Lawful Interception for 3GPP: Cisco Service Independent Intercept in the GGSN

Contents

Introduction

The Cisco Service Independent Intercept ™ (SII) architecture is a generic architecture in IP networks that is independent of the service being intercepted. The Cisco Gateway GPRS Support Node (GGSN) provides solutions based on the Cisco SII architecture that facilitate lawful electronic surveillance of communications. Previously available for data and voice services, it has been extended for 3GPP mobile systems.

This paper presents two methods for intercepting mobile targets: One uses the new mobile inception filter in the GGSN. The other employs the IP interception functions of the Cisco 7600 Series Router. It enables the interception of roaming targets inside their home network. It also facilitates the use of direct tunnel architecture, specified in 3GPP Release 7, which bypasses the Serving GPRS Support Node (SGSN) for data traffic.

Elements of Lawful Interception

The term *Lawful Interception* (LI) describes the process by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications as authorized by judicial or administrative order. The means and authority of conducting LI is often recorded in government legislation or regulatory mandates.

LI is initiated by a warrant from the Law Enforcement Agency (LEA), which identifies a target identity, a specific LI service, and a period of time. It requires the service provider (SP) to deliver Intercept-Related Information (IRI) and/or Content of Communication (CC) associated with sessions initiated by a specific target.

Note that data retention is a different regulatory requirement than LI. It requires the SP to retain data associated to specific services (that is, fixed telephony, mobile telephony, Internet telephony, and Internet access) for every subscriber during a specific period of time. The data to be retained does not include the CC. The LEA sends a warrant to the SP to collect the data associated with past communications for specific targets and services for a period of time. Data retention is not in the scope of this document.

LI is a new requirement for GGSN. In the past, LI for mobile data traffic was requested in the SGSN only. The SGSN captures the IRI and the CC for most of the mobile data communications and, for LEAs, LI in SGSN was the first priority. It appeared recently that LI must also be supported in the GGSN for two main reasons:

- There is no SGSN in the home network for roaming targets.
- The SGSN does not handle the CC with the Radio Network Controller (RNC)-GGSN direct tunnel architecture that has been specified in 3GPP Release 7.

3GPP Standards

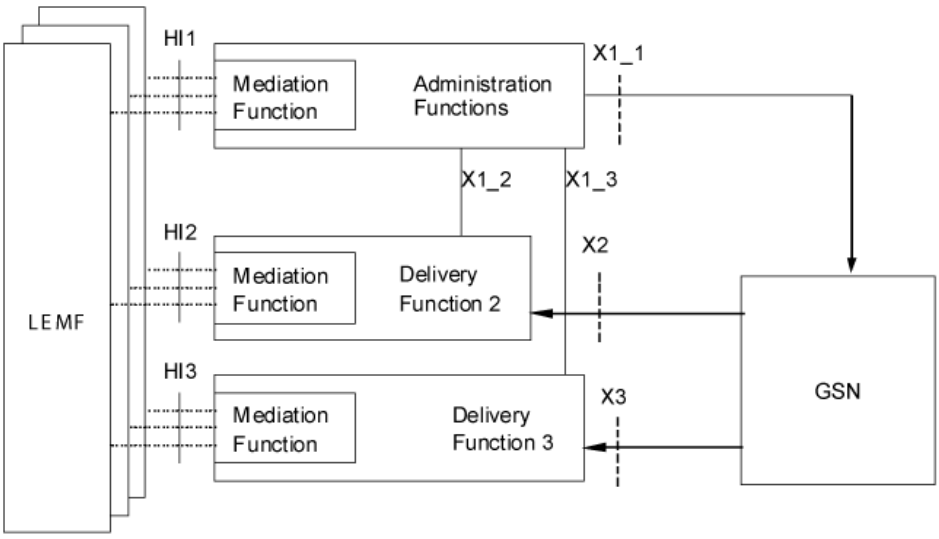
3GPP has published the following specification for LI:

- TS 33.106: *Lawful interception requirements* [5] specifies the requirements for all 3GPP services.
- TS 33.107: *Lawful interception architecture and functions* [6] specifies the functional architectures for different 3GPP services, including GPRS Support Node (GSN) packet data services.
- TS 33.108: *Handover interface for Lawful Interception* [7] specifies the Handover Interface (HI) between the SP and the LEA. The objective of the Cisco 3GPP LI solution is to support a number of regional interception regulations using specific (regional) mediation functions, allowing only required information to be transported over the national HI.

Packet Switched Intercept Configuration

The Packet Switched Intercept configuration specified in TS 33.107 is shown in Figure 1:

Figure 1. Packet Switched Intercept Configuration



The Mediation Function is split into three parts:

- Administration function
- Delivery function 2 for HI2
- Delivery function 3 for HI3

The GSN includes the SGSN and the GGSN. The GSN provides both the IRI and CC.

The interfaces X1, X2, and X3 are listed, but the specification does not define a protocol.

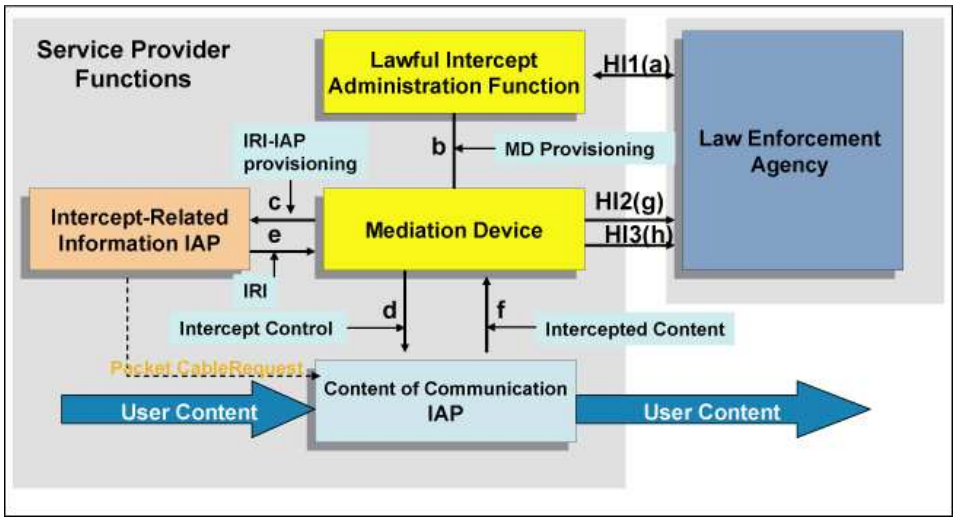
Cisco Service Independent Intercept Architecture

The objective of Cisco SII is to define an LI architecture in IP networks that is independent of the service to be intercepted. This section describes the functions and characteristics of the Cisco SII architecture.

Cisco SII Functional Model

Figure 2 provides a functional view of the Cisco SII architecture.

Figure 2. Functional Model for Lawful Interception



The functions shown in Figure 2 are as follows:

LI Administration Function

The LI administration function communicates administrative information with the LEA through the HI1 interface and provides a provisioning interface to the other SP components that is specific to a particular LI request.

LI Mediation Device

The LI mediation device receives provisioning information from the LI administration function, IRI from the IRI Intercept Access Point (IRI-IAP), and CC from the CC Intercept Access Point (CC-IAP). It delivers to the LEA the country-specific and service-specific IRI using the HI2 interface and delivers the CC using the HI3 interface. The LI Mediation Device is third-party equipment.

IRI-IAP

The IRI-IAP controls the data connections established by the target subscriber.

When data intercepts are conducted, the data connection may be a AAA server, a DHCP server, or a probe connected in the path between the target subscriber and the AAA or DHCP server. The IRI interface to the LI mediation device has the following functions for data intercepts:

- Indicates when the target subscriber logged on
- Indicates when the subscriber logged off
- Provides the IP address of the target subscriber with optional filters
- Provides the address of the CC-IAP, which intercepts the CC

In the case of voice intercepts, the data connection may be a line-side Call Agent, a Media Gateway Controller, a session initiation protocol (SIP) server, or an H.323 gatekeeper. The IRI interface to the LI

mediation device has the following functions for voice intercepts:

- Provides the target subscriber IRI used to establish the telecommunication service and control its progress (for example, target identification, identification of the other parties of a communication, basic service used, direction of the call or the event, answer indication and/or release causes, time stamps)
- Provides the IP address and the UDP ports used for the voice over IP (VoIP) call

The LI mediation device provisions the target identity list in the IRI-IAP with the IRI-IAP provisioning interface.

CC-IAP
The CC-IAP duplicates the filtered traffic and forwards it to the LI mediation device through an IP tunnel.

When voice intercepts are conducted, the CC-IAP is the target subscriber edge router or the trunk gateway at the public switched telephone network (PSTN) interconnection. It intercepts the media stream identified by an IP address and UDP port associated to the Real-Time Transport Protocol (RTP) stream.

In the case of data intercept, the CC-IAP is the edge router of the target subscriber. It intercepts the data stream identified by an IP address and optional filters and forwards them to the LI mediation device. The LI mediation device controls the CC-IAP with the Intercept Control secured Simple Network Management Protocol Version 3 (SNMPv3) API.

Monitoring Center
The monitoring center, also called the collection function, is outside the scope of the SP's responsibilities. This capability resides within the LEA.

Cisco SII Architecture Security and Characteristics

The Cisco SII architecture has been designed to meet the following security requirements:

- Prevent detection by unauthorized entities: The interception takes place on equipment that is within the trust domain of the SP for example, the edge router or trunk gateway) and is done along the normal path of the data (for example, the edge router).
- Prevent unauthorized activation of interception: The interfaces to provision or control the IRI-IAP and CC-IAP are dedicated for LI, and have strong cryptographic authentication to establish the identity of the principals, and correlate the identity of the principals with the action they are attempting to perform. Message integrity checking is also used to counter replay attacks. The interception functions in the IRI-IAP and CC-IAP should be provisioned only by the LI mediation device, which should be carefully controlled and accessed only by authorized personnel.
- Prevent disclosure of target information: Target information and intercept states in the IRI-IAP and CC-IAP are not accessible to unauthorized personnel from any operational management station, via management protocols, command-line interfaces (CLI), and traces or dumps, and they are not stored in nonvolatile memory. If the IRI-IAP or CC-IAP device fails or reboots, all intercept-related information and states disappear and are not accessible by any means.
- Perform logging and auditing: Logging and auditing are used to detect unauthorized attempts to access the intercept capability. Log files are controlled, retrieved, and maintained by the mediation device in a secure manner. To avoid being viewed or detected, these log files are not stored on the interception devices.
- Separate activities of multiple LEAs. If multiple LEAs are intercepting the same subject, they are not aware of each other. This objective is achieved by having a one-way flow of intercept information from the mediation device to the LEA such that no information in the flow could indicate the presence of multiple flows to different LEAs. Separation also implies limited LEA access to the SP's equipment.
- Correlate the identification information and the content information.
- Maintain confidentiality and authenticity of the information streams.

The main characteristics of the Cisco SII architecture are the following:

- Provides a common architectural solution for intercept of IP communications (voice and data)
- Provides a solution that is cost effective (both acquisition and recurring costs) and fits in as naturally as possible with architectures deployed or defined by Cisco
- Places control of LI on the mediation device (instead of on call-control equipment)
- Provides a common interface for the mediation device and call-control equipment

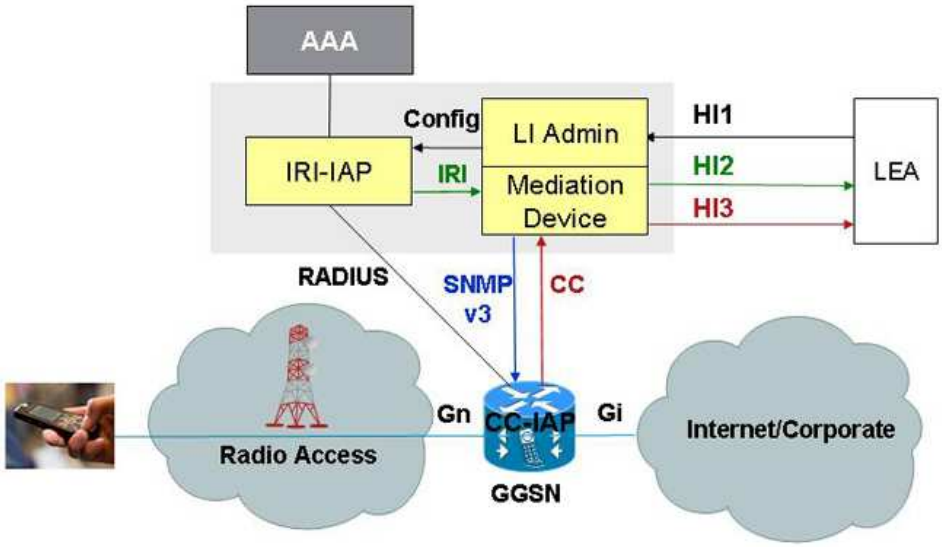
The Cisco SII architecture is described in more detail in the Internet draft RFC 3924[1].

SII for Mobile

In a mobile environment where the target user is attached to a GPRS, Edge, or 3G network, the legal interception can be performed either on the SGSN or the GGSN depending on the architecture and the roaming status of the user. LI on SGSN is applicable only if direct tunnel is not deployed between the RNC and the GGSN and if interception does not target a roaming user for a warrant located in the home network. For all other cases, LI is required to happen on another node that supports the Cisco SII framework, such as Cisco GGSN or any Cisco router sitting on the Gi or Gp interface.

The following figure highlights the LI configuration:

Figure 3. SII for Mobile



The IRI-IAP is independent of the GGSN. It duplicates the RADIUS traffic of the target subscribers and sends it to the mediation device.

The IRI-IAP may be implemented as a passive probe located between the GGSN and the AAA server that filters the target RADIUS traffic.

The IRI-IAP may also be integrated into the mediation device. In this case, the GGSN is configured to broadcast all the accounting messages to the AAA server, and the mediation device must implement the RADIUS handshake protocol.

The CC-IAP functions are available with two different options, which are described in the following sections.

Overview of LI Integrated in the GGSN

With LI integrated in the Cisco GGSN, the CC-IAP is integrated in the GGSN card. It includes the LI filters, the interface with the LI mediation device, and the encapsulation of the target traffic.

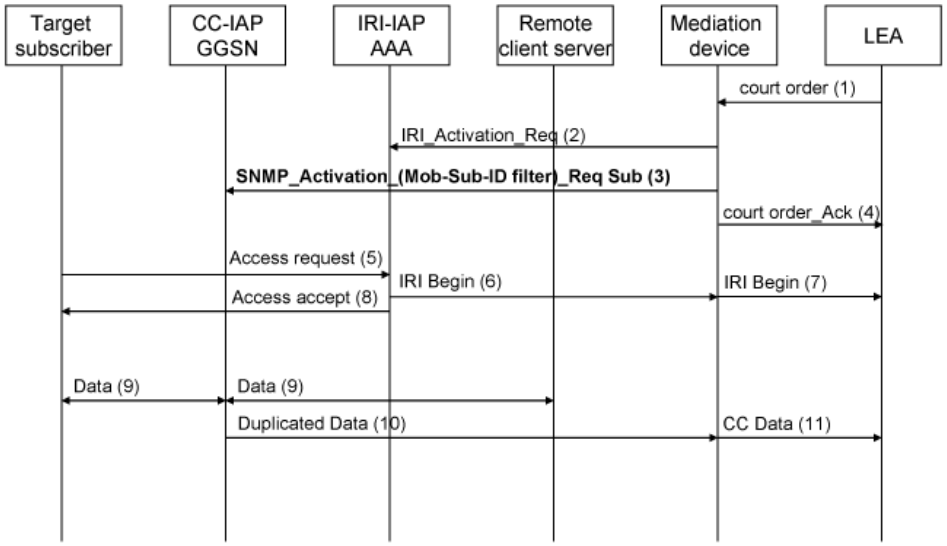
This option introduces the International Mobile Subscriber Identity (IMSI) number filter, which is defined in a new Management Information Base (MIB) called *CISCO-MOBILITY-TAP-MIB*.

When the LEA makes a request to intercept a target, the mediation device provisions the IRI filters in the IRI-IAP and the mobile subscriber identity filter in the GGSN. These filters do not need to be updated during the activation of the target PDP context. This solution simplifies the LI mediation device activation process.

When the target activates a PDP context, the GGSN associates the mobile subscriber identity with the IP address that is allocated to the target traffic. It starts duplicating all the target traffic and sends it to the mediation device. The LI mediation device does not need to activate dynamic IP filters in the GGSN each time the target activates a connection.

Figure 4 depicts the message exchange among the target subscriber, remote client or server, CC-IAP/GGSN, IRI-IAP, mediation device, and LEA during the establishment of a 3GPP data connection with RADIUS authentication.

Figure 4. Call Flow with LI Integrated in the GGSN



The following list describes the sequence of messages shown in Figure 4:

1. The LEA delivers a court order to the LI mediation device (MD).
2. The MD sends an IRI_Activation_Request to provision the IRI-IAP with the target IRI filter.
3. The MD sends an SNMPv3_Activation_Request to provision the CC-IAP/GGSN with the target CC filter (mobile subscriber ID).
4. The MD sends a court order acknowledgment to the LEA.
5. The target subscriber sends username and password to a RADIUS client, which sends an Access Request to a RADIUS server. The Access Request is intercepted by the IRI-IAP.
6. The IRI-IAP sends an IRI_Begin to the MD.
7. The MD sends an IRI_Begin to the LEA.
8. The RADIUS server sends an Access Accept to the RADIUS client in the GGSN.
9. The target subscriber sends and receives IP packets with the remote client or server. These IP packets are intercepted by the CC-IAP in the GGSN.
10. The CC-IAP duplicates and sends the filtered data packets to the MD.
11. The MD forwards the duplicated data packets to the LEA.

Overview of LI in the Cisco 7600 Series Router

With LI integrated in the Cisco 7600 Series Router, the interface with the LI mediation device and the encapsulation of the target traffic are located in the Cisco 7600 supervisor or in the shared port adapter (SPA) interface processor–400 (SIP-400). The IP filters that duplicate the target traffic are distributed in the 7600 line cards.

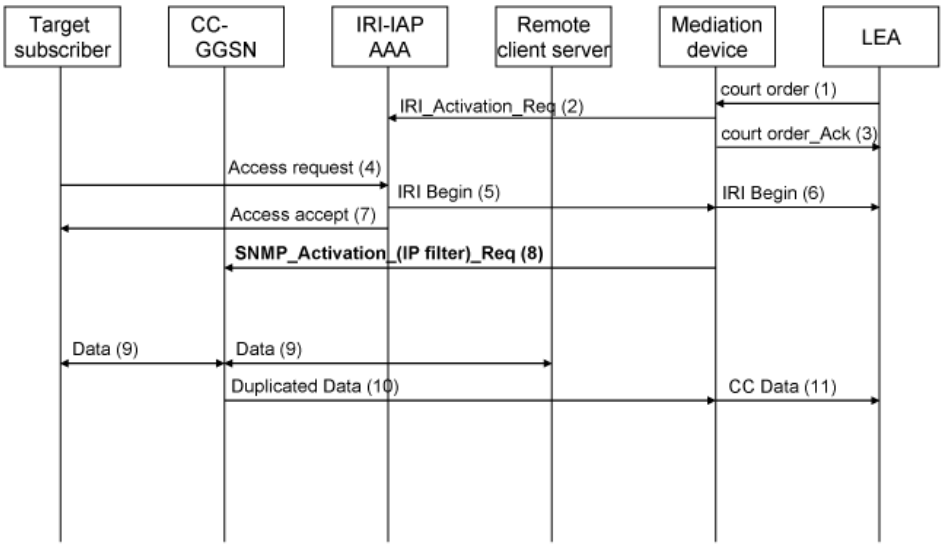
When the LEA makes a request to intercept a target, the mediation device provisions the IRI filter in the IRI-IAP.

When the target activates a PDP context, the IRI-IAP sends the target Radius Access-Request/Response or RADIUS Accounting messages to the mediation device. The RADIUS vendor-specific attributes (VSAs) that are supported on the Cisco GGSN Gi interface are listed in " Mapping of GGSN RADIUS Parameters for IRI and CC Control." These messages enable the mediation device to correlate the mobile subscriber identity (for example, MSID, IMSI, ESN, or NAI) with the dynamic IP address that is allocated to the target.

The mediation device activates the interception of the target traffic in the Cisco 7600 Series Router with IP filters that are defined in the *CISCO-IP-TAP-MIB*.

Figure 5 depicts the message exchange among a target subscriber, remote client or server, CC-IAP/GGSN, IRI-IAP, mediation device, and LEA during the establishment of a 3GPP data connection with RADIUS authentication.

Figure 5. Call Flow with LI in the Cisco 7600 Series Router



The following list describes the sequence of messages shown in Figure 5:

1. The LEA delivers a court order to the LI MD.
2. The MD sends an IRI_Activation_Request to provision the IRI-IAP with the target IRI filter.
3. The MD sends a court order acknowledgment to the LEA
4. The target subscriber sends username and password to a RADIUS client, which sends an Access Request to a RADIUS server. The Access Request is intercepted by the IRI-IAP.
5. The IRI-IAP sends an IRI_Begin to the MD.
6. The MD forwards an IRI_Begin to the LEA.
7. The RADIUS server sends an Access Accept to the RADIUS client in the GGSN.
8. The MD sends an SNMPv3_Activation_Request to provision the CC-IAP/GGSN with the target CC filter (IP filters).
9. The target subscriber sends and receives IP packets with the remote client or server. These IP packets are intercepted by the CC-IAP in the GGSN.
10. The CC-IAP duplicates and sends the filtered data packets to the MD.
11. The MD forwards the duplicated data packets to the LEA.

Mobile Use Cases

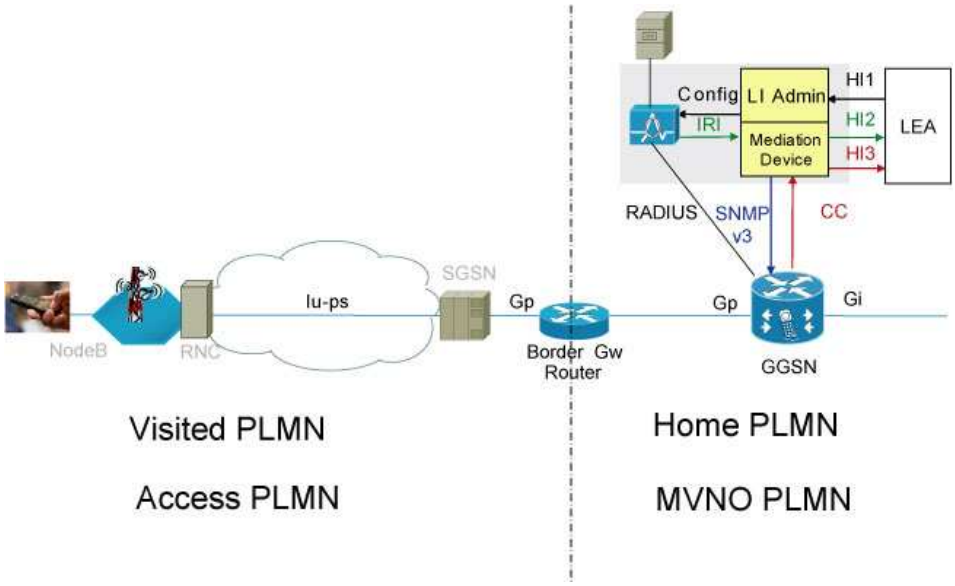
Case 1: Target in Visited or Access Network, Warrant in the Home or MVNO Network

This use case applies in the following configurations:

- The target is in a visited network and the warrant is received by the home network.
- The warrant is received by the MVNO that controls the GGSN. The SGSN is controlled by the access operator.

In this case, the following architecture facilitates the interception on the Gi interface.

Figure 6: Use Case 1

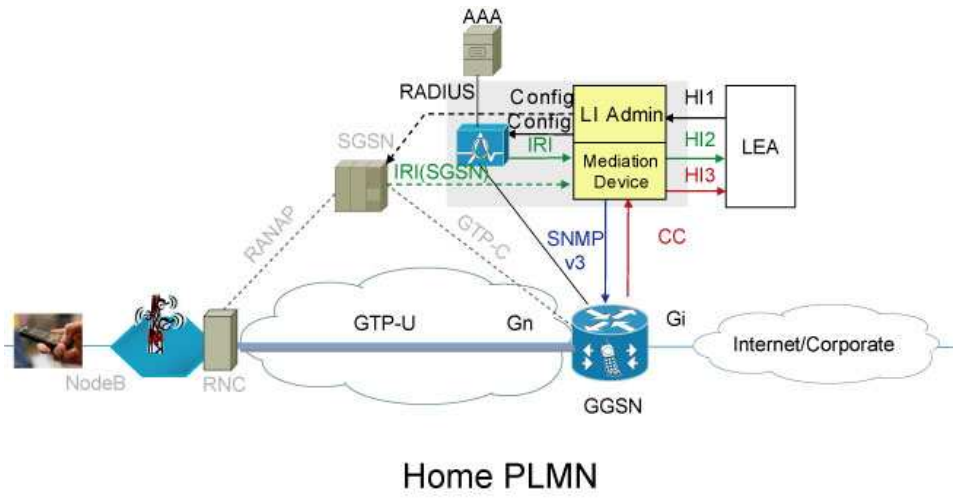


The preceding architecture shows that LI could be performed using the Cisco SII framework on a Cisco 7600 Series Router that hosts the GGSN application. There is no need to request LI on the SGSN, which is located on the visited or access network.

Case 2: Target and Warrant in the Home Network with RNC-GGSN Direct Tunnel

When the target and warrant are in the home network, the following architecture facilitates the interception on the Gi interface.

Figure 7. Use case 2



The solution facilitates LI when the SGSN is not in the data plane. In that case, a solution based on the LI capability of the SGSN will not work.

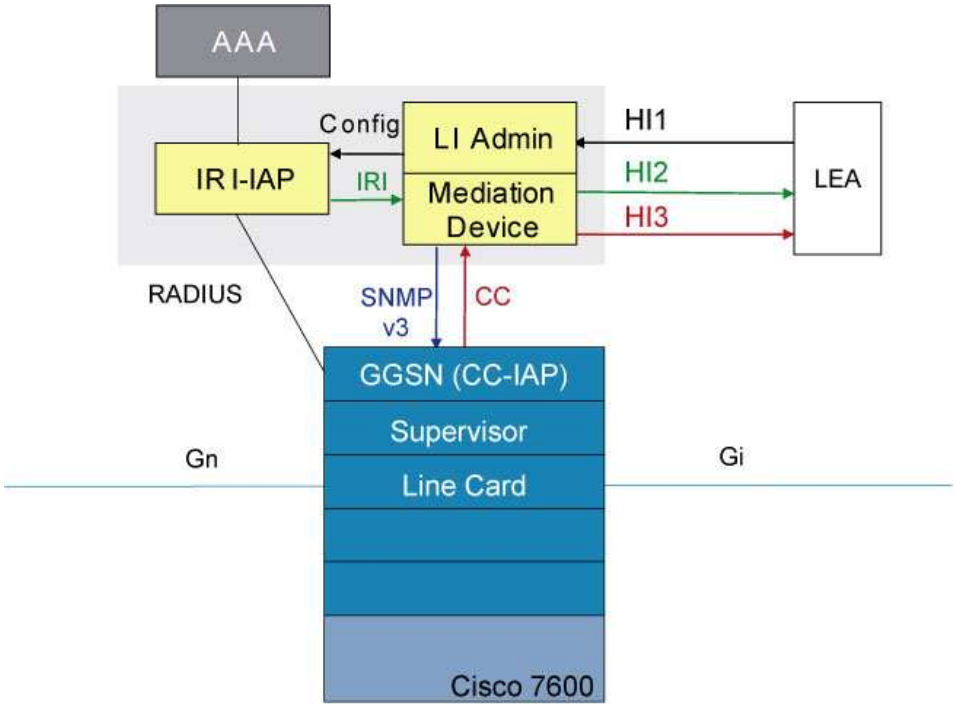
The GGSN provides the CC and the RADIUS probe provides the IRI.

SGSN may provide additional IRI, such as *location*, depending on the SGSN software release, but it is not mandatory for the interception to work.

Design of LI Integrated in the GGSN

The configuration of LI in the GGSN is depicted in Figure 8:

Figure 8. LI in the GGSN Service Module



The CC-IAP functions are handled by the GGSN service application module for IP (SAMI), which is hosted by the Cisco 7600 Series Router. This functionality has been supported since GGSN Release 9.

The IRI interception is not directly supported by the GGSN; instead, Cisco offers two solutions. First, the SP can set up a probe between the GGSN and the AAA server. The probe then duplicates all accounting traffic and sends it to the mediation device. The mediation device then finds the relevant accounting messages and sends them to the LEA.

Second, broadcast accounting can be used. In this instance, the Cisco GGSN is configured to broadcast all accounting messages to both the AAA server and the mediation device, which must implement the RADIUS handshake protocol.

GGSN-Based LI Features

The Cisco GGSN service module duplicates packets and encapsulates the LI packet with an IP, UDP, and call content connection identifier (CCCID) header according to the SII specification. The GGSN manages the SNMPv3 control interface and the CC interface with the LI mediation device.

When the Cisco GGSN receives the TAP trigger, the gateway starts replicating and encapsulating the packets to send to the mediation device using Packet Cable UDP as the transport protocol for the content.

The Cisco GGSN Release 9 LI implementation supports the MIB2 with the *CISCO-MOBILITY-TAP-MIB* and the IMSI filter.

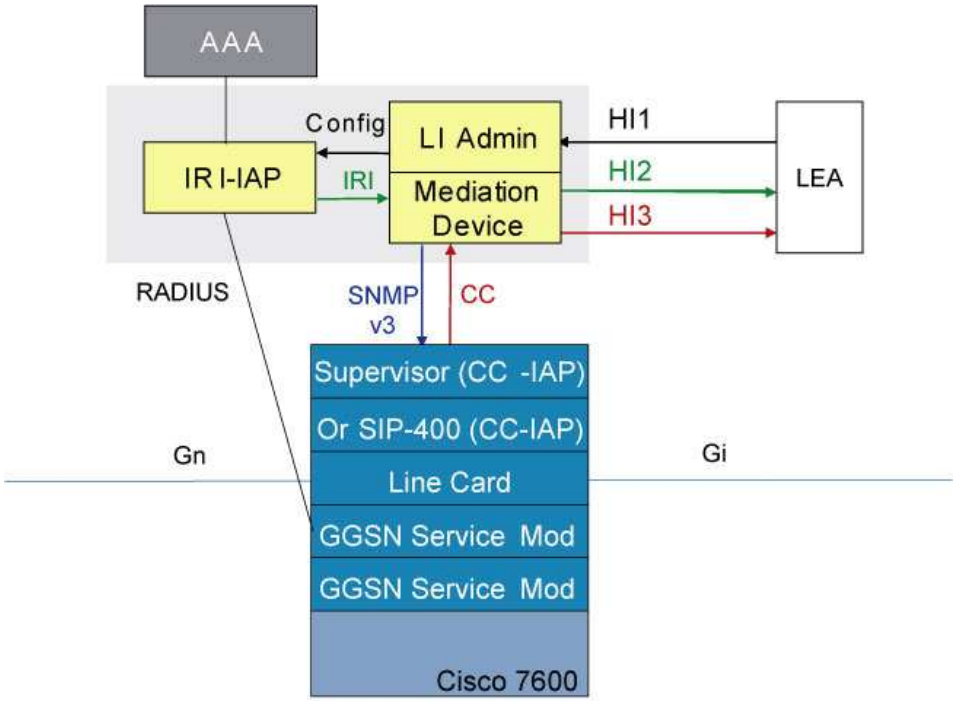
Because the intercept is based on physical criteria such as IMSI, the packets forwarded to the MD may include multiple formats for the same intercept. Cisco GGSN Release 9 supports IPv4 and IPv6 packet interception. Mobility MIB implementation is flexible and future releases will allow interception of PPP or Ethernet packet.

At the time of writing, interworking testing for the LI feature of GGSN Release 9 is still under progress with mediation device partners. The testing is necessary because this feature requires the mediation device to support IMSI-based interception and interception of different types of packets, such as IPv4 or IPv6 packets.

Design of LI in the Cisco 7600 Series Router

The configuration of LI in the Cisco 7600 Series Router is depicted in Figure 9:

Figure 9. LI in the Cisco 7600 Series Router



The CC-IAP functions are handled by the Cisco 7600.

The ACL LI filters are set in every line card and GGSN service module.

The switch fabric performs the duplication of the original filtered packet. One packet is forwarded to the egress line card. The other packet is forwarded to the Route Processor or to the SIP-400 for LI hardware acceleration.

For the inbound traffic from the Internet to the target, the LI access control list (ACL), which duplicates the target traffic, is located in the line card of the Gi interface. For the outbound traffic from the target to the Internet, the LI ACL is located in the GGSN service module.

Supervisor-Based LI Features

The supervisor configuration does not involve the SIP-400.

The supervisor receives the duplicated filtered packet from the switch fabric. It encapsulates the LI packet with an IP, UDP, and CCCID header according to the SII specification. The supervisor manages the SNMPv3 control interface and the CC interface with the LI mediation device.

It supports the MIB2 with the following MIBs:

- *CISCO-TAP2-MIB* for the generic LI control information
- *CISCO-IP-TAP-MIB* to define IP filters: Dest IP Addr, Dest Port Range, Src IP Addr, Src Port Range, and Protocol ID

The route processor must be a Supervisor Engine 32, Supervisor Engine 720, or Route/Switch Processor 720. These features were introduced in Cisco IOS Software Release 12.2(33)SRB and are available now.

Hardware-Accelerated LI Features

The SIP-400 accelerates the throughput of LI traffic in two phases.

Phase 1: Layer 2 LI

Layer 2 LI does not apply for the Cisco GGSN. This phase supports the *CISCO-802-TAP-MIB* to filter MAC addresses only. The ingress or the egress interface to be intercepted must be on the SIP-400.

Layer 2 LI was introduced in Cisco IOS Software Release 12.2(33)SRB.

Phase 2: Acceleration of Supervisor LI Features
The SIP-400 receives the duplicated filtered packet from the switch fabric and encapsulates the LI packet with an IP, UDP, and CCCID header according to the Cisco SII specification. The SIP-400 manages the SNMPv3 control interface and the CC interface with the LI mediation device using the same MIBs as the supervisor:

- *CISCO-TAP2-MIB* for the generic LI control information
- *CISCO-IP-TAP-MIB* to define IP filters: Dest IP Addr, Dest Port Range, Src IP Addr, Src Port Range, and Protocol ID

Packets can ingress any line card and egress any line card.

Administrators can configure a list of SIP-400s to be used for LI processing.

Only one SIP-400 from the configured list will be actively processing LI at any point in time.

The SIP-400 can run in either dedicated or nondedicated mode. In dedicated mode, shared port adaptors will be deactivated.

If a SIP-400 that is configured as the LI processing card comes online after the supervisor, the system will switch the LI functionality from the supervisor to the SIP-400.

This feature was introduced in Cisco IOS Software Release 12.2(33)SRC.

VRF-Aware LI

The Cisco 7600 Series Router provides support for VRF-lite (ip2ip) and MPLS VPN (ip2tag for ingress and tag2ip for egress).

The filters are based on IP flows in a VRF, not on MPLS/VPN labels.

A hardware limitation requires packet recirculation, resulting in halving the actual data performance for the particular VRF that is being tapped. This is not just a duplicate packet, but actual traffic. Because of recirculation, VRF-lite (ip2ip) traffic may be intercepted twice if incoming and outgoing interfaces are under the same VRF.

VRF-aware LI is supported in Cisco IOS Software Release 12.2(33)SRC. This feature will work for both supervisor-based LI and SIP-400 hardware-accelerated LI.

The use of VRF in the mobile environment is enabled by using a specific access point name (APN) on the GGSN, for which a mapping between APNs and VRFs is performed. The APN ID is included in the RADIUS Access Request/Response or Accounting messages, and will allow the IRI-IAP and the mediation device to correlate a user ID with the IP address and VRF used. Correlation capabilities are available when the mediation device is aware of the APN-VRF mapping table.

Note that the VRF name and target IP filters in the VRF must be available in the GGSN service module for outbound traffic from the target to the Internet. The VRF name and target IP filters in the VRF must be available in the line card of the Gi interface for inbound traffic from the Internet to the target.

Cisco 7600 Series Router LI Performance

The following table summarizes the performance of the Cisco 7600 Series Router LI features:

Table 1. Cisco 7600 Series Router LI Feature Performance

7600 LI Feature	Release	Type of Tap Supported	Performance
Supervisor-based LI	12.2(33)SRB	Layer 3/Layer 4 tap (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB)	- 50 Bidirectional Taps (100 Unidirectional taps) - 6kpps–8 kpps @ 64 byte packets, depending on choice of Sup720/rsp720 (supervisor limited)

SIP-400 broadband LI phase 1	12.2(33)SRB	Access interface, dot1q vlan tap (CISCO-802-TAP-MIB, CISCO-TAP2-MIB)	- 150 subscribers (or taps) - 340Mbps
SIP-400 accelerated supervisor-based LI	12.2(33)SRC	Layer 3/Layer 4 tap (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB)	- Up to 500 simultaneous bidirectional taps (1,000 unidirectional taps • Up to 1 Mpps @ 64 byte packets if SIP-400 is running in nondedicated mode • Up to 5.5Mpps @ 64 byte packets if SIP-400 is running in dedicated mode

Mapping of GGSN RADIUS Parameters for IRI and CC Control

The following tables list the RADIUS attributes that the LI mediation device may use to generate IRI and control the CC interception in the Cisco 7600.

Table 2. Access-Request

Attribute No.	Attribute Name	Description	IRI	Session ID
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.		NAS IP @
5	NAS-Port	NAS port allocated by GGSN		NAS port
7	Framed-Protocol	Indicates the type of protocol for this user		GPRS PDP context
30	Called-Station-Id	Identifier for the target network	Target network	
31	Calling-Station-Id	MSISDN in international format according to 3GPP 03.03 UTF-8 encoded decimal	MSISDN	
26/10415/1	3GPP-IMSI	IMSI for this user	IMSI	
26/10415/3	3GPP-PDP Type	Type of PDP context, e.g., IP or PPP	Type of PDP	
26/10415/6	3GPP-SGSN-Address	SGSN IP address that is used by the GTP control	SGSN address	
26/10415/7	3GPP-SGSN-Address	GGSN IP address that is used by the GTP control plane for the context establishment. It is the same as the GGSN IP address used in the GCDRs.	GGSN address	

26/10415/8	3GPP-IMSI-MCC-MNC	MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI)	IMSI-MCC-MNC	
26/10415/10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion	NSAPI	
26/10415/18	3GPP-SGSN-MCCMNC	Contains the RAI form Create PDP Context Request and Update PDP Context Request	MCC MNC LAC RAC	
26/10415/20	3GPP-IMEISV	International Mobile Equipment Identity and its software version	IMEISV	

Table 3. Access-Accept

Attribute No.	Attribute Name	Description	IRI	Session ID
8	Framed-IPAddress	IP address allocated for this user, if the AAA server is used to allocate IP address	Target IP @	Target IP @

Table 4. Accounting-Request START

Attribute No.	Attribute Name	Description	IRI	Session ID
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server		NAS IP @
7	Framed-Protocol	Indicates the type of protocol for this user		GPRS PDP context
8	Framed-IPAddress	User IP address	Target IP @	Target IP @
30	Called-Station-Id	Identifier for the target network	Target network	
31	Calling-Station-Id	MSISDN in international format according to 3GPP 03.03 UTF-8 encoded decimal	MSISDN	
26/10415/1	3GPP-IMSI	IMSI for this user.	IMSI	
26/10415/3	3GPP-PDP Type	Type of PDP context, e.g., IP or PPP	Type of PDP	

26/10415/6	3GPP-SGSN-Address	SGSN IP address that is used by the GTP control	SGSN address	
26/10415/7	3GPP-SGSN-Address	GGSN IP address that is used by the GTP control plane for the context establishment. It is the same as the GGSN IP address used in the GCDRs.	GGSN address	
26/10415/8	3GPP-IMSI-MCC-MNC	MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI)	IMSI-MCC-MNC	
26/10415/10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion	NSAPI	
26/10415/18	3GPP-SGSN-MCCMNC	Contains the RAI form Create PDP Context Request and Update PDP Context Request	MCC MNC LAC RAC	
26/10415/20	3GPP-IMEISV	International Mobile Equipment Identity and its software version	IMEISV	

Conclusion

This white paper presented two solutions to intercept mobile targets in the Cisco GGSN based on Cisco SII architecture. The first solution integrates the IMSI mobile subscriber identity filter in the GGSN. This filter remains static for every connection of the target. This solution simplifies the LI mediation device activation process. The second solution reuses the LI functions of the Cisco 7600 Series Router. It requires the LI mediation device to discover the dynamic IP filters that are associated to the target during the activation of the PDP context. The two solutions enable the interception of roaming targets and direct tunnel connections between the Radio Access Network and the GGSN.

Acknowledgments

Maurice Duault
Consulting Engineer
Maurice has been working as a technical Consulting Engineer with the Cisco European organization for 10 years, specializing in Voice over IP, Next Generation Networks. He is the rapporteur of an European Telecommunications Standards Institute (ETSI) specification on Lawful Interception; Interception Domain Architecture for IP Networks.

Patrice Nivaggioli
Consulting Systems Engineer
Patrice has been working as a technical Consulting Systems Engineer with the Cisco European Service Providers organization for 9 years, specializing in Mobile Networks. He is currently focused on designing Service Control architecture for mobile access networks, such as 3G, HSPA, and Wimax, as well as defining the migration path toward Evolved Packet Core as specified in 3GPP Release 8.

Glossary

The following list provides expansions for acronyms and initialisms used in this document:

IAP: Intercept Access Point

CC: Content of Communication

ESN: Electronic Serial Number

IMSI: International Mobile Subscriber Identity

IRI: Intercept-Related Information

LEA: Law Enforcement Agency

LI: Lawful Interception

MIB: Management Information Base

MSID: Mobile Station Identification

NAI: Network Access Identifier

SNMP: Simple Network Management Protocol

References

[1] RFC3924, Cisco Architecture for Lawful Intercept in IP Networks

[2] ETSI TR 102 528 Interception Domain Architecture for IP networks

[3] ETSI ES 201 671 Handover Interface of telecom traffic

[4] ETSI TS 102 232 Handover for IP delivery

[5] 3GPP TS 33.106: Lawful Interception requirements

[6] 3GPP TS 33.107: Lawful interception architecture and functions

[7] 3GPP TS 33.108: Handover Interface for Lawful interception

This document is part of the Cisco Security Intelligence Operations.

Back to Top

Cisco Security Intelligence Operations

Contacts | Feedback | Help | Site Map