



Using Hardware Accelerated 10-40 Gb/s Packet Analysis in IMS Policy Applications

Executive Summary

Network operators need real-time access to signalling and media content information that is conveyed in their networks. The information is required by sophisticated DPI / policy applications that preserve network health and integrity, and enable new revenue-generating opportunities. To achieve this, passive probes for the collection, identification and analysis of packet media and signalling information must be connected to today's high-speed, IMS networks.

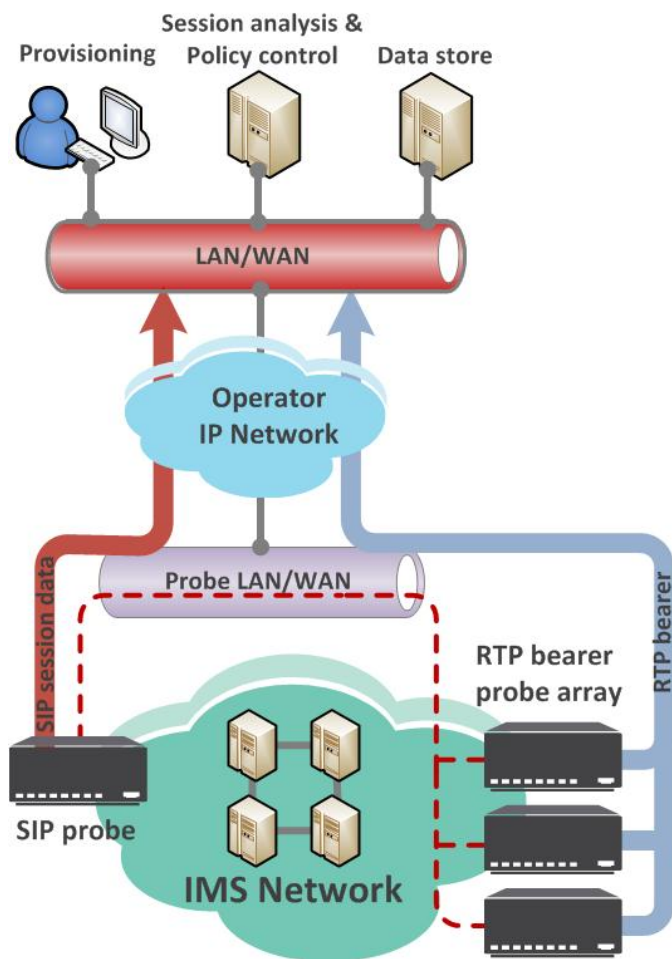


Figure 1 – DPI for IMS SIP session analysis and control

However, current solutions for passive packet capture and filtration are increasingly strained by the burden of access information for many thousands of concurrent call sessions in evolving high capacity networks such as the IMS and LTE/SAE environment. Host-based solutions are unable to keep up with the demands of 40Gb/s or even 10Gb/s high-speed networks.

A solution is to leverage hardware acceleration, in the form of Telesoft Technologies MPAC-IP DPI accelerator card, which performs filtering, processing and collection of signalling and content under the control of a DPI application.

This removes the burden from existing platforms and enables more efficient, scalable probes to be deployed that can meet the demands of high-speed networks and ensure a future proof solution to the needs of network operators and evolving DPI / policy solutions.

This white paper explains how the MPAC-IP DPI accelerator card resolves the challenges of delivering data to DPI applications and explains the process by which on-board filtering and processing is achieved in today's SIP-based networks.

Overview – Monitoring IMS Networks

Deep Packet Inspection (DPI) is an essential tool for preserving network health and integrity. As network traffic growth continues to approach stratospheric levels, network operators are increasingly challenged to manage traffic flows, protect customer experience and troubleshoot potential and actual problems.

In addition to the preservation of network integrity, DPI is also being deployed to deliver innovative, revenue-generating policy services. Policy control will enable the next generation of personalised services, optimised for individual users and subscribers and based on specific offers and charging plans.

DPI relies upon the passive collection, monitoring and analysis of network signalling and media information carried in IP packets, which provide detailed statistics, data and reporting, enabling proactive network management.

As illustrated in Figure 2, IP packets in an IMS network can be monitored using passive taps, located at the Session Border Controllers (SBC), which feed the signalling and media content for the entire visible network to the probes. In this application, the media and signalling on the network are handled by separate physical SBC equipment to manage the processing load. A signalling probe and multiple bearer probes are therefore deployed in order to provide monitoring access to all traffic on the network.

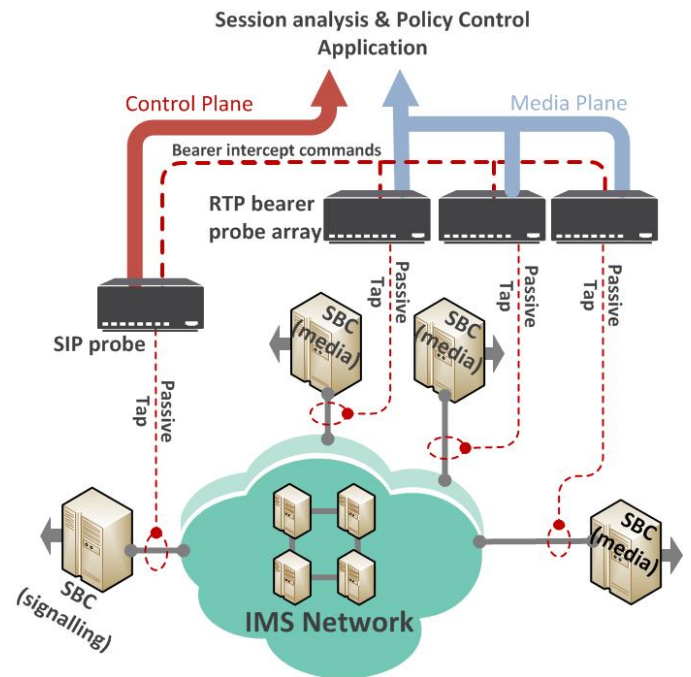


Figure 2 – Analysis and control using passive taps

The information collected is available to DPI application solutions. The DPI applications are integrated into an overall network policy framework, which delivers optimised user experience and manages sessions according to charging and personal profiles.

Functions of the SIP probe:

- Detects any SIP packets passing its network node;
- Compares the SIP sessions against records and profiles established;
- Generates CDRs on selected sessions;
- Analyses the session information (SDP) in SIP packets to identify media sessions; and
- Issues intercept commands to the media bearer probes accordingly.

The network operator provisions the SIP probe over a defined interface.

Functions of the RTP bearer probe:

The RTP media bearer probes compare the traffic received on their monitoring nodes to the intercept commands issued by the SIP probe. The RTP bearer probes deliver any media session packets that match the session list as provisioned by the SIP probes to the user network.

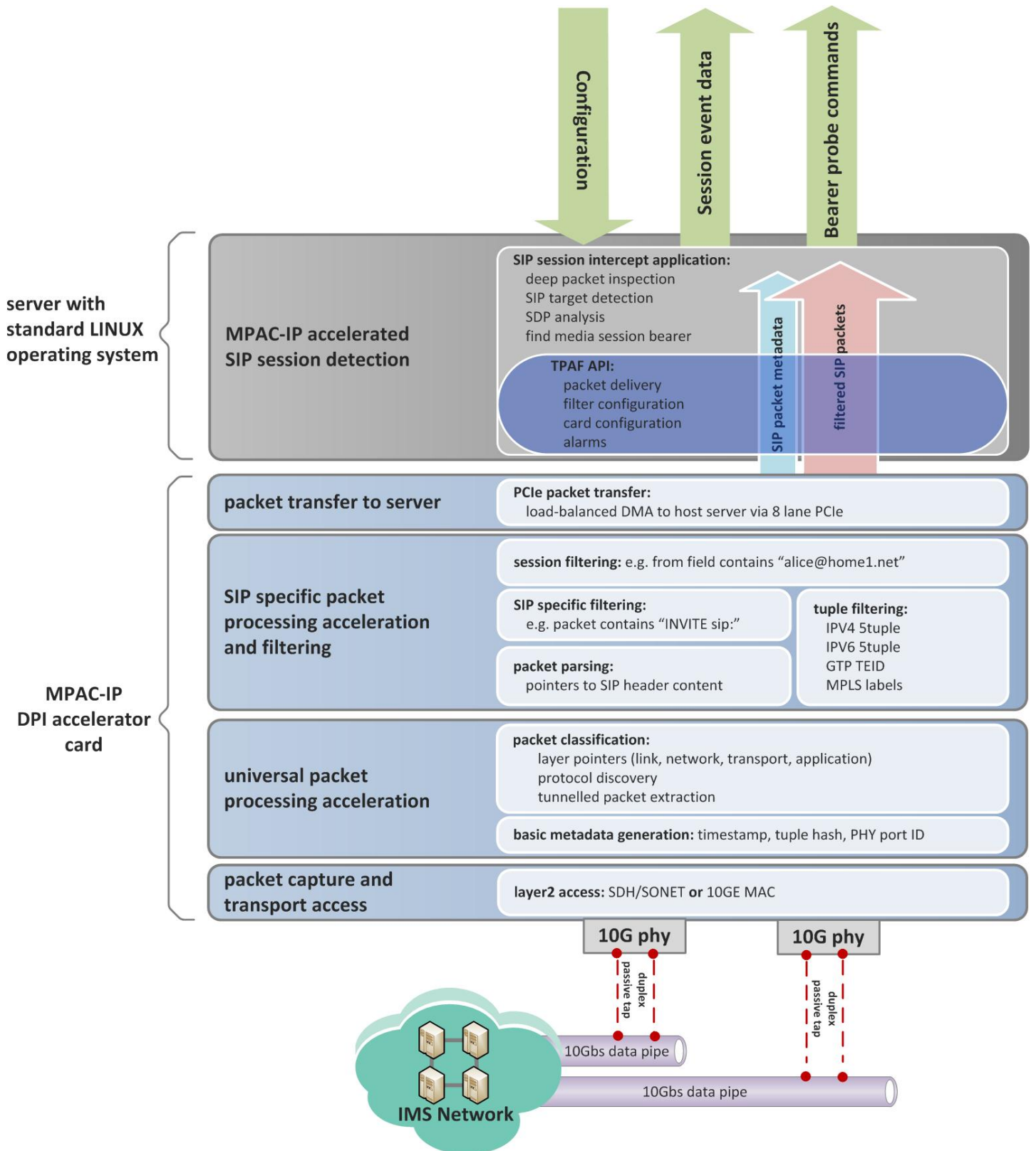


Figure 3 – MPAC-IP Hardware-Accelerated SIP Probe

MPAC-IP Hardware-Accelerated SIP Probe

The text box opposite lists the key requirements for an IMS monitoring system.

The SIP probe is connected to 40Gb/s or 10Gb/s monitored network via duplex passive taps. It consists of a SIP Deep Packet Inspection (DPI) analysis application running on a Commercial, Off-The-Shelf (COTS) server, with Telesoft's 40Gb/s 10Gb/s MPAC-IP card providing packet access, filtering, and DPI acceleration. This architecture is illustrated in Figure 3.

The SIP DPI application has to detect any SIP sessions related to its configured list, process them for media bearer identification and generate the session event data, CDR, and bearer control messages. At 10G/s, inspecting every packet against a session list is not practical on a COTS server because the processing requirements punish even the most capable standard processors. At 40Gb/s, it is impossible for COTS processors to keep pace with traffic load.

The proposed system solves this problem using the MPAC-IP DPI accelerator card to offload much of the packet processing requirements from the application.

The MPAC-IP DPI accelerator card executes this offload in four stages:

- Packet capture and transport access;
- Universal packet processing acceleration;
- SIP specific packet processing and filtering; and
- Packet delivery using DMA to the DPI application through the TPAF API

IMS Monitoring Key Requirements

Capture every packet on the network node

De-frame Layer 2 (e.g. align to and remove SDH framing)

De-tunnel network data (e.g. disregard GTP tunnel headers to get to user IP datagrams)

Identify the different layers within the IP packet

Identify all SIP packets, and discard anything else

Group SIP packets from common communication sessions

Timestamp SIP packets

Parse - i.e. find the useful information within - the SIP packets

Track SIP session states

Generate CDR for all SIP sessions

Compare the SIP URI against the session list

Generate IRI for SIP sessions

Ascertain media session details from SIP sessions

Generate media session intercept commands

Stage 1: Packet Capture and Transport Access

At stage 1, the MPAC-IP card aligns to the layer 2 protocol using Ethernet or PoS framing, and captures every packet on the network node. In the PoS case, the MPAC-IP card extracts IP packets from whatever format they're carried – (e.g. ATM, PPP, or raw Ethernet over SDH). In the Ethernet case, the MPAC-IP card captures complete Ethernet packets for processing and delivery.

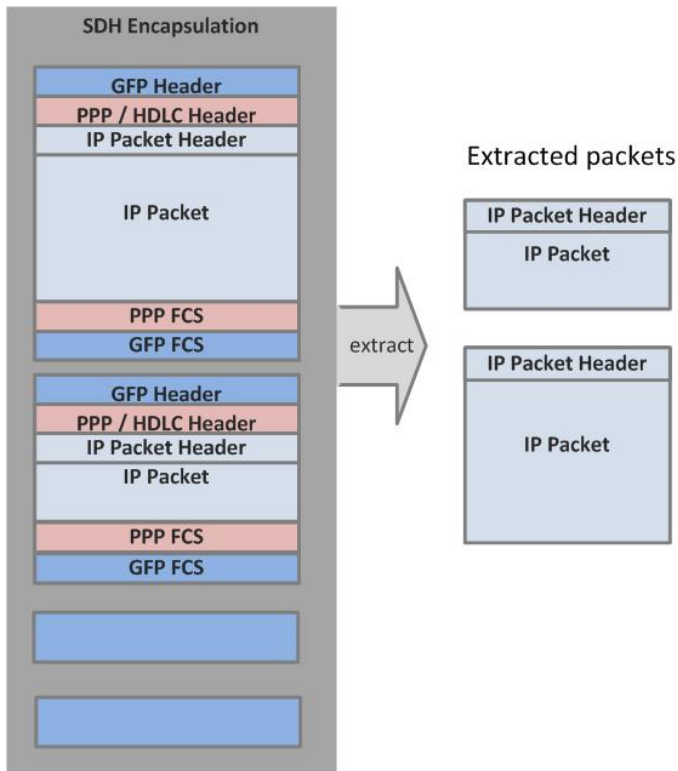


Figure 4 – Packet Capture and transport Access

Stage 2: Universal Packet Processing Acceleration

At stage 2, the MPAC-IP card maps and classifies the protocol for each packet it receives (See Figure 5-1), generates a precision timestamp and generates a hash code to group packets from common flows (See Figure 5-2).

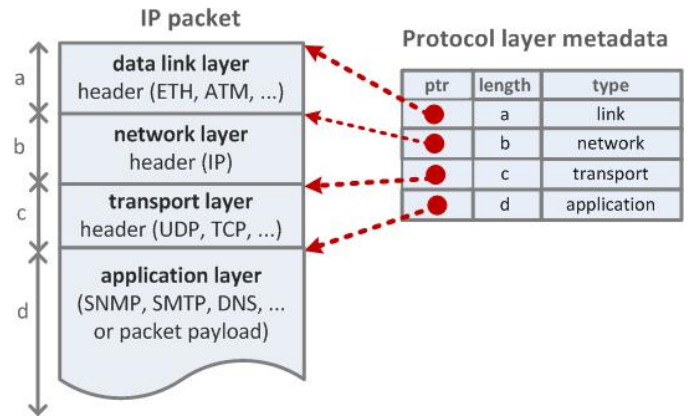


Figure 5-1 – Packet Classification

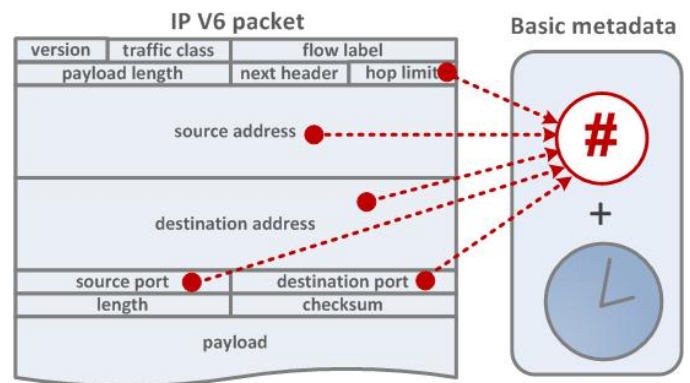


Figure 5-2 – Generating timestamp and hash

Stage3: SIP Processing Acceleration and Filtering

The MPAC-IP card's stage 3 processing layer filters packets to ensure that only interesting packets are delivered to the DPI application. When each packet arrives at the stage 3 processing layer, the MPAC-IP card compares it against a list of criteria defined by the DPI application. Parsing the SIP packets, it also aids the DPI application to track SIP session state

Example application: Monitor SIP sessions initiated by specified uri

For this example application, it is required to intercept any SIP communication sessions initiated by the user "alice@home1.net". There are perceived issues with session quality experienced by the user and the network operator needs to determine a solution.

The implementation illustrates how the DPI application configures the MPAC-IP card to deliver only relevant packets to enable this interception using minimal host CPU resources

The intercept is achieved through a number of stages:

1. Detect the start of any SIP session associated with alice@home1.net
2. Select only sessions initiated by alice@home1.net
3. Monitor the state of the SIP session

Figure 6 illustrates the filtering stages implemented by the MPAC-IP card.

Stage 1

First, the DPI application needs to detect the start of any SIP session associated with user alice@home1.net. It does this by detecting every SIP INVITE packet involving alice@home1.net.

One method is to pass every packet up to the application, allowing the software to search through all of the data; however, this obviously wastes valuable CPU resources, and is not practicable at high line data rates. The solution is for the application to off-load the required processing by configuring the MPAC-IP card to detect and deliver packets only containing both "INVITE sip:".

Stage 2

To identify outbound sessions from alice@home1.net the DPI application has then to make sure that the "from" field in the SIP packet contains the "alice@home1.net" URI.

To enable rapid access to this variable position and variable length field in the SIP message, the MPAC-IP card parses any SIP packet it delivers to identify the locations of the SIP header fields. When the DPI application receives the packet matching "INVITE sip:", the packet includes a **metadata** list that includes a list of pointers, offsets and lengths to variable length SIP header fields.

The software application can then quickly access the "from" header field indicated in the metadata delivered by the MPAC-IP card and check that this contains the "alice@home1.net" string. The check is simplified by being at a known offset from the start of the packet, and being for a known length

Stage 3

Once the start of the session from alice@home1.net has been detected, the application needs to see all other packets in the same flow in order to track the session state.

It does this by configuring the MPAC-IP card to deliver all - or a finite number of subsequent packets within the same bidirectional IP 5tuple flow as that which contained the invite from alice@home1.net.

In the 'all subsequent packets' case, the DPI application clears the 5tuple filter once the session is ended. (*note: in certain network configurations, the reverse flow may need to be detected separately).

The DPI application then receives all packets for the SIP session, and keeps track of the session state, aided by the MPAC-IP card parsing the packets to minimize CPU requirements

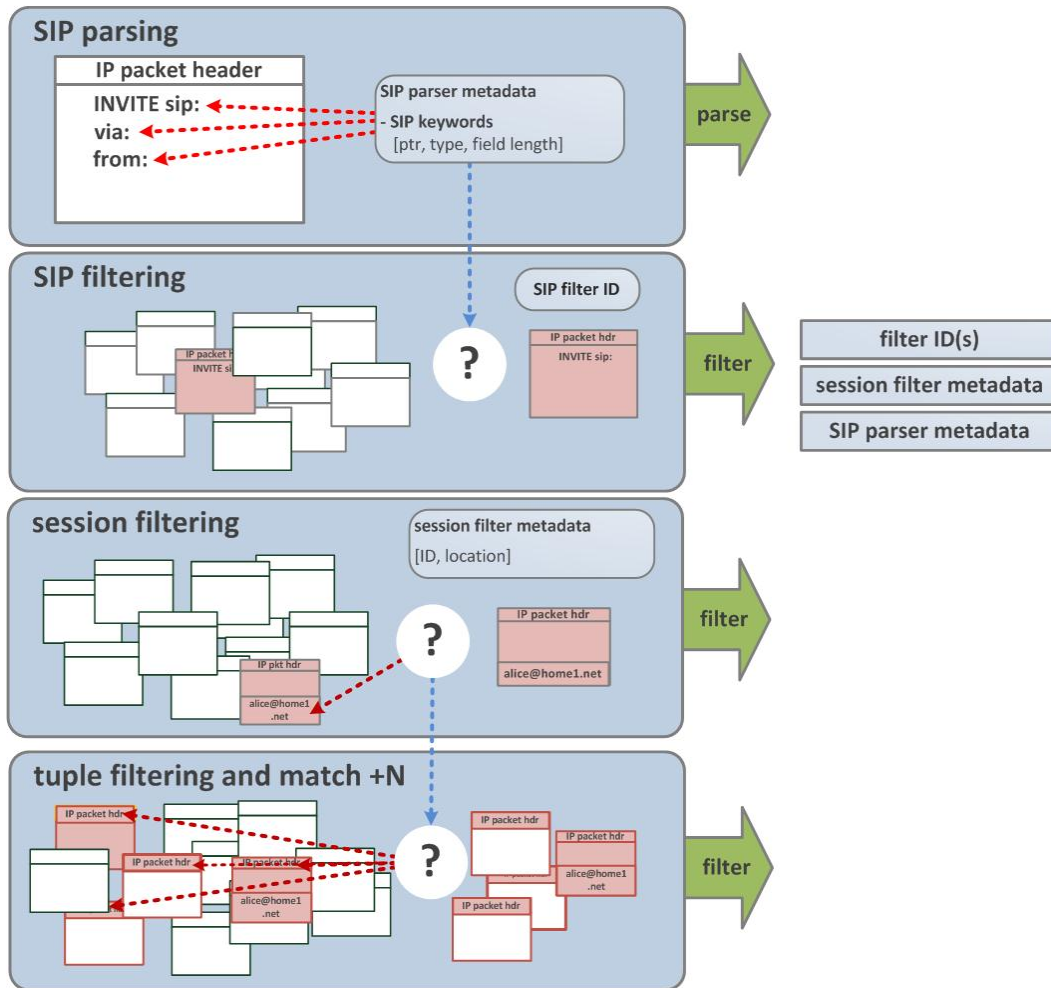


Figure 6 – Example SIP Monitoring Application

DMA Packet Transfer to Server via PCIe

Once the MPAC-IP card has filtered and pre-processed the packets, it needs to deliver them, along with their associated metadata, to the DPI application running on the host server. To minimize CPU requirements on the host server, the MPAC-IP card writes directly to packet-monitoring queue memory on the host server using a DMA mechanism. To facilitate load-balancing and to group packet flows, the DPI application configures the MPAC-IP card to distribute packets to different queues according to the 5tuple hash of each packet.

SIP Session Intercept Application

The DPI application configures, manages, monitors, and receives packets and associated metadata from the MPAC IP card using the TPAF API library. Accelerated by the card, it must analyse any potential SIP sessions, generate session event data, and extract media session information from the SIP packet content. For any media sessions it identifies, the SIP session intercept application sends a message to the RTP bearer probe array to intercept the session based on its IP addresses and UDP ports.

Conclusion

The collection of information from communications networks that is required by DPI applications has become increasingly complex. Filtering, processing and delivering signalling and media content from large numbers of concurrent sessions to DPI applications from high-speed (10Gb/s +) SIP-based networks is too demanding for host-based processing systems. The inclusion of the MPAC-IP DPI accelerator card relieves the host CPU of this burden and provides a more efficient means of capturing and processing data required for the purpose of DPI applications.

By integrating the MPAC-IP DPI accelerator card into probes for DPI applications, network operators can deploy highly scalable probe solutions that can filter and capture of many thousands of concurrent sessions on high-speed NGN IMS networks in real-time.

Where **innovative thinking**
meets **engineering excellence**

Telesoft Technologies Ltd,
Observatory House,
Blandford, Dorset DT 11 9LQ UK

T. +44 (0)1258 480 880
F. +44 (0)1258 486 598
E. sales@telesoft-technologies.com

Telesoft Technologies Inc.
Suite 601, 4340 Georgetown Square,
Atlanta GA 30338 USA

T. +1 770 454 6001
F. +1 770 452 0130
E. salesusa@telesoft-technologies.com



Telesoft Technologies Ltd (Branch Office),
Building FC-24, Sector 16A, Noida 201301,
Uttar Pradesh, India

T. +91 120 466 0300
F. +91 120 466 0301
E. salesindia@telesoft-technologies.com