Utimaco

LIMS Access Points

Realtime Network Monitoring for Lawful Interception and Data Retention

utimaco®

a member of the Sophos Group


LIMS Access Points

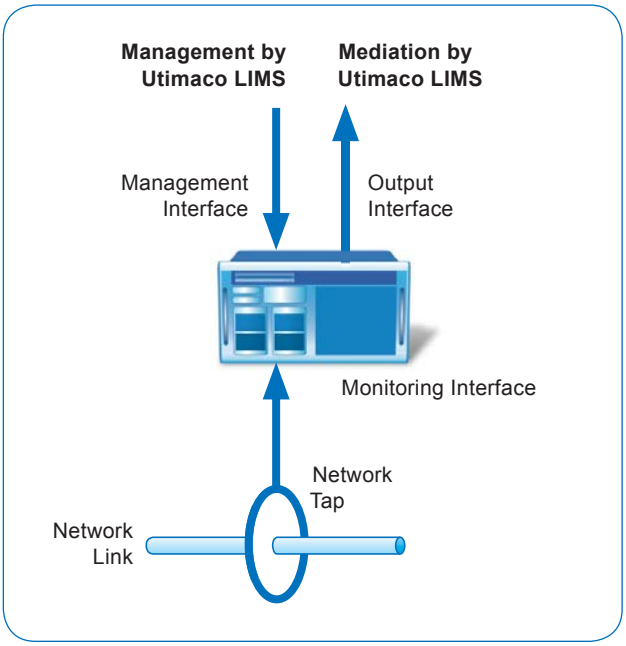
Realtime Monitoring
with Passive Probes

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

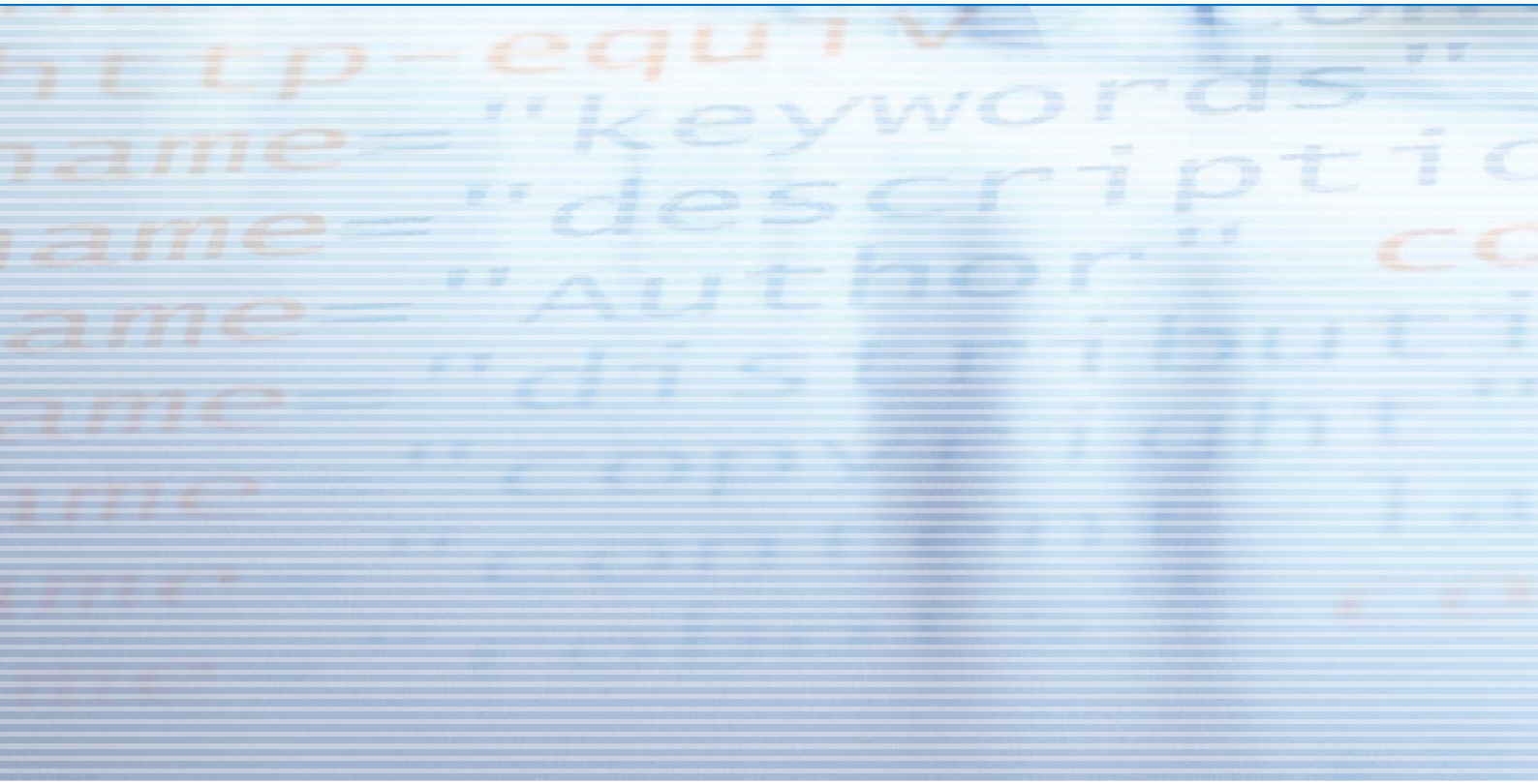
Deep Packet Inspection (DPI) is the name of a state-of-the-art technology designed to meet some of the key challenges relating to the plethora of IP-based communication services. The ever-growing number of Internet applications and IP-based protocols make it hard for law enforcement agencies (LEAs) and 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

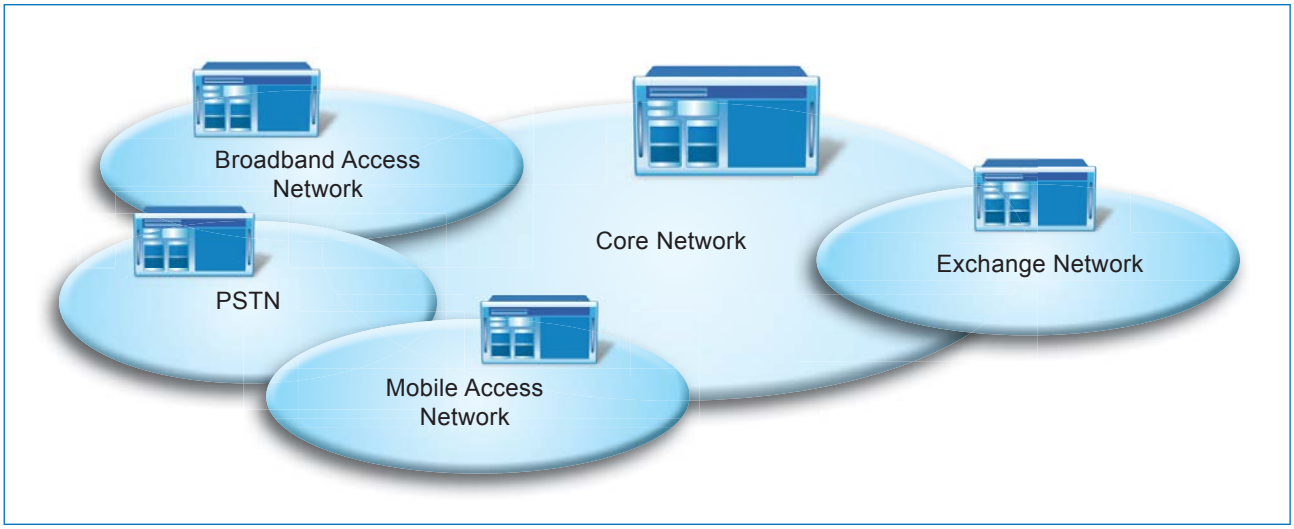
- Networking protocols
  IPv4, IPv6, TCP, UDP, Ethernet, EtherIP, FTP, HTTP
- Tunneling protocols
  MPLS, GRE, L2TP, PPP, PPTP, GTP
- AAA protocols
  RADIUS, DHCP
- E-Mail
  POP3, SMTP, IMAP, MAPI
- Webmail
  Yahoo mail, Microsoft Hotmail, google mail, Maktoob, OWA
- VoIP
  SIP, RTP, H.323, SCCP
- Signaling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



LIMS Access Points are designed for non-intrusive monitoring without alerting subscribers or disrupting the service. The probes can be seamlessly integrated into networks of various kinds, such as broadband access networks, IP core networks, or Internet exchange networks. Common network access techniques such as passive taps (splitters) or switch span ports help ensure that there is no outgoing traffic from the IP probe back to the network.

Keeping Pace with New Types of Traffic

Internet applications are constantly evolving. Regularly, new communications applications appear on the Internet and established application protocols are modified. So customers must be prepared to keep pace with this evolution. To this end, Utimaco provides support plans that give customers access to quarterly protocol updates and new protocol plug-ins. Such plug-ins can also be customized according to individual customer needs.



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 multimedia 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

High-Speed Monitoring

Utimaco offers a range of probe models to meet customer requirements in terms of performance, capacity, and price. There are small appliances with a 100/1000 Mbit interface and single protocol support as well as blade-server systems with multiple 10 Gbit interfaces and sufficient capacity to monitor many protocols and thousands of targets simultaneously. All models are designed to provide line-speed performance with zero packet loss. Blade systems can be expanded by means of additional line cards and processor cards to accommodate growing network capacity.

Flexible Target Identification

LIMS Access Points can identify targets by various kind of triggers related to a certain protocol or service. A target ID can be an IP address, MAC address, user ID, device ID, SIP-URL, TEL-URI, email address, URL, MSISDN, IMSI, IMEI, a keyword, or several other application-level IDs. A virtual ID manager correlates target IDs of different protocols and applications in order to capture all relevant traffic associated with a certain intercept target. For instance, a MAC address monitored in the DHCP traffic can be automatically correlated to the associated IP address to capture all IP traffic, a SIP-URI can be mapped to an IP address to capture all RTP traffic, or an instant messaging login can be mapped to the IP address to intercept all IP traffic to and from such a target. For investigators, this feature represents a great new tool for identifying the communications of a person under surveillance even when the information available for identification is limited.

Interception of Ongoing Sessions

LIMS Access Points keep track of all online users authenticated via the DHCP, RADIUS, or GTP protocol. This feature enables intercepts to start immediately, even if a target user has been authenticated before the intercept is activated.

Protocol Updates

As new Internet applications emerge and communication protocols change, network operators must be prepared for changes and updates. Utimaco offers support plans that include free updates for new versions of protocols at predictable costs.

Security & Availability

Utimaco LIMS Access Points are designed to protect data from unauthorized access and to provide timely, secure delivery to the law enforcement agencies. Security features include full audit trails, communication encryption, access control, operating system hardening, automatic consistency checks and alarms. The probes are continuously monitored by the Utimaco LIMS or Utimaco DRS system and can support redundancy concepts with hot-standby functionality.

Compliance

Utimaco LIMS mediates and delivers intercepted communications in compliance with ETSI standards, CALEA, and other national lawful interception mandates. Utimaco DRS retains the data generated by the LIMS Access Points and provides controlled access to such data in accordance with national data protection and data retention laws.

Monitoring Telephony Networks

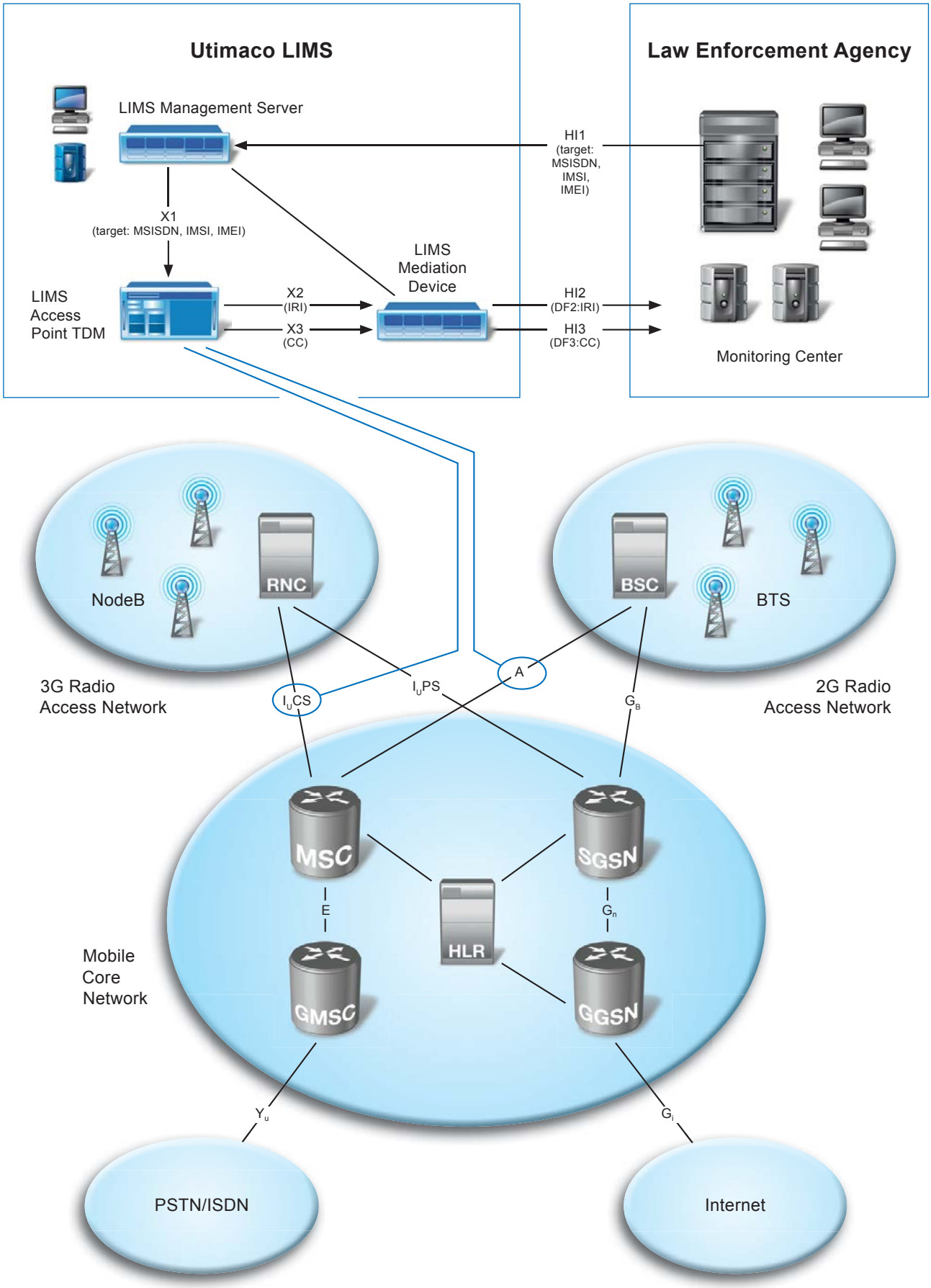
Circuit-switched connections are still widely deployed in modern telecom networks to carry telephone calls, fax or SMS messages. When monitoring a standard PSTN network or a 2G or 3G cellular network for interception purposes, passive probes offer a worthwhile alternative to on-switch interception. Probes can either enhance the interception capabilities of switching systems or replace the integrated interception functionality of switches entirely.

Benefits

- Highly scalable
  from one to thousands of circuits, up to 100,000 simultaneous targets
- 100% transparent
  no impact on existing network links
- Mass intercept
  monitors all calls and messages and generates CDRs
- Standards-compliant
  ETSI conform hand-over via ISDN or IP

Utimaco LIMS Access Points can be deployed at various positions in a network for monitoring both signaling and media. The probes associate the signaling to the bearer traffic and then acquire the targeted call data and usage information. All intercepted data are mediated by the Utimaco LIMS before they are delivered to the law enforcement agency over standardized interfaces.

Alternatively or in addition, the same LIMS Access Points used for targeted interception can also generate call detail records (CDR) for all communications session. The CDRs can be collected by the Utimaco DRS for long-term retention and further analysis.


Utimaco LIMS
Law Enforcement Agency
LIMS Management Server
HI1
(target:
MSISDN,
IMSI,
IMEI)
X1
(target: MSISDN, IMSI, IMEI)
LIMS
Mediation
Device
LIMS
Access
Point TDM
X2
(IRI)
X3
(CC)
HI2
(DF2:IRI)
HI3
(DF3:CC)
Monitoring Center
NodeB
RNC
BSC
BTS
3G Radio
Access Network
2G Radio
Access Network
A
IuCS
IuPS
GB
MSC
SGSN
E
Gn
HLR
GMSC
GGSN
Mobile
Core
Network
Yu
Gi
PSTN/ISDN
Internet

LIMS Access Points TDM

Realtime Monitoring of Circuit-Switched Networks

Communications Interception and Data Retention

The LIMS Access Point TDM supports the interception of signaling, content and location data of telephony calls, SMS messages and faxes on a wide range of networks:

- PSTN
- GSM
- UMTS
- CDMAone, CDMA2000

The probes are fully integrated in the Utimaco LIMS and DRS, where intercepted data is mediated and retained.

Target Identification

The LIMS Access Point is capable of correlating different identities of a single subscriber, even over multiple interfaces. Each probe tracks in realtime all occurrences of MSISDNs, IMSI, MSRN, IMEI, and TMSI. This allows the probe to acquire all data related to a target by just defining one of its identities.

Content Analysis

Realtime monitoring with the LIMS Access Point is not restricted to signaling only. The probe can also detect and extract DTMF tones, CAS tones (C5, R2), and fax/modem calls from bearer channels. The integrated CIC mapping technology assures accurate automatic correlation between signaling and bearer channels.

Interface Support

- E1/T1
- SDH/SONET (STM-1/OC3, STM-4/OC-12)
- 1G Ethernet (1000Base-T)

Protocol Support

- SS7 ISUP/TUP (incl. country specific implementations)
- ISDN PRI, C5, R2, DTMF, fax/modem
- GSM/CDMA A-Interface, Abis-Interface
- UMTS IuCS, IuPS, RANAP
- ATM, HDLC, TCP/IP
- SIGTRAN, SMPP

Performance Figures

- Scalable to monitor up to 16,000 TDM connections in realtime
- Supports up to 100,000 concurrent targets

Hardware Platforms

- Server:
  1U 19” rack mount
  - 110/230V AC power, redundant
  - CE, FCC, UL compliant
- Chassis:
  2U 19” rack mount w/ 3 cPCI slots or
  5U 19” rack mount w/ 8x cPCI slots
  - 110/230V AC power, -48V DC power, redundant
  - CE, FCC, UL compliant
- Switch:
  1U 19“ Ethernet switch 10/100/1000 Base-T
  - 110/230V AC power, FCC, CE compliant

Standards

- ETSI TS 101 671 (TDM delivery)
- ETSI TS 102 232-1, TS 102 232-6 (IP delivery)

Models

LIMS Access Point TDM-S
- up to 4x E1/T1 (duplex) integrated
- 2 x 1 Gb Ethernet (copper)
- 1U server

LIMS Access Point TDM-M
- up to 32 x E1/T1 (duplex) or
- up to 2 x STM-1 (duplex)
- 2x1Gb Ethernet (copper)
- 1U server + 2U cPCI chassis

LIMS Access Point TDM-L
- up to 64 x E1/T1 (duplex) or
- up to 4 x STM-1/STM-4 (duplex)
- 2x1Gb Ethernet (copper)
- 1U server + 2U cPCI chassis

utimaco®
a member of the Sophos Group

For more information on the Utimaco LIMS and Utimaco DRS, please visit:

www.utimaco.com/lims

Utimaco Safeware AG
Germanusstraße 4
52080 Aachen
Germany
Phone +49 (0) 241-16 96-0
li-contact@utimaco.com

Utimaco Safeware Partner: