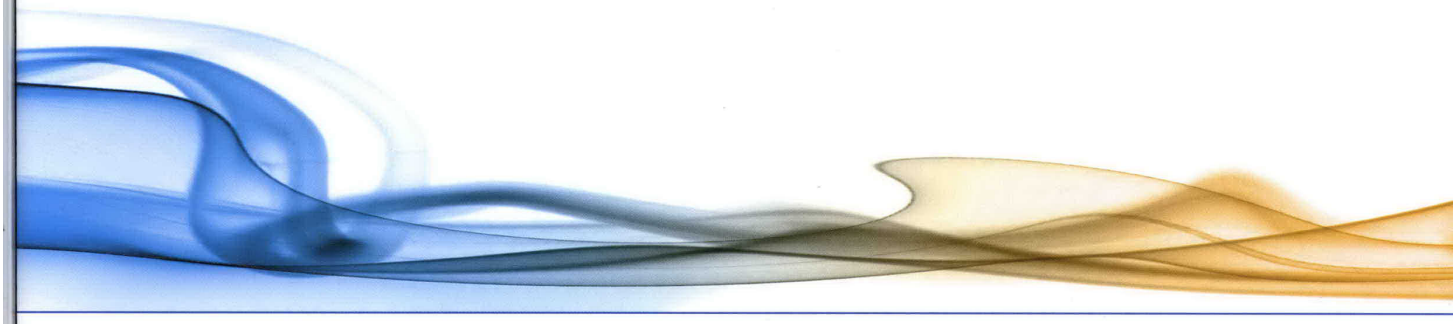
Utimaco
LIMS Access Points

Realtime Network Monitoring for Lawful Interception and Data Retention



utimaco®
a member of the Sophos Group


LIMS Access Points

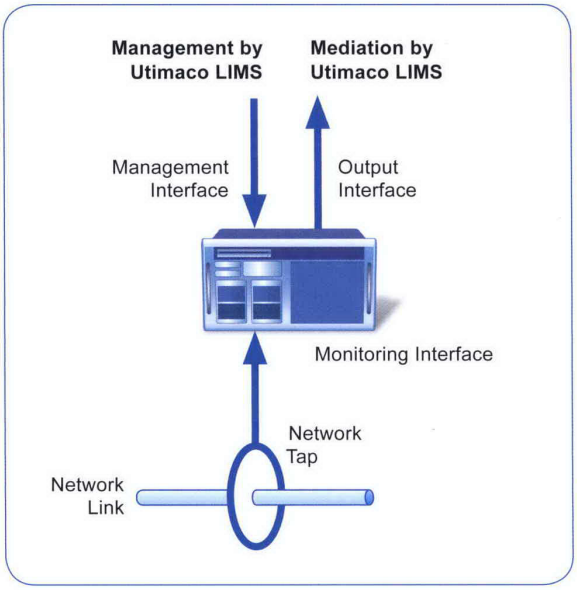
Realtime Monitoring
with Passive Probes

Realtime monitoring of network connections has been used by telecom operators for years for various purposes, like quality of services monitoring, performance analysis, fraud detection, E911 location and billing. Specialized network probes are typically connected to the network by taps, thus receiving a copy of the communications traffic. These probes analyze the traffic based on defined filter rules and can extract data of specific interest.

Law enforcement and intelligence agencies make use of passive probes for non-intrusive surveillance of communication links. Compared to the common approach of active monitoring, where network nodes, e.g. switches or routers, acquire the required data, probes have a number of advantages with regard to:

- Performance, bandwidth support
- Capacity, number of simultaneous targets/filter rules
- Transparency
- Accuracy, level of details

Telecom operators and Internet service providers sometimes prefer network probes for similar reasons. That`s why probes are an integral part of the Utimaco Lawful Interception Management System (Utimaco LIMS™) and of the Utimaco Data Retention Suite (Utimaco DRS™).



Utimaco provides three types of probes:

LIMS Access Points for IP services	Cost-effective probes for single IP services like e-mail, VoIP, AAA, SMS, MMS
LIMS Access Points DPI	Deep Packet Inspection Probes for 1Gb to 10Gb Ethernet networks
LIMS Access Points TDM	Probes for circuit-switched networks based on E1/T1, SDH/SONET (STM-1 to STM-4)

LIMS Access Points are centrally controlled by the Utimaco LIMS and Utimaco DRS. All data intercepted by the probes are encrypted and protected from unauthorized access. Before data is handed over to law enforcement agencies it is mediated to comply with international LI standards.

Deep Packet Inspection

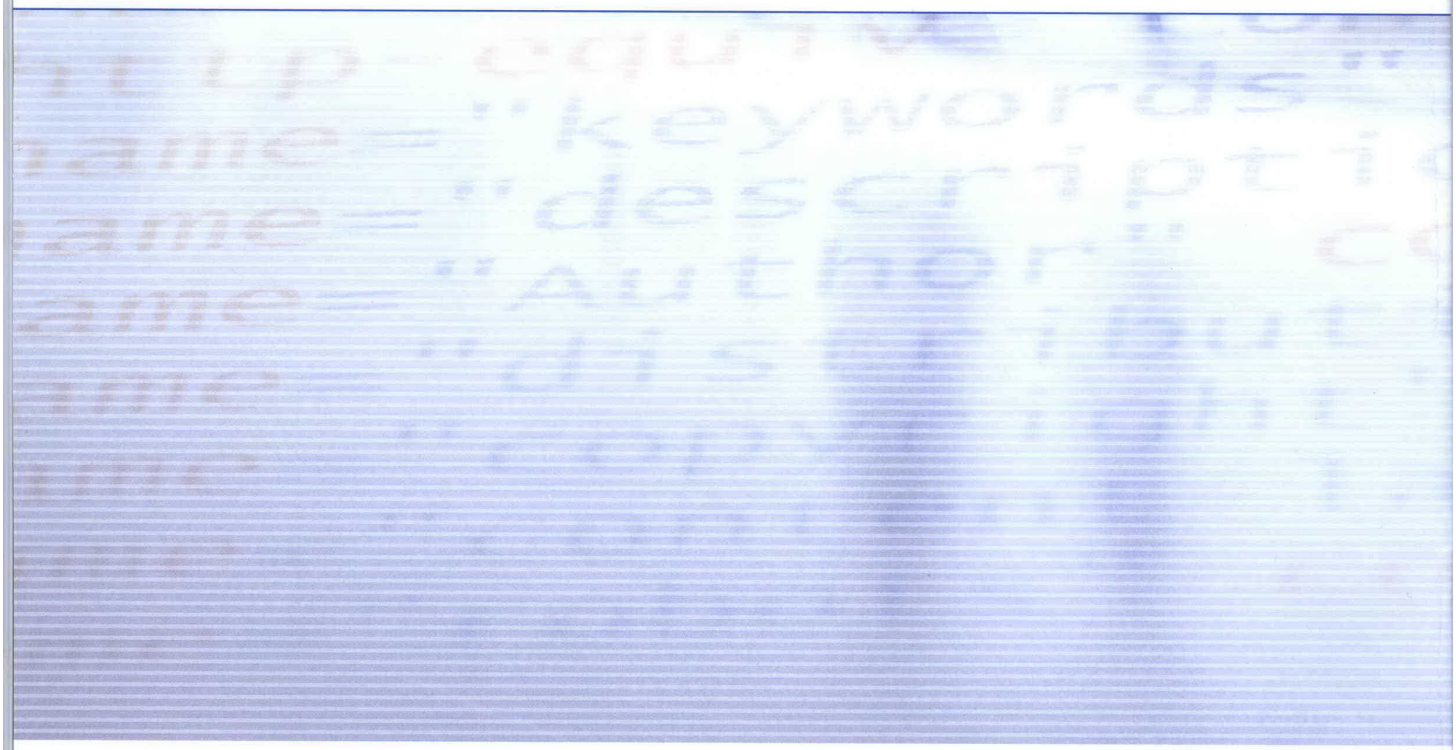
Deep Packet Inspection (DPI) is the name of a state-of-the-art technology designed to meet some of the key challenges relating to the plethora of IP-based communication services. The ever-growing number of Internet applications and IP-based protocols make it hard for law enforcement agencies (LEAs) and communication service providers to identify 'bad guys' or criminals on the net and to analyze their communications for the purpose of criminal investigations and prevention of terrorism.

Utimaco LIMS Access Points implement DPI technology not only to filter individual IP packets but also to decode and analyze complete communications flows of more than 300 different Internet applications. The probes can either extract only the metadata (e.g. source ID, destination ID, IP addresses, port numbers, timestamps) or intercept entire communication sessions. Intercept targets can be identified by a range of application specific user IDs, device IDs, network addresses or by keywords.

Utimaco offers a variety of carrier-grade probes for different networks and services. Customers can select from a range of LIMS Access Points according to their actual needs for performance, protocol support and scalability.

Supported services and protocols

- Networking protocols
  IPv4, IPv6, TCP, UDP, Ethernet, EtherIP, FTP, HTTP
- Tunneling protocols
  MPLS, GRE, L2TP, PPP, PPTP, GTP
- AAA protocols
  RADIUS, DHCP
- E-Mail
  POP3, SMTP, IMAP, MAPI
- Webmail
  Yahoo mail, Microsoft Hotmail, google mail, Maktoob, OWA
- VoIP
  SIP, RTP, H.323, SCCP
- Signaling
  SIGTRAN, MTP, MAP, SCCP, RANAP
- and many more Internet applications



LIMS Access Points DPI

Realtime Monitoring of IP Networks

Deep Packet Inspection

In contrast to many other network probes, Utimaco LIMS Access Points do not just filter IP packet headers on well-known ports but reassemble complete IP flows in order to analyze the header fields and the content of more than 300 IP-based protocols and Internet applications. By carrying out semantic analysis, the LIMS Access Point can track control connections that induce dynamically negotiated connections on temporary ports such as passive FTP, VoIP or full multi-media conferencing streams, gnutella or BitTorrent peer-to-peer traffic and instant messaging, and is able to automatically decode complex encapsulation tunnels.

Lawful Interception and Data Retention

Utimaco LIMS Access Points are fully integrated in the Utimaco LIMS (Lawful Interception Management System) and Utimaco DRS (Data Retention Suite). Intercept targets can be provisioned centrally in LIMS and will then be distributed to all connected LIMS Access Points for interception. For data retention purposes the probes can generate IPDRs (IP data records, or metadata) for all IP services or for those of specific interest. These IPDRs are sent to the Utimaco DRS for further processing and storage.

Models

LIMS Access Point for IP services
- 4x1Gb Ethernet (copper)
- up to 100kpps
- E-Mail
- AAA
- VoIP
- Mobile data

LIMS Access Point DPI 1G
- 4x1Gb Ethernet (fiber or copper)
- up to 800kpps
- HW accelerated data aquisition
- Multi-protocol support

LIMS Access Point DPI 10G
- up to 4x10Gb Ethernet (fiber or copper)
- up to 4,000kpps
- HW accelerated data aquisition
- stackable
- Multi-protocol support