iMediator

Development of IP Technology and Lawful Interception on Internet Access

Legacy voice switch technology is always the core of electronic communication from the age of PSTN to mobile phone network nowadays. By fast progress with technology of IP network, it is a trend that most people communicate each other through application service platform (E-Mail、MSN or Whats App...etc) by Internet access, so do criminals.

It is absolutely necessary and mandate to conduct lawful interception (LI) operation on internet access service based on the justice causes of cyber crime investigation and home land security. Though there is difference between IP network and voice switch network in term of technology, legal liability of lawful interception operation on IP network is the same with that on voice switch network:

"Internet service provider should offer communication content and information of target to law enforcement agency"

To fulfill state LI mandate, it is obliged for all internet access service providers (ISP) to transmit IP packets (communication content) and access log (information) of target subscribers to remote monitoring facility of law enforcement agency. Without appropriate solution to meet such requirement, it will definitely prevent development of business and technology of IP access.

Solution from Decision Group: iMediator

For requirement of public interest and advanced technology, DG provides the complete solution: iMediator, which comes with complete functionality of mediation device under three tiers of standard ETSI architecture. It has below features:

- Telco Grade

In order to meet the telco reliability requirement, solution can be implemented by Active/Active or Active/Standby configuration of HA deployment in the core network of ISP POP center. For rapid growth of LI capacity align with traffic, solution can be simply expanded by adding more server systems.

- Multiple Access Type Support

Since most ISPs provide multiple access solution for subscribers (such as xDSL, Cable ,FTTB, 3G WCDMA...), the correspondent core network structure varies. For example, the network edge router is usually BRAS in wired ISP while 3G GPRS relies on SGSN for the same purpose. iMediator supports all of them by the single system.

-Flexible Interception Adaptor Architecture

Mediation device should be integrated with internal LI module (active interception) of the major network devices; however, different network device vendor provides proprietary interface (X interface) for filtering packets and filtered packets delivery. iMediator has different adaptor for each proprietary interfaces.

When the network device has no internal LI module, there exists the correspondent adaptor to control IP probe for filtering packets. iMediator can enable multiple adaptors simultaneously that fits the ISP having a multi-vendor network .

Internet Access and its LI implementation byiMediator

- Access Network and Core Network

There are two major domains for Internet access service implementation: The first one is access network, which can be networks of Cable, xDSL, FTTx, 802.16e(WiMAX) or 3G WCDMA; the second one is the core network. Generally speaking, different access networks can be connected with core network by edge devices, such as B-RAS.

- Control Plane and User Plane

Core network in ISP POP center can be divided conceptually into three areas: Control Plane, User Plane and Management Plane. Control Plane plays the role of transmitting control messages among different network devices, User Plane transmits data packets for Internet behaviors made by subscribers, and Management Plane is in charge of network management of both Control Plane and User Plane. Sometimes, User Plane is called Data Plane or Bearer Plane.

Subscriber must pass through the authentication process of ISP, i.e. entering correct account and password in the terminal device, such as xDSL modem, and will

be assigned a legal IP address. By this IP address, the subscriber can access Internet or communicate with other IP address. Once subscriber login in ISP network, there will be some associated communication information for that session, such as accounting event, network usage, time stamp, and access position ...etc, generated by some network devices. The above are the procedures of Authentication/Authorization/Accounting through RADIUS protocol within Control Plane.

- Relation between IP packets and accounting messages

IP packets are exchanged for web pages browsing or Facebook surfing made by ISP subscribers: from IP address of subscriber to remote IP address (Tx packets) and from remote IP address to IP address of subscribers (Rx packets). These data packets are within User Plane and pass through multiple network devices in core network.

However, it is hard for network devices to identify which subscriber is related to which IP packets in User Plane. To identify account ownership, the IP address distributed to that account is either the source or the destination of those packets, is to go through information in RADIUS message within Control Plane.

- Thumb of rules for LI in ISP network

Lawful interception on Internet access service, by the same principle of voice LI, should be conducted by the following way:

Target-based interception: the target identity can be the subscriber account in wired Internet ISP or MSISDN (mobile phone number) in 3G GPRS.

ISP should submit the packets of the User Planes owned by that target account only.

ISP should also submit the sufficient correlation information to assist monitoring facility to classify data from Control Plane and User Plane by targets.

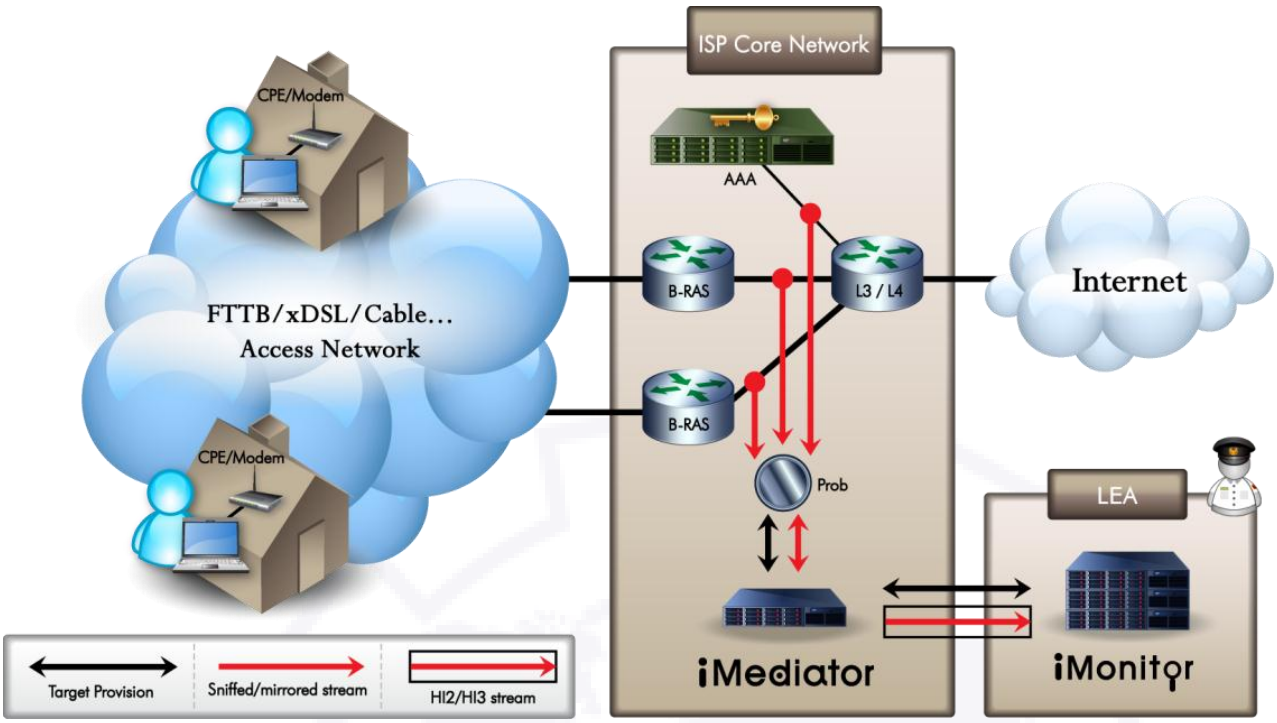
- Enable lawful interception with iMediator

Some network devices are equipped with their own internal LI module for filtering data by targets and we call it "active interception" (or internal Interception function, IIF). If network devices come without such function, iMediator can filter the packets with IP Probe, we call it "passive interception".

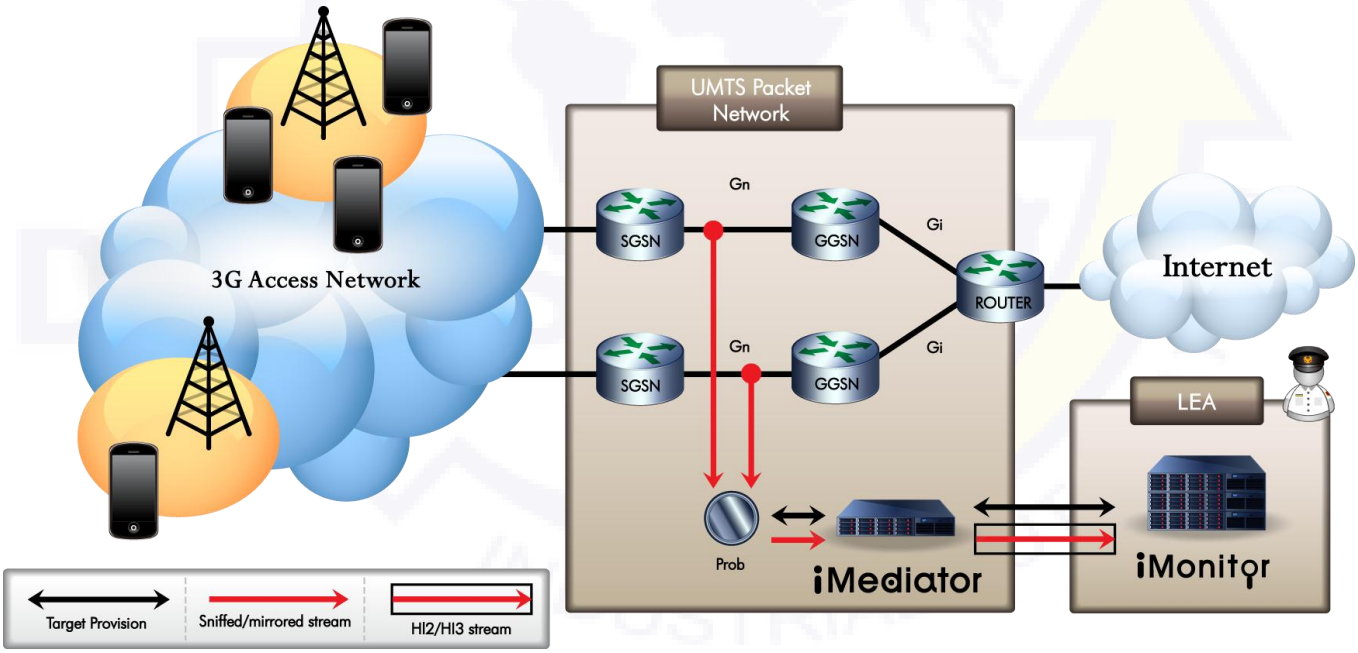
Due to less traffic within Control Plane, it is recommended to intercept all AAA messages within Control Plane through the sniffer between B-RAS and AAA system or by forwarding AAA message from B-RAS/AAA systems to iMediator. As for IP packets within User Plane, those can be intercepted no matter by active interception or passive Interception.

IP packets can be transmitted by the way of tunnel, and it must be handled with care especially for passive interception: taking example of 3G PS network, GTP tunnel between SGSN and GGSN, whereas GRE tunnel between ASN-GW and HA of WiMAX. In such case, iMediator with IP probe is able to de-tunnel packets first.

(Fig 1: Active interception under User Plane of Wired ISP)

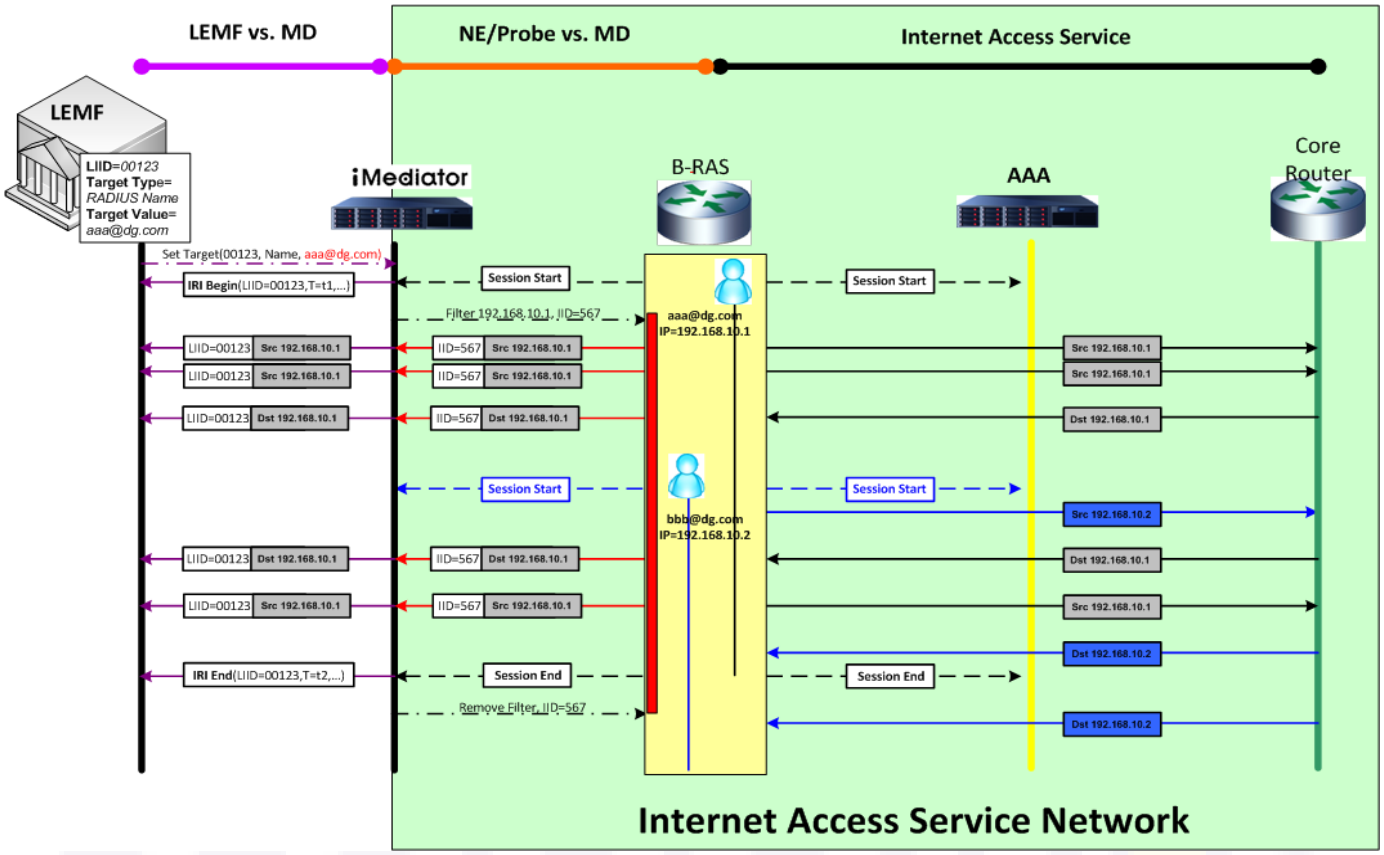


(Fig 2: passive interception under User Plane of Wired ISP)



(Fig 3: passive interception under both User Plane and Control Plane of 3G network)

Taking example of active interception on the architecture in fig 1, the flow chart of lawful interception is as following by the assumption of one specific target of two parties:



The principles of network devices chosen for interception are following:

1. If there are some core network edge devices which have internal LI modules, they can be selected to execute the active interception process. However, the filtering criteria of the target should apply on all of them except the route of target packets are known.

2. If some traffic may not passes through those network devices with internal LI modules, we must choose passive interception so that to deploy TAPs or enable port mirroring to make sure all those traffic into IP probe.

3. Ethernet interface is preferred if passive interception is adopted.

Advanced Application of iMediator: Subscriber Behavior Discovery

It is the routine process for telecom operators to retain subscriber activity log for certain period in order to review later on. It could be required by customer service department or for internal auditing and state mandate. In telephony service, subscriber activity log is just CDR, which can be retrieved from voice switch within Control Plane, also used for billing purpose. It is doubtless that CDR retention has been done for a long time while retaining subscriber activity log for ISP is a new demand.

- Accounting message retention for ISP

The straight idea is adopting the lesson learned from telephony：to retain RADIUS accounting message, like CDR, within ISP Control Plane with information of online time, offline time and location ...etc. iMediator can make this for ISP：to save all accounting message into the database with a convenient enquiry mechanism although it is not a part of lawful interception practices.

The enquiry mechanism is as following two:

1. Retrospective Tracking

Due to dynamic assignment of IP address, online IP address of the same subscriber is not persistent. When network management staff of ISP found abnormal activities of certain IP address, or police find certain IP address involved crimes in the scope of the same ISP, network management staff and police can find account identity easily by the query: (IP, time)-to-ID.

2. Real-time Reverse Tracking

For the value-added web sites hosted by the ISP, it is better to provide single sign-on service to grant transparent login to subscribers. iMediator can provide online IP-to-ID API to identify subscribers to assist the single sign-on service cross web sites.

- Accounting message retention for ISP

However, the accounting messages cannot represent the whole picture of subscriber behavior. For example, which website or which online services (MSN, BBS, Facebook or FTP...etc) the specific subscribers access cannot be acquired through AAA within Control Plane in ISP. In the same time, only L3 or L4 information can be identified by network devices within User Plane (IP address and port), so those L7 application-layer information, such as which web sites or services are accessed, is not recognized.

ISP is only the Internet gate keeper while knowing little about the exact behaviors of their subscribers. It is truly a pity. Most telecom operators, ISPs

included, take raising ARPU as the key mission. However, the correspondent strategy cannot be formed without understanding the subscriber behaviors.

For this approach, iMediator can perform subscriber behavior discovery by adding eDecision module by leveraging passive interception:

1. Correlate data within User Plane and Control Plan
2. Abstract packet header information from L2 to L7 into the structured format
3. Content indexing of L7 packet payload

- Burden to Investment

It is legal obligation for ISP to deploy the mediation devices without any business benefits. Once ISP chooses to deploy iMediator, the subscriber accounting message retention and IP-to-ID mechanism are implemented; the valuable information of subscriber online behavior could be taken through eDecision module. iMediator can fulfill LI requirement by mandate with potential constructive investment on marketing for ISP.

Product Specification of iMediator

- Target Type
  - ISP account/RADIUS
  - CPE MAC address/RADIUS
  - IP address
  - MSISDN/GTP-C
- Packet Pre-processing

  - GTP-C, GTP-U, RADIUS….

- Interception Adaptor:
  - Passive Interception: DG certified IP Probe
  - Active Interception : L3/L4 switch, B-RAS,GGSN,HA
- Data Delivery for LEMF
  - Proprietary Handover Interface: DG Handover Interface
  - ETSI TS 102 232-1/3/5
  - ETSI ES 201 671
- Capacity per 1U server
  - Concurrent Target: Max 300 targets
  - Provision Targets: 5000 targets
- High Availability
  - Active/Active
  - Active/Stand by
- Basic hardware spec
  - HP DL380G: CPU 2.4GHz, 16GB DRAM, 300G SAS HDD
  - DG certified IP probe, only for passive interception
- Options
  - Strategic E-Detective
  - IP-reversing Module
  - e-Decision Module

Decision Group Inc.
Address: 4/F No. 31, Alley 4, Lane 36, Sec.5,
Ming-Shan East Road Taipei, Taiwan.

Phone: +886227665753
Fax: +886227665702
Sales Email: decision@decision.com.tw

Global Website: www.edecision4u.com
Chinese/Traditional Website:
www.internet-recordor.com.tw