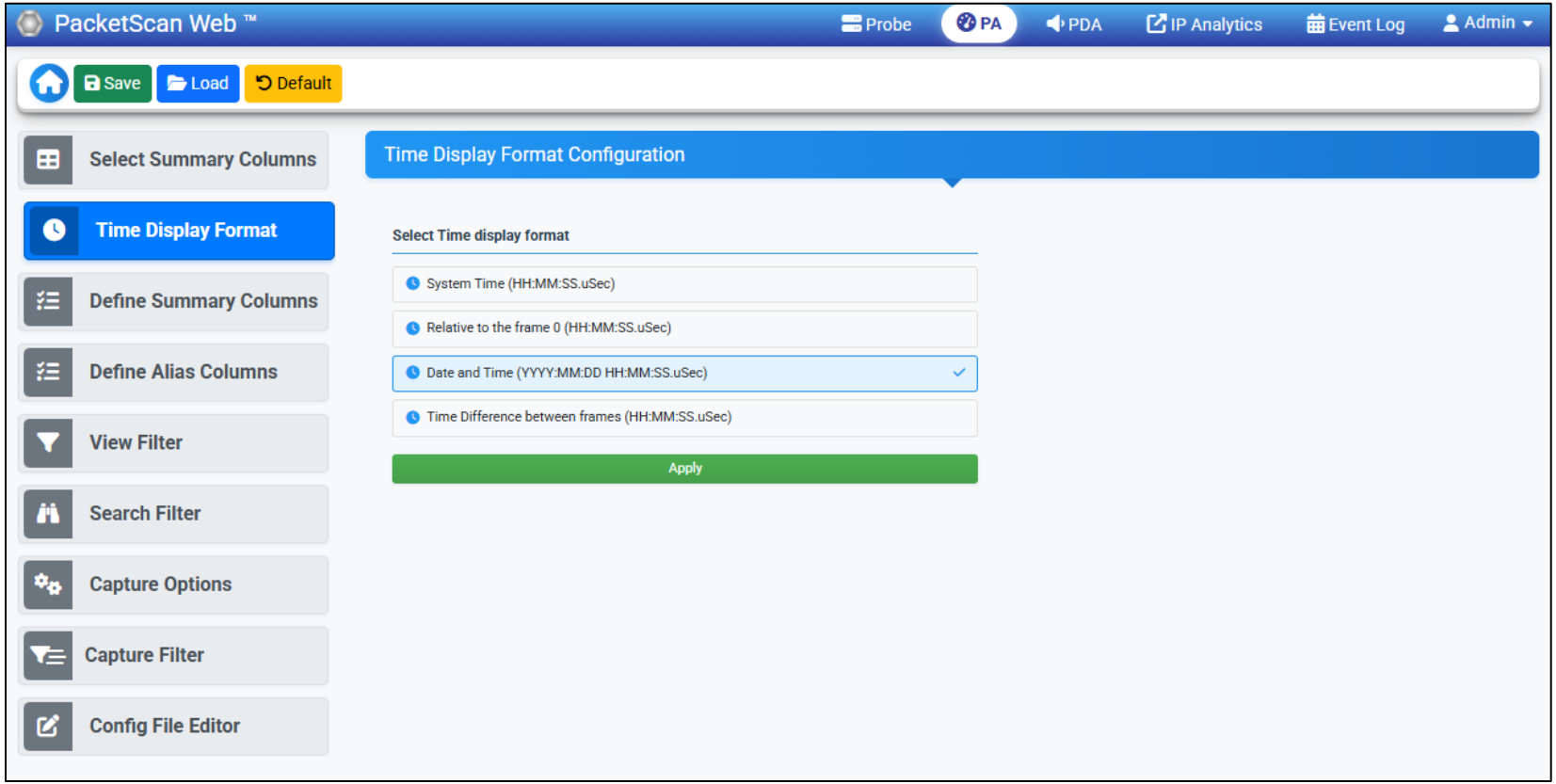
Summary View

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



Time display Format

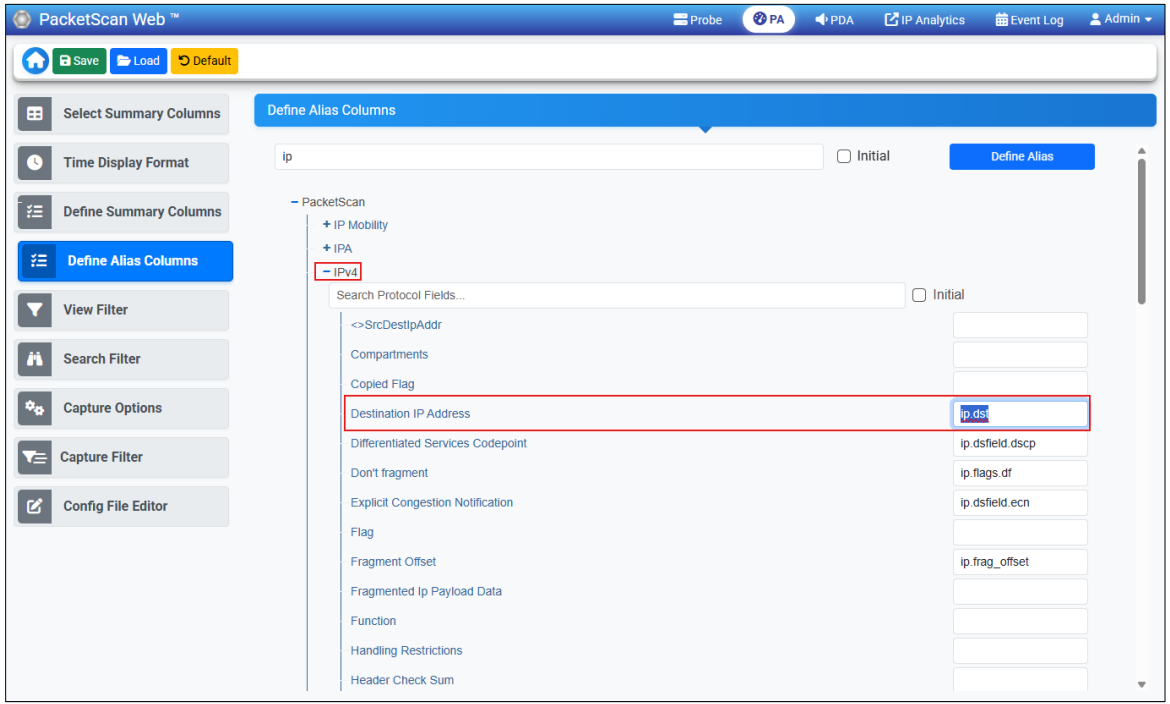
- Four- time formats are supported for both real-time and offline analysis



Define Alias

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

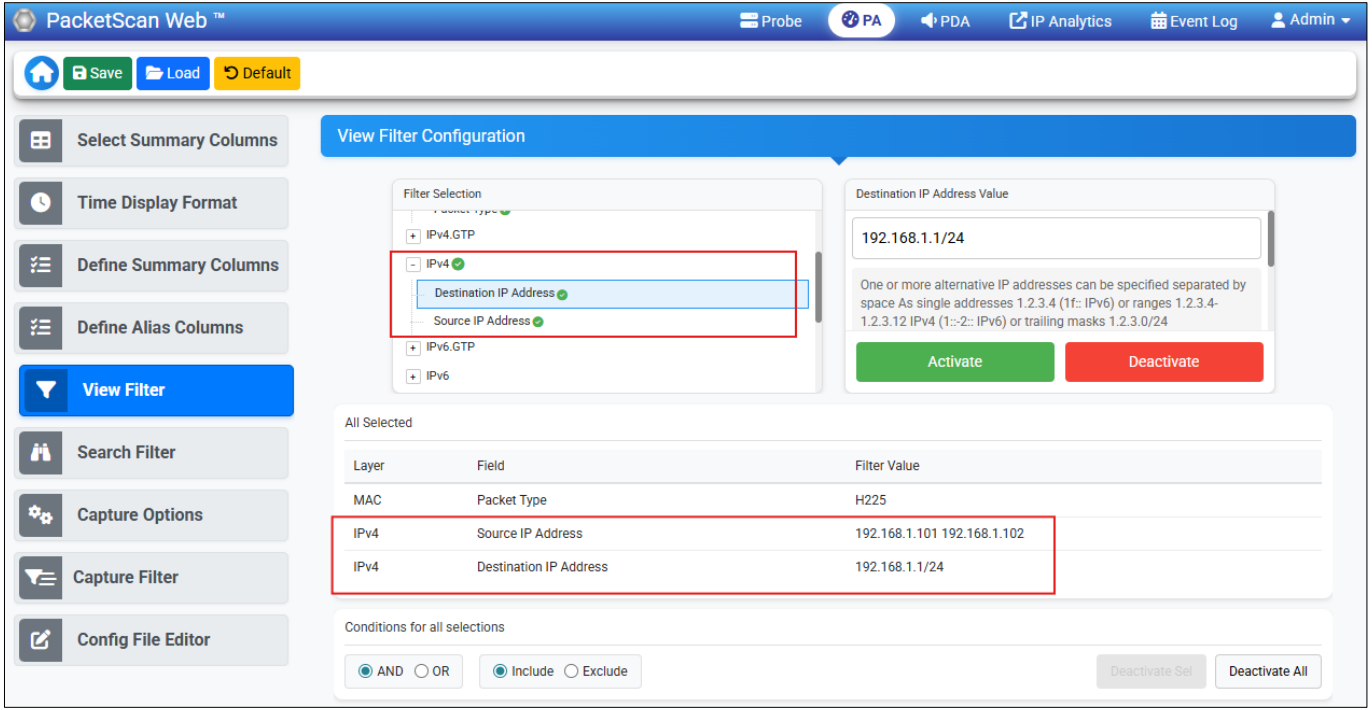
- Enter the required protocol name or keyword in the Search Protocols field (for example, IP)
- Expand the required protocol (for example, IPv4) and select the desired protocol field
- Enter a custom alias name in the corresponding Alias field (for example, ip.dst for Destination IP Address)
- Click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



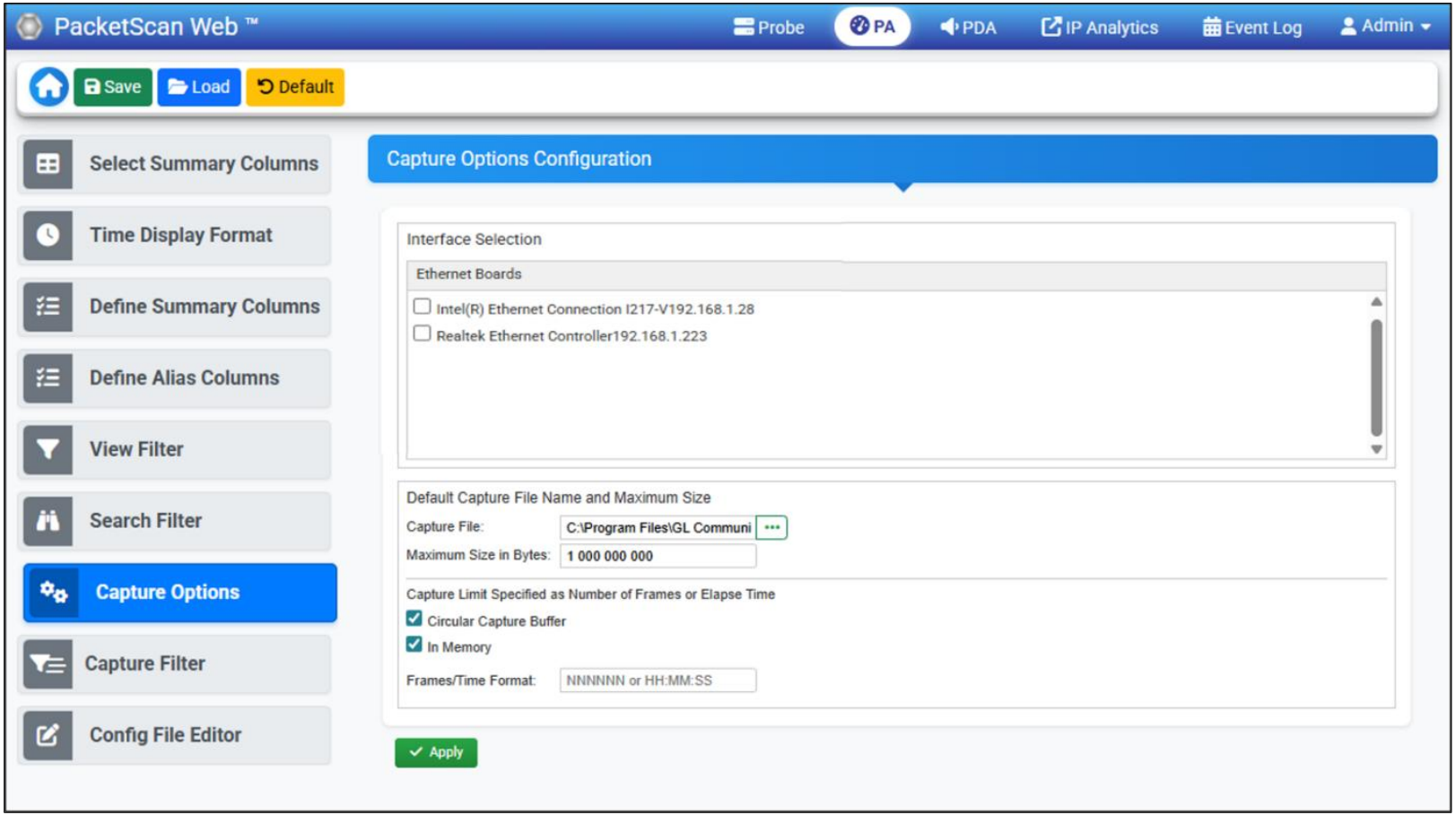
Filter Configuration

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.

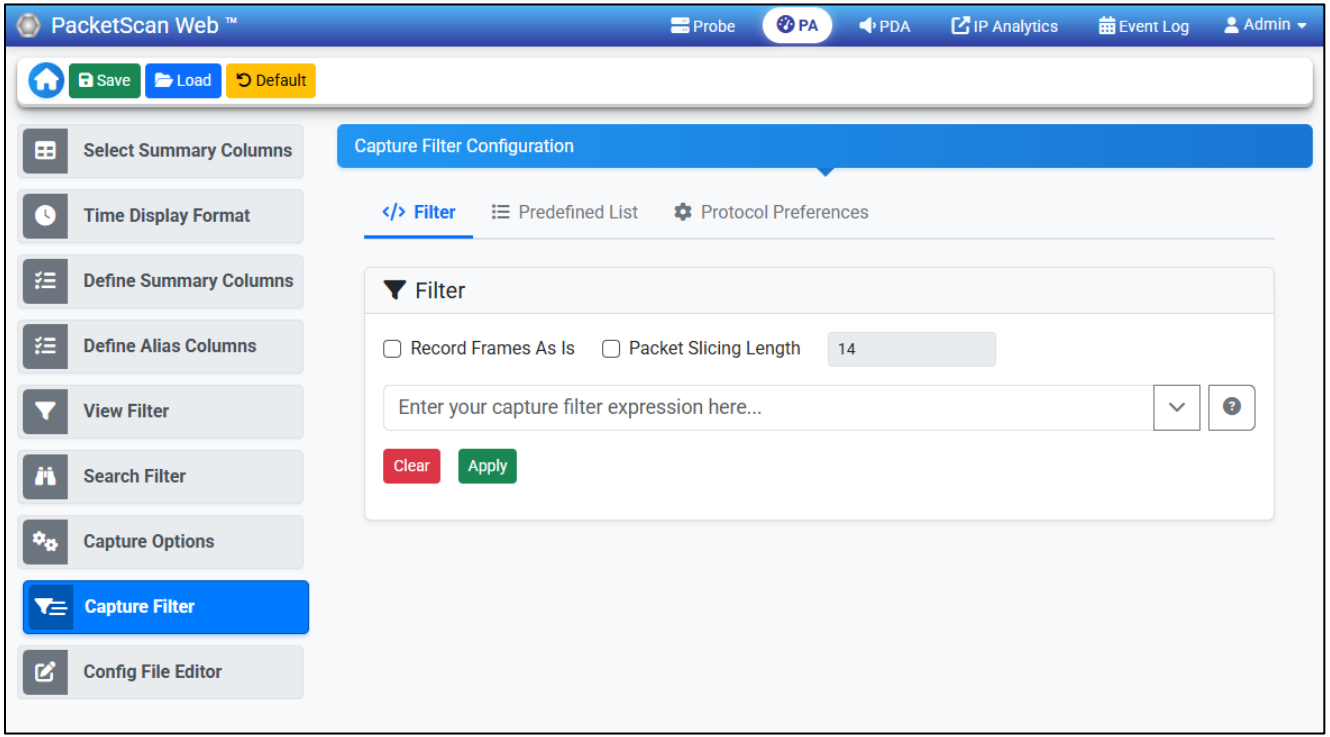


Capture Options



Capture Filter

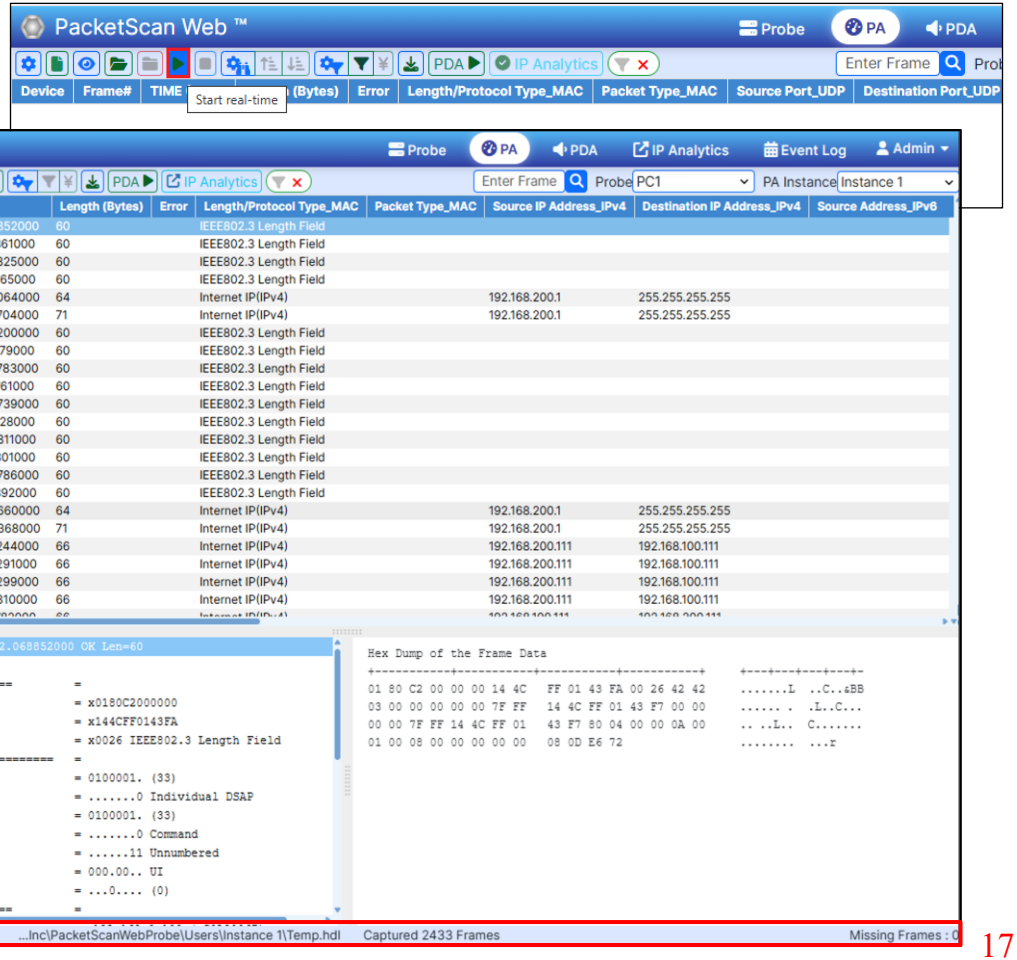
- Configure the **capture file location**, **maximum file size**, and **capture limit** based on file size, frame count, or time duration
- Enable **Circular Capture Buffer** for continuous packet capture by overwriting the oldest packets when the buffer is full
- Select the required **network interface(s)**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



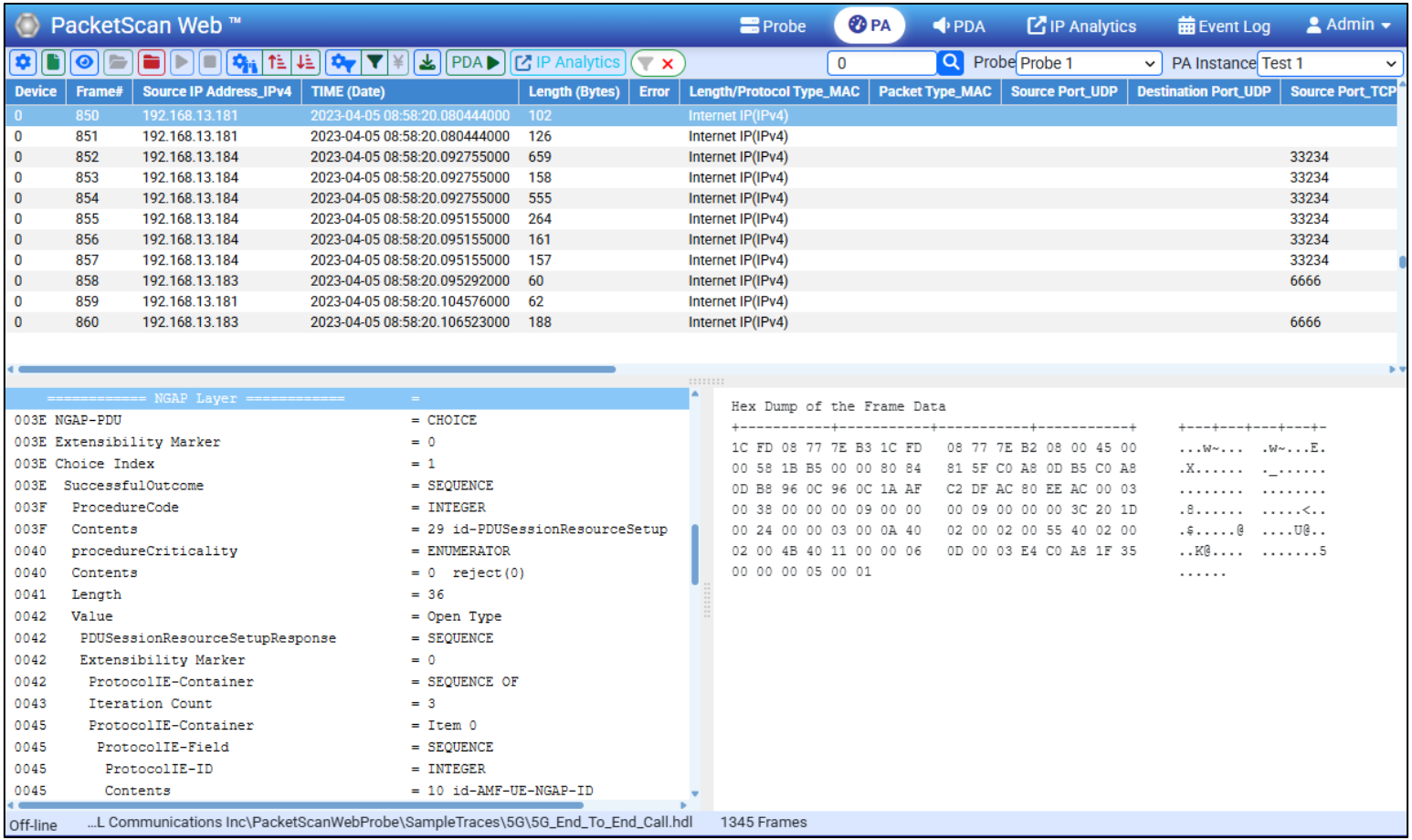
Starting Real Time Capture

- 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

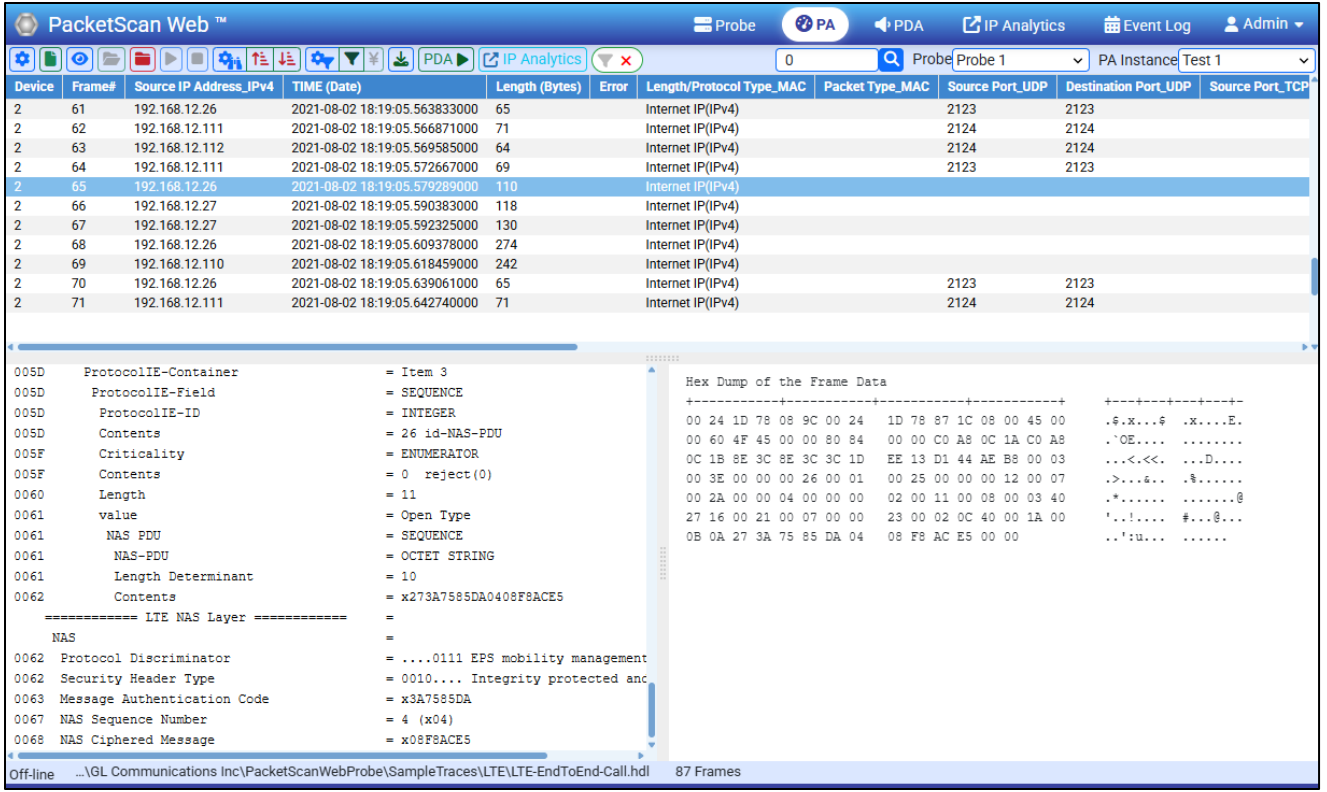


Decode View - 5G NGAP Layer



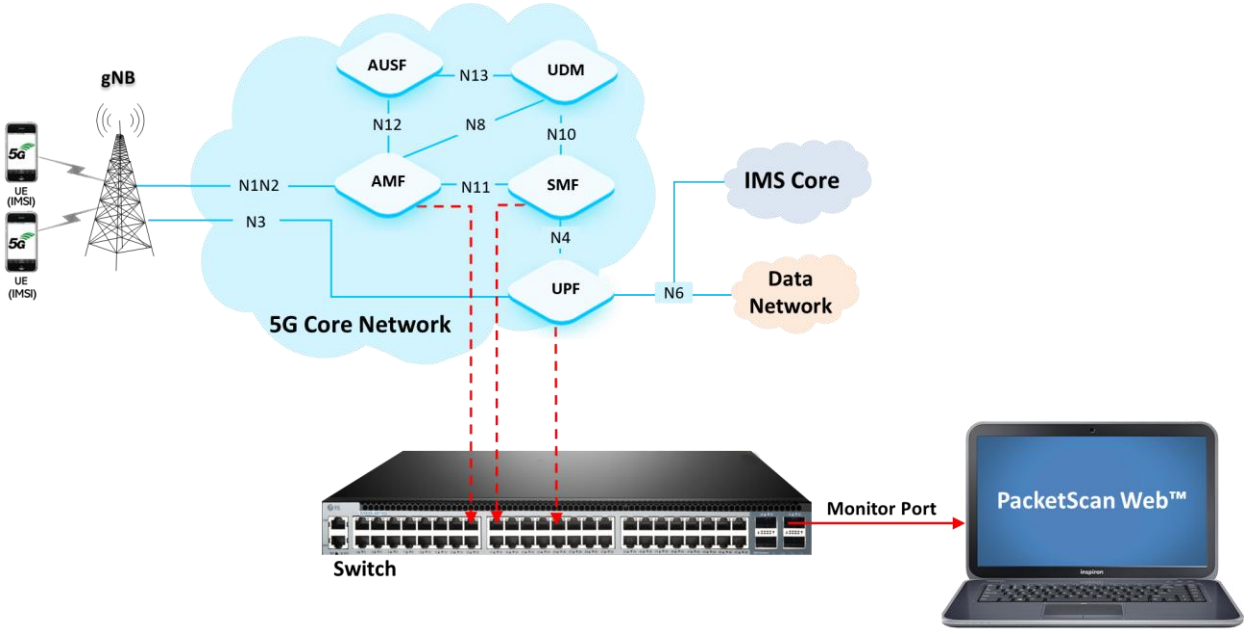
LTE Protocol Analysis

- 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



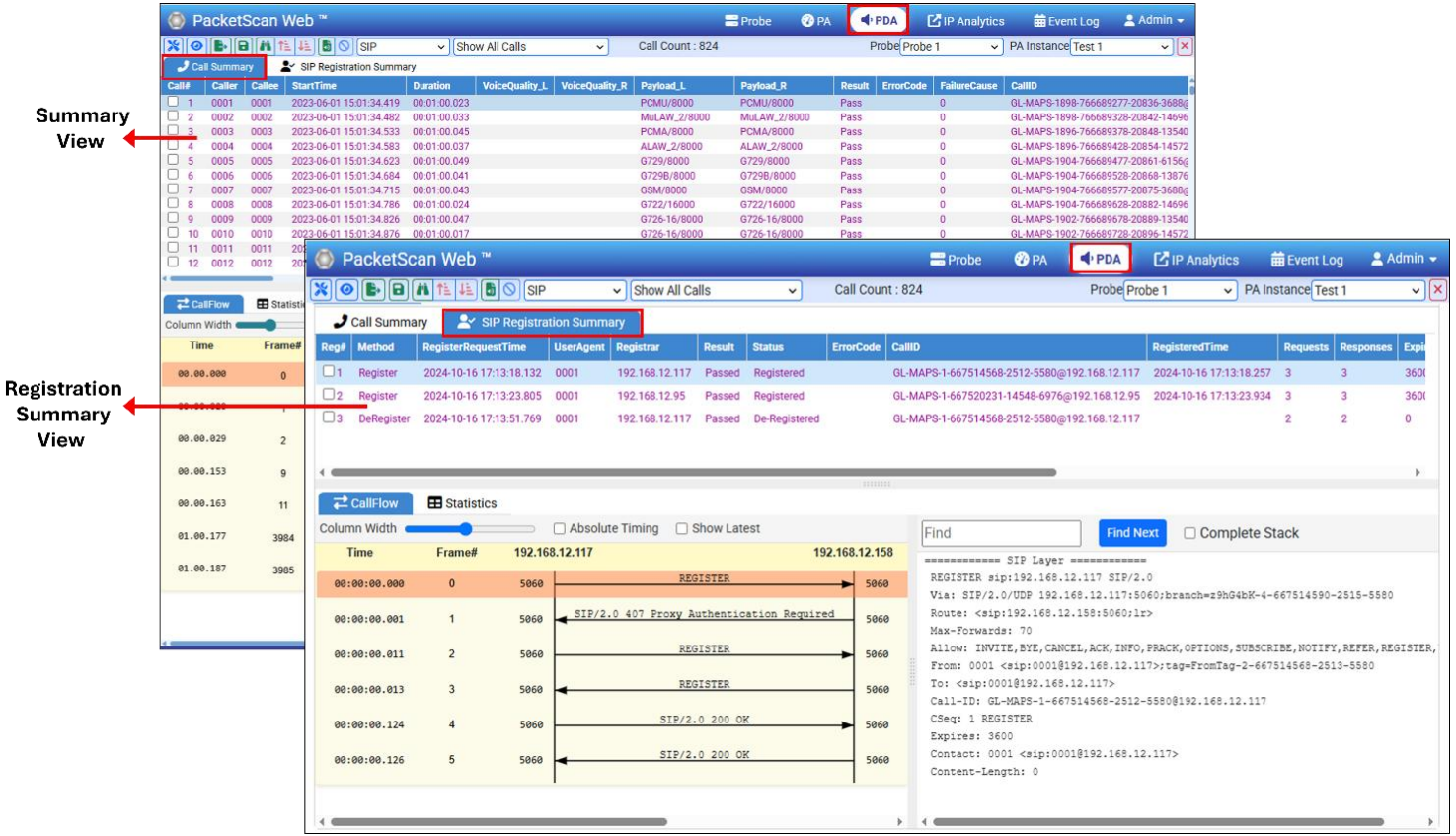
5G Protocol Analysis

- 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



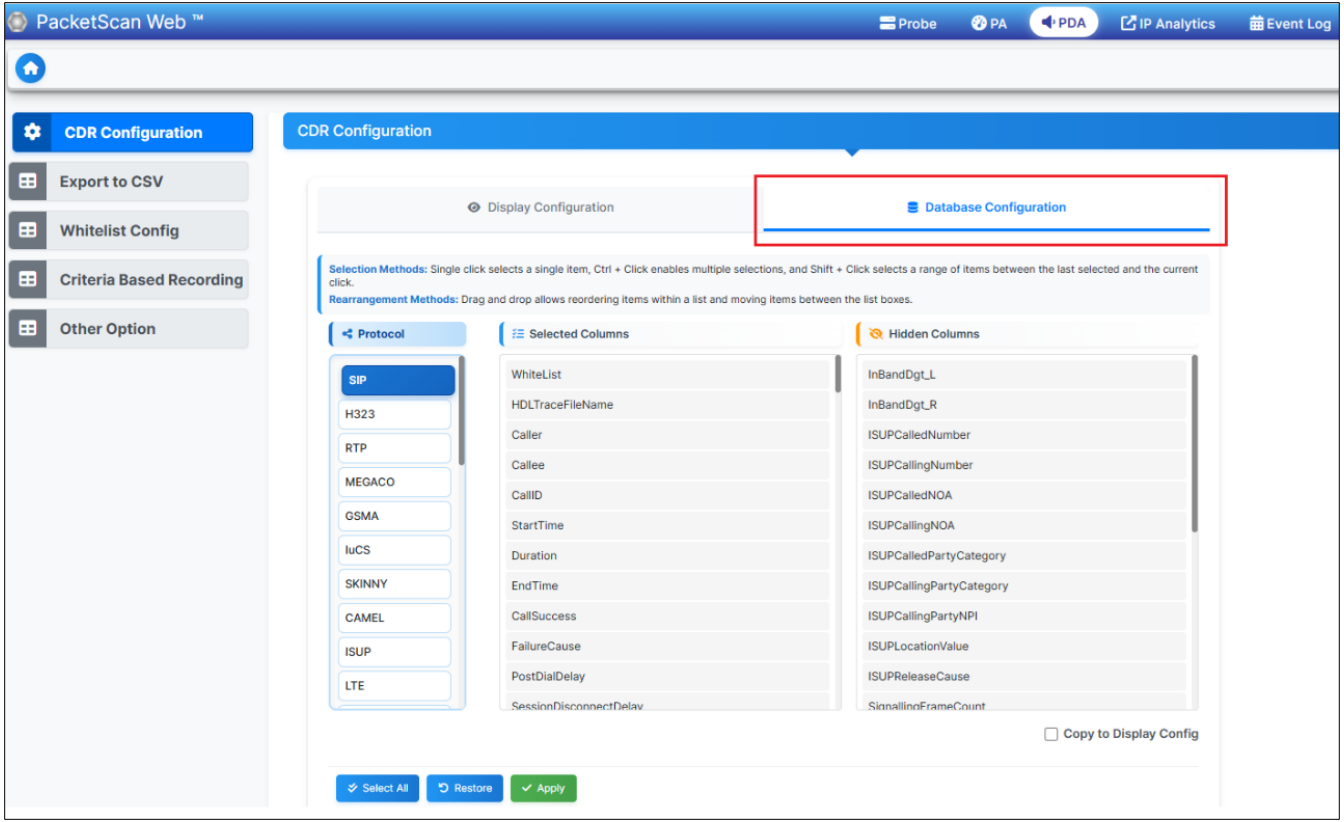
Packet Data Analyzer (PDA)

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



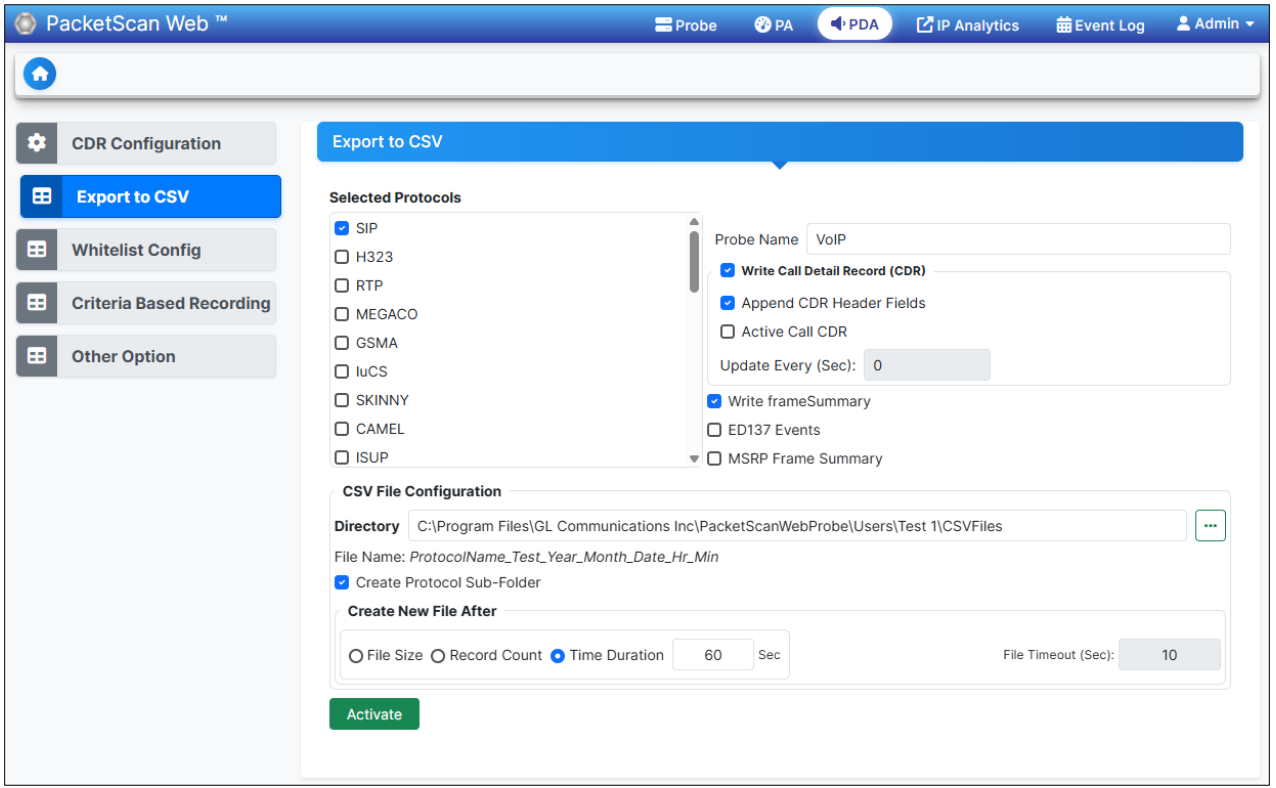
CDR Configuration

- **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



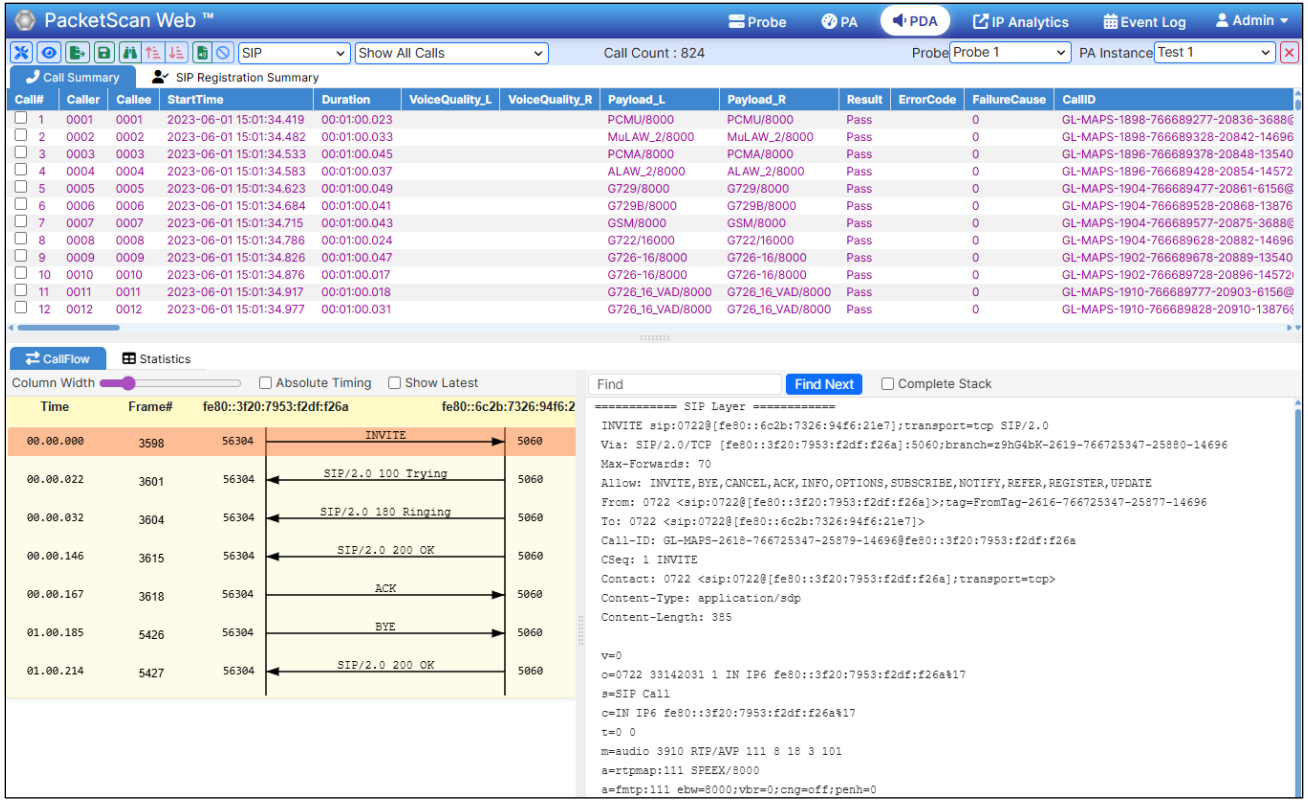
Export to CSV

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



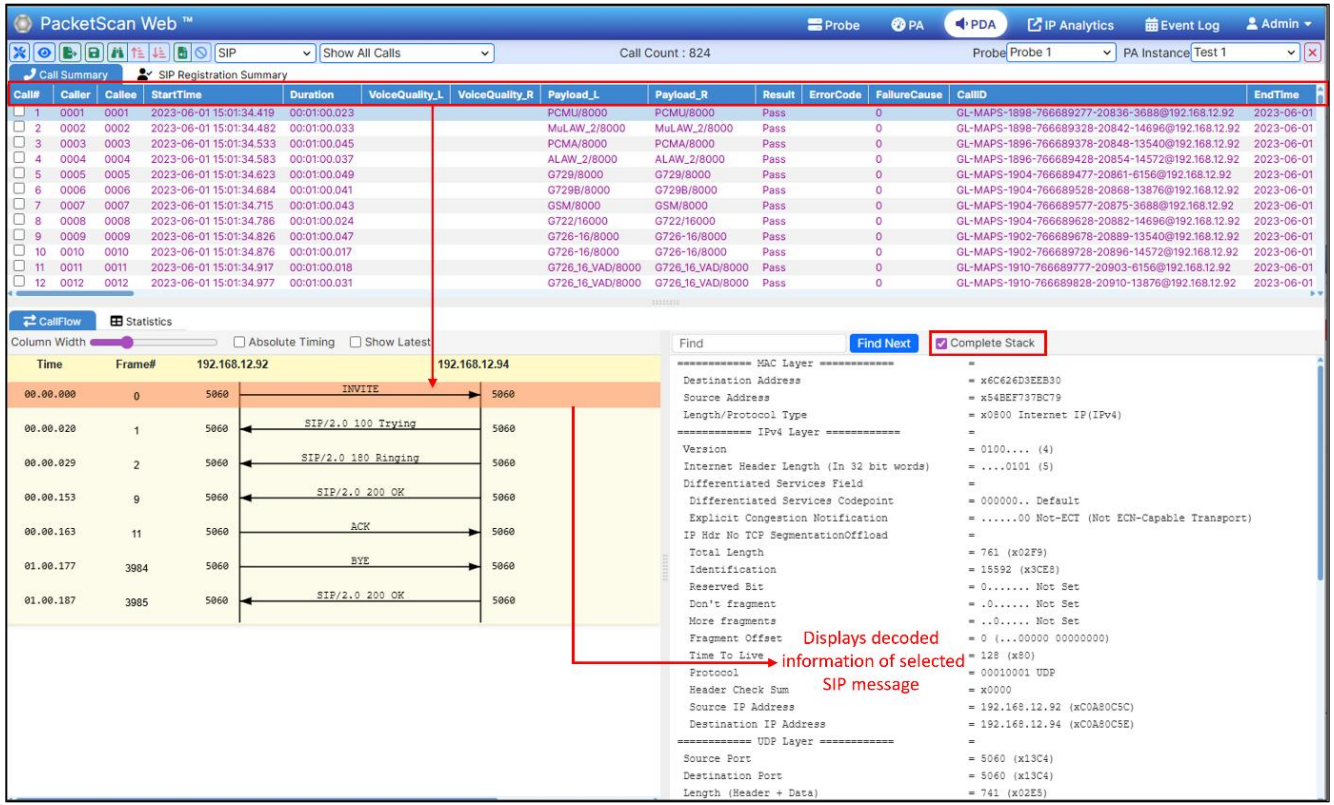
PDA Summary View

- 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



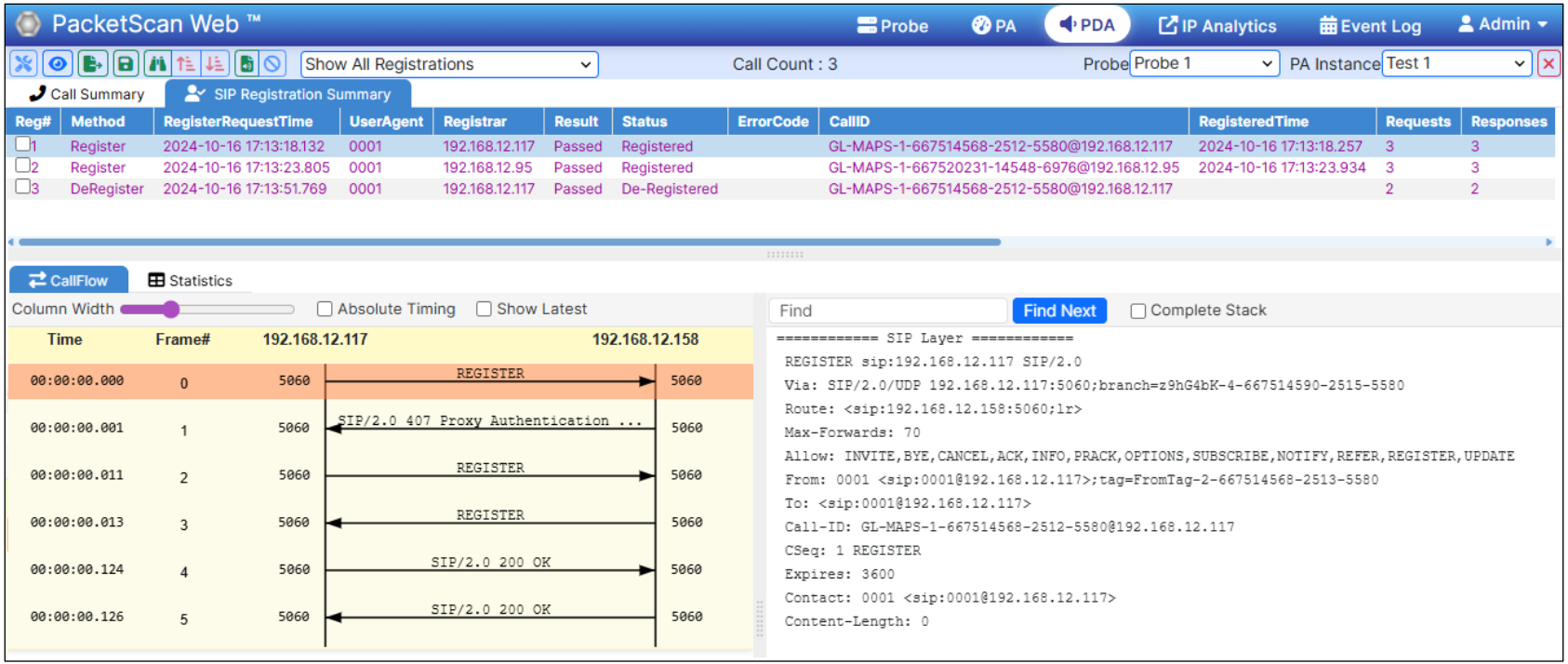
Call Graph – SIP Call

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



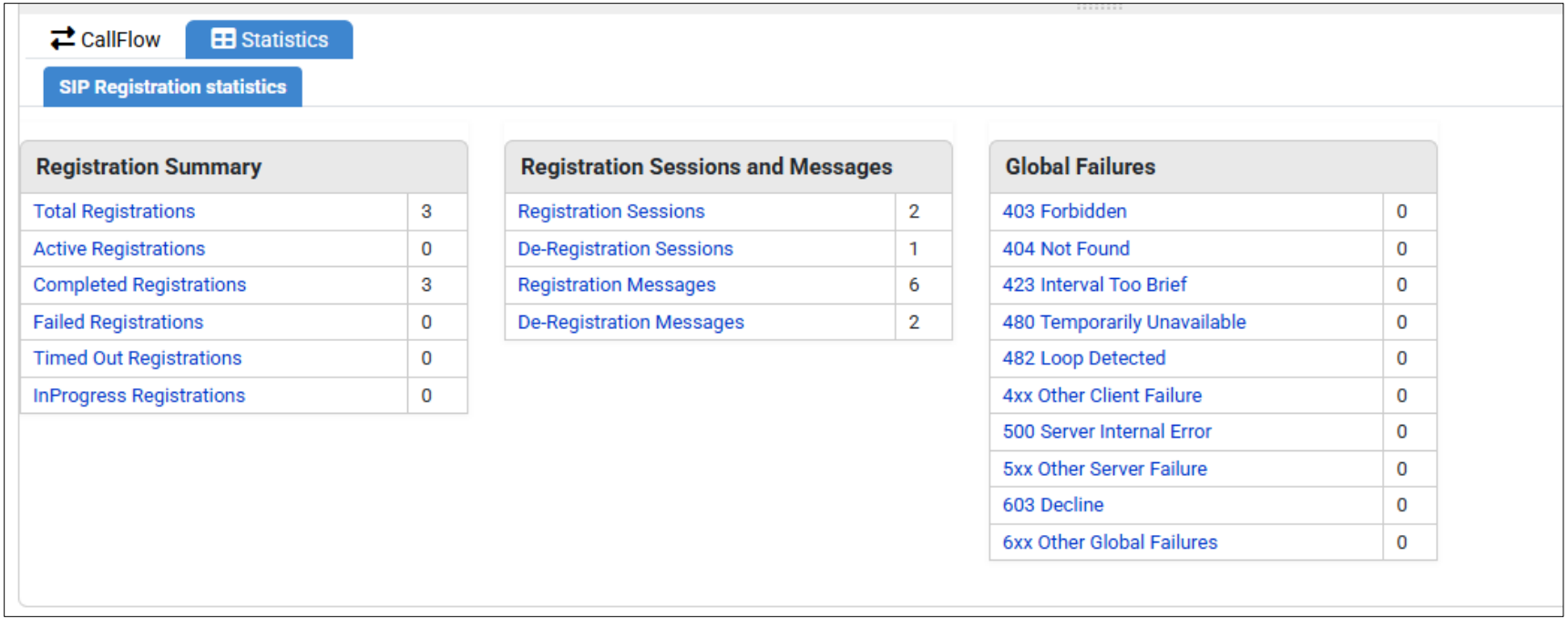
Registration Summary

- 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



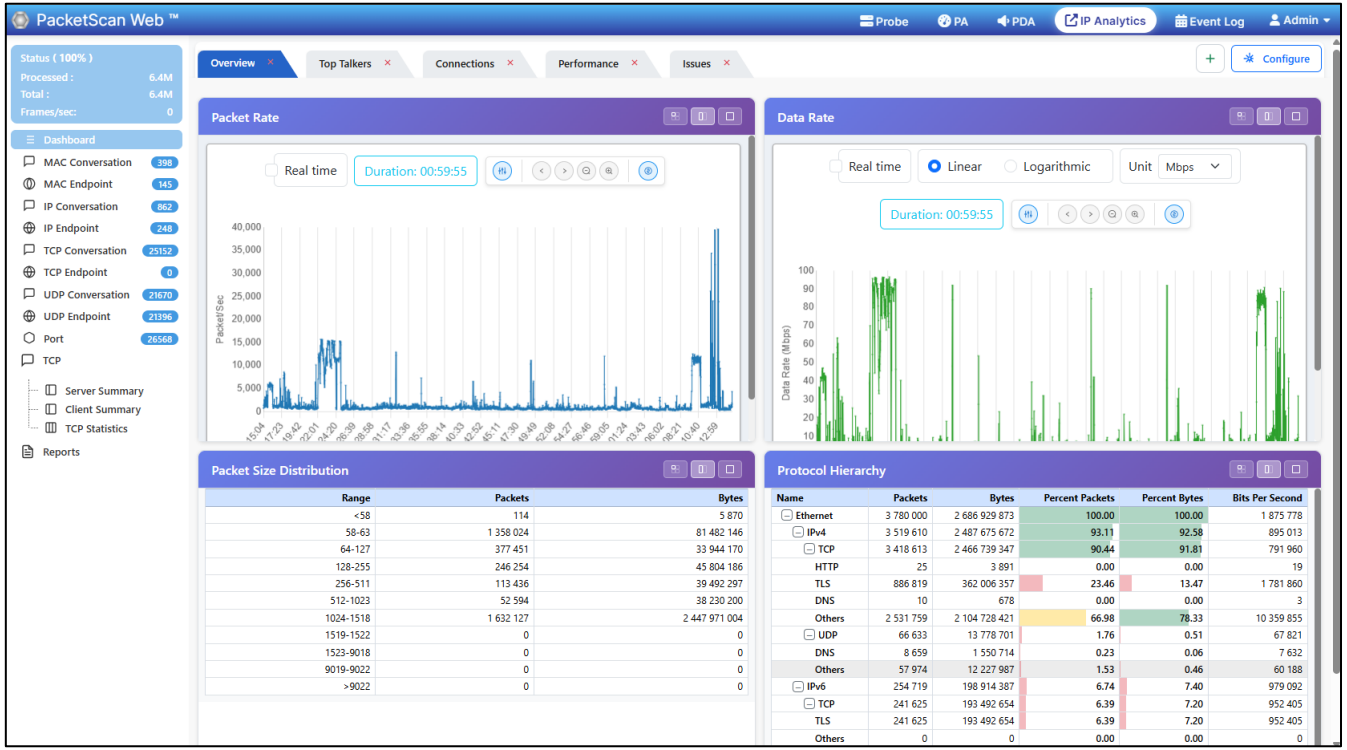
Registration Statistics

- Display the count of the registration details



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