Monitoring Center

Application Note

IP Interception System - IPIS

The IP Interception System offers flexible and scalable solutions to mark and intercept at multiple and varied points in the Internet and to deliver this data to one or more authorised Law Enforcement Agencies.

Where integrated in Internet components, IPIS supports the embedded LI functions. With no embedded LI, IPIS offers a range of Data Collectors to capture and filter the data.

SIEMENS

Global network of innovation

Overview

The IP Interception System (IPIS) performs Lawful Interception (LI) based on captured data from the Internet, mediation of various network devices and delivery of the intercepted data to Law Enforcement Agencies (LEA).

It can operate with the Siemens Monitoring Center or other Law Enforcement Monitoring Facilities (LEMF) chosen by the LEA. It supports the integrated LI functions of market leading switch and router vendors, and where none is available, offers a range of Data Collectors to filter and capture the desired data.

The Data Collectors directly offer Ethernet and ATM interfaces and bandwidths ranging from small ISPs to peering points in the Internet. Other interfaces are supported using adapters. IPIS can also manage ETSI LI sources.

A well conceived security architecture ensures access to targets and data only by authorized persons. Security of both data and management transmissions is always offered with IPIS but customer specific solutions can be easily implemented.

IPIS Applications

The IPIS is capable of intercepting data in the Internet, in other IP based networks and VoIP in Next Generation Networks (NGN). It can be configured to intercept and deliver a range of data using very granular triggers to select the types of data or the targets to be intercepted.

The IPIS is used in several application scenarios including the following:

- Email only interception and delivery
- VoIP interception in NGN
- General Internet interception

All IP data received into the IPIS can be distributed to LEAs according to ETSI standards. The LEA can extract IP data based on triggers set in the IPIS. The following trigger types can be set in the IPIS:

- Email, such as SMTP, POP3, IMAP4 & Webmail
- Web/HTTP, FTP or IRC
- VoIP
- Keyword/String Search
- IP Address
- Instant Messaging

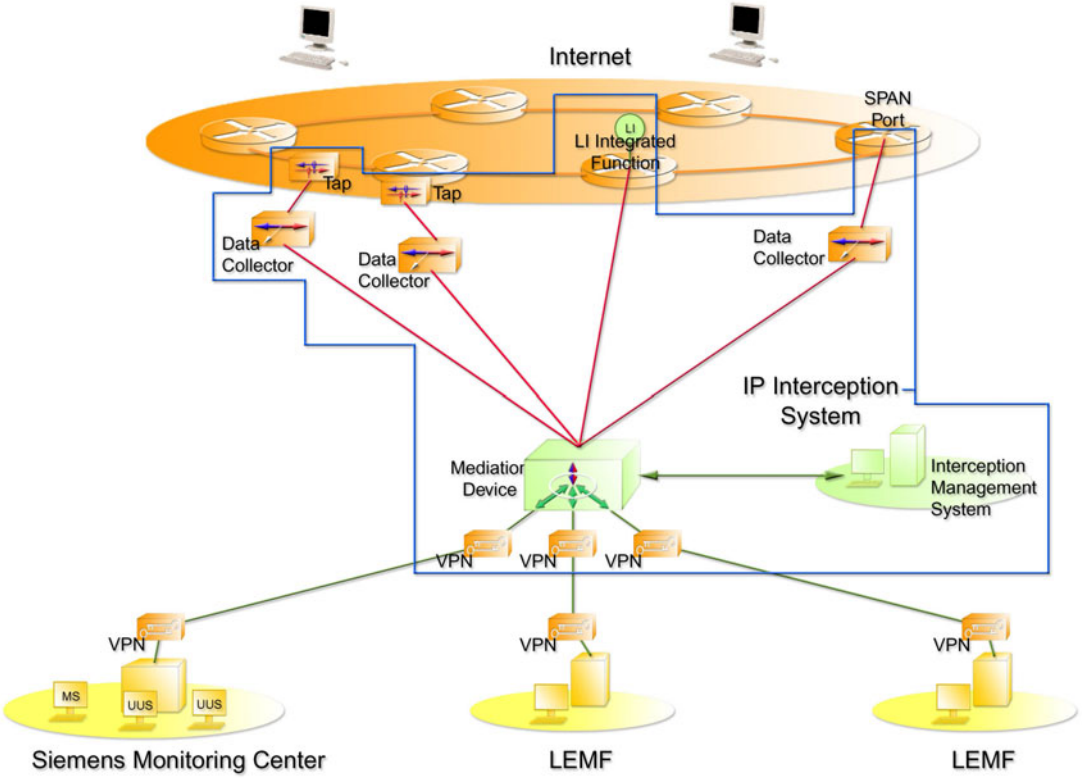

Figure 1. LI Network, Mediation and LEMF environment

Background to IP Interception

Most modern Circuit Switched networks have an integrated Lawful Interception (LI) function. The Lawful Interception function intercepts the targeted calls and forwards them to Law Enforcement Agencies (LEA), as directed by an Interception Management System (IMS). Meta-data about the call (Intercept Related Information) is sent to the IMS which forwards it to the appropriate LEA.

In contrast to this mature standards environment, the Internet is still in the process of LI standardisation. Most IP interception is performed by Data Collectors that are located near or inside the Internet nodes and essentially filter it for desired data.

There are a few IP Switch and Router vendors that have started to implement LI functions and these will become more common in networks over time.

The varied mixture of Switch or Router integrated LI function and Data Collectors from different vendors needs a Mediation and Delivery application to mediate between the Internet and the LEA.

Siemens IP Interception System

Siemens offers the IP Interception System to address the needs of Lawful Interception in the Internet. There are several components in the solutions as well as flexible configurations to suit the needs of the customer. This application note looks more closely at these solutions from Siemens.

The Networks

There is an ever-increasing array of networks that use IP as their data transmission protocol. The Internet is the first that comes to mind, but it also includes GPRS, UMTS, VoIP networks – Next Generation Networks (NGN) and many Wireless Networks. Where there is a mandate to perform Lawful Interception in any or all of these networks, the first questions are how and where to access the data.

IPIS offers a wide variety of possibilities to gain access to and manage the flow of the intercepted data from the networks.

These include:

- Taps
- SPAN Ports
- Devices with integrated LI functions
- Data Collectors
- Load balancing techniques, including IP Application and Aggregation switching
- Interface/Protocol Mediation

Taps

Network Taps are used to connect to different physical signals in an unobtrusive manner.
They are available for electrical and optical lines for different transmission speeds.

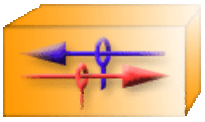

Figure 2. IP Tap

SPAN Ports

In most network switches, a SPAN or mirroring Port can be configured to copy the traffic of a single or of multiple switch ports. Also complete VLANs can be mirrored. However, over-subscription of SPAN Ports can lead to a loss of data.

Figure 3. SPAN Port

Integrated LI Function

Due to the evolving requirements of Lawful Interception in IP networks, leading Internet Switch and Router manufacturers have started development to integrate an LI Function directly into their devices.

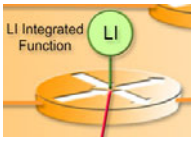

Figure 4. Integrated LI function

Advantages:

- More security as only the targeted data leaves the network
- No additional components within the network

Data Collectors

A Data Collector is a device used to intercept data from IP based networks, most notably the Internet.

They come in many forms but generally operate by passively tapping the traffic on a communications link and filtering an unobtrusive copy of the data for desired content. Only the filtered data is forwarded to the LEA.

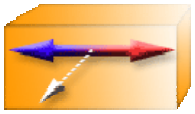

Figure 5. Data Collector

Advantages:

- Independence from other network components
- High data output rates

Load Balancing Techniques

Load Balancers can aggregate Ethernet based signals and distribute them to multiple Data Collectors based on load balancing and/or traffic filtering schemes. The Load Balancer ensures that data, which belongs to a unique session, is forwarded to the same connected Data Collector. In addition to aggregation and load balancing, pre-filtering of traffic can be performed based on an IP protocol and port qualifier (e.g. protocol TCP with port 25).

Interface/Protocol Mediation

With special components like Routers, transport protocols (e.g. Frame Relay, HDLC, ATM) can be removed. In addition, the IP traffic can be mediated from various electrical or optical transmission media (e.g. E3/T3, STM-1/OC-3, STM-4/OC-12) to Ethernet connections.

Mediation Device

The Mediation Device sits between the Data Collectors and/or the integrated LI functions on the network side and the LEMFs or Monitoring Centers on the Law Enforcement Agencies' side.

Figure 6. Mediation Device

Its purpose is to mediate requests for intercepted content by authorised entities and convert them into commands that are understood by the various Data Collector implementations and integrated LI functions in the networks. It must also understand the delivery protocols and mechanisms of the Data Collectors and the integrated LI functions and convert the intercepted data into a form suitable for delivery to one or more Law Enforcement Agencies.

Marking Terminals

Marking Terminals connect to the Mediation Device and are used by Operators to mark parts of the Internet traffic for interception by setting or defining targets/triggers.

Figure 7. IMS – Marking Terminal

The marking process specifies identifying aspects of Internet Traffic such as an IP address, an email address, etc. The targets/triggers are placed by the Mediation Device into the Data Collectors or integrated LI functions of the networks.

Law Enforcement Monitoring Facility (LEMF)

LEMF is the term used by ETSI to denote the application used by the Law Enforcement Agency to receive, analyse and archive intercepted data. The Monitoring Center (MC) from Siemens is such a LEMF and it is a typical representative of a system that receives intercepted data from the Mediation Device of the IPIS.

Figure 8. Law Enforcement Monitoring Facility

The MC is designed with a flexible architecture and can also be used to play the role of the Marking Terminal where this is allowed under a country's LI laws. It can receive and process

intercepted data from the Internet as well as from PSTN, Mobile, 3G and NGN networks.

GPRS and UMTS networks

In GPRS and UMTS networks, subscribers can be marked for monitoring of IP traffic by IMS systems. The Intercept Related Information (HI2) is transmitted via the IMS system to the LEMF while the Call Content (HI3) is transmitted directly from the appropriate network element to the LEMF. These transmissions are IP connections which can be based on various transport networks (e.g. Ethernet, ISDN, X.25).

For marked GPRS and UMTS subscribers, the whole IP traffic is intercepted and forwarded to the LEMF, regardless of the IP application used (Web, Mail, Chat, etc.). This traffic does not need to pass through the Mediation Device.

The Challenge of Rapid Evolution

No network has evolved as far and as fast as the Internet. Its constant change presents continuous challenges to the LI technology developers to keep pace with the communications applications being used in the Internet. As an example, the use of VoIP is spreading rapidly and presented its own challenges to LI technology. VoIP interception is now supported in the IPIS and MC.

Another evolution of the Internet is towards broadband and the consequent increase in amounts of data that the LEA must manage.

The Siemens VDR group is proactive and anticipatory in its analysis and development of technologies and architectures to address the constant change in Internet applications and mass data management. This is reflected in the range of protocols supported and the various load-balancing and data segregation techniques employed in the Siemens solutions.

Feature	Highlights
Direct Access capabilities	- 100 Mbps and 1 Gbps Ethernet electromagnetic taps - 1, 2.5, 10 Gbps Ethernet optical taps - E3 electromagnetic taps - STM-1/OC-3 and STM-4/OC-12 optical taps
Interface/protocol mediation	- E3 with HDLC to Ethernet - E3 with Frame Relay to Ethernet - E3 with PPP to Ethernet - STM-1/OC-3 Packet-over-SONET with HDLC to Ethernet - STM-1/OC-3 Packet-over-SONET with Frame Relay to Ethernet - STM-1/OC-3 Packet-over-SONET with PPP to Ethernet - STM-1/OC-3 ATM with AAL5 to Ethernet - STM-4/OC-12 Packet-over-SONET with HDLC to Ethernet - STM-4/OC-12 Packet-over-SONET with Frame Relay to Ethernet - STM-4/OC-12 Packet-over-SONET with PPP to Ethernet - STM-4/OC-12 ATM with AAL5 to Ethernet
Data Collectors	- Filtering of IP-based traffic according to various trigger criteria - High throughput rates
Interfaces to Integrated LI Functions	- Various, dependent on the vendor
Triggers	- E- mail (SMTP, POP3, IMAP4, Webmail) - Web/HTTP, FTP, IRC - VoIP - Keyword/String Search - IP Address - Instant Messaging
Mediation Device	- Supports numerous Data Collectors - Load Balancing - Supports multiple LEMF for delivery - Marking terminal - Access and marking security
Marking Terminal	- Remote locations - GUI for Trigger creations
VPN Devices (Optional)	- Secures the connection between Data Collector and Mediation Device when they are deployed in different locations as well as the connection between the Mediation Device and the LEMF. - Appropriate models can be supplied by Siemens but also dedicated customer equipment can be integrated on request if required by national legislation.

Abbreviation	Description
3G	Third Generation
AAL5	ATM Application Layer 5
AOL	America OnLine
ATM	Asynchronous Transfer Mode
E3	34.368Mbps ITU standard - Europe
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
H.323	ITU H series standard
HIx	Handover Interface
HDLC	High level Data Link Control
LI	Lawful Interception
ICQ	Chat protocol (Pronounced "I seek you")
IMAP4	Internet Message Access Protocol version 4
IMS	Interception Management System
IP	Internet Protocol
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
LEA	Law Enforcement Agency

Abbreviation	Description
LEMF	Law Enforcement Monitoring Facility
MC	Monitoring Center
MS	Management Station
MSN	Microsoft Network
NGN	Next Generation Network
NNTP	Network News Transfer Protocol
OC-x	Optical Carrier - x
POP3	Post Office Protocol version 3
PPP	Point To Point Protocol
PSTN	Public Switched Telecommunications Network
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SONET	Synchronous Optical Network
SPAN	Switched Port Analyser
STM-x	Synchronous Transport Module - x
T3	44.736Mbps ITU standard - US
TCP	Transmission Control Protocol
UMTS	Universal Mobile Telecommunications System
UUS	Unified User Station
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
X.25	ITU-T standardisation for wide area communications

Contact:
Siemens Voice and Data Recording (VDR)
Sales Office Fax: +49 89 722 49801
VDR-sales.com@siemens.com

Voice & Data Recording
Hofmannstr. 51
D – 81379 Munich
Germany

Document number S41045-N691-B018-03-7629