Document Type: Technical Report
TITLE: Location Acquisition and Location Parameter Conveyance for Internet Access Networks in Support of Emergency Services
DOCUMENT NUMBER: ATIS-XXXXXX.
SOURCE: Emergency Services Interconnection Forum
CONTACT: Anand Akundi, Telcordia Technologies, (732) 699-6031; Christian Militeau, Intrado Inc., (720) 864-5245

1.1 Abstract

This document describes the specific areas of location acquisition and location parameter conveyance in Internet access networks. It concerns itself with both the architectures and protocols for supporting these functions. In brief, this is about the manner in which IP devices such as VoIP clients request location information from a LIS function in any access network – location acquisition. It is also about the manner in which the LIS function obtains the value of parameters from access networks pertinent to the IP address of the requesting IP device in order that it can actually calculate the device's location.

The LIS function is identified as an essential component of the NENA-defined i2 architecture for VoIP emergency services and continues to be required in the i3 architecture currently under definition. This document starts with the LIS requirements specified by NENA in terms of those architectures. It examines candidate protocols for location acquisition – HELD, DHCP, LLDP-MED – and provides a gap analysis.

The concepts of location parameter conveyance are described and a specific architecture – the LIS-ALE architecture – is elaborated on. A flexible LIS-ALE protocol is described – FLAP – and examples are provided of its application in some common forms of broadband access networks.

This technical report is intended to be used as input to further decision-making processes leading to any necessary policy and/or American National Standards formulation. It will be used as a vehicle for communicating concepts in liaisons with other relevant SDOs.

1.2 Notice

Document ATIS-XXXXXX.
Prepared by
Emergency Services Interconnection Forum
Working Group
Next Generation Emergency Services Subcommittee (NGES) Issue 50

ATIS-XXXXXX

Location Acquisition and Location Parameter Conveyance for Internet Access

Abstract

This ATIS Technical Report is not intended to be seen as an American National Standard. Rather it is intended to be used as input to further decision-making processes leading to any necessary policy and/or American National Standards formulation. It will be used as a vehicle for communicating concepts in liaisons with other relevant SDOs.

This document describes the specific areas of location acquisition and location parameter conveyance in IP access networks. It concerns itself with both the architectures and protocols for supporting these functions. In brief, this is about the manner in which IP devices such as VoIP clients request location information from a LIS function in any access network – location acquisition. It is also about the manner in which the LIS function obtains the value of parameters from access networks pertinent to the IP address of the requesting IP device in order that it can actually calculate the device's location.

The LIS function is identified as an essential component of the NENA-defined i2 architecture for VoIP emergency services and continues to be required in the i3 architecture currently under definition. This document starts with the LIS requirements specified by NENA in terms of those architectures. It examines candidate protocols for location acquisition –DHCP, LLDP-MED, HELD – and provides a gap analysis.

The concepts of location parameter conveyance are described and a specific architecture – the LIS-ALE architecture – is elaborated on. A flexible LIS-ALE protocol is described – FLAP – and examples are provided of its application in some common forms of broadband access networks.

1.3 Foreword

The rapid rise of Voice over IP telephony services was anticipated by the National Emergency Number Association (NENA). In 2003, it established working groups to define a "migratory" architecture (i2) and an "end game" architecture (i3) to provide the ability to reliably deliver and process emergency calls originated by Internet-based VoIP telephony users. Both the i2 and i3 architectures depend on the ability to determine and communicate the location of the caller so that a) the call can be routed to the correct PSAP and b) the location can be delivered to the PSAP operator for dispatch and other procedural purposes. The network element identified to perform this function is associated with the access network used by the VoIP caller and is called the Location Information Server (LIS). NENA i2 documents define the LIS related requirements, and the form of location information provided, however they do not provide the detailed protocol specifications associated with LIS functionality.

In practice, the role of the LIS can be split into at least two key functions:

- Location acquisition – the protocol and associated semantics by which IP devices and applications request location information from the LIS.
- Location measurement and determination – the function and any associated protocols associated with obtaining and evaluating network and other parameters that are associated with the device in order to calculate the device's location. Getting these relevant parameters delivered from the network may be termed "location parameter conveyance".

In order to provide global consistency for devices such that location information can be retrieved in the same way regardless of the kind of network they are currently attached to, it is important that Location Acquisition is done in the same way independent of the technology underpinning that access network. On the other hand, the parameters important to location determination, the manner in which location is calculated, and the form of location (e.g. civic and/or geodetic) will vary significantly depending on the nature of the access technology. That is, the parameters and algorithms associated with determining location in an ADSL network will be significantly different than doing the same in a WiMAX network. By definition, then, location acquisition is ideally network technology independent while location parameter conveyance and determination is network technology dependent.

1.4 Revision History

Revision	Date	Remarks
.01	July 5 2006	Version .01 skeleton document for group discussion
.02	July 19 2006	Added NENA acquisition protocol requirements matrix
0.3	Sept 11 2006	Added example for DSL
0.4	21 Sept 2006	Added examples for cable, 3G Cellular
0.5	22 Sept 2006	Added examples for wired Ethernet
018-R3	October 3, 2006	Added sections 4 – 7
018-R4	October 11, 2006	Continued editing process throughout the document, added Definitions and Acronyms sections
018-R5	October 25, 2006	Completed sections on WiMAX and WiFi. Address action points

		arising from detailed review conducted at ESIF-19 meeting. Added RELO to the location acquisition protocol comparison matrix.
018-R6	November 8, 2006	Further updates to diagrams and text following review. Added LREP-SIP to the location acquisition protocol comparison matrix.
018-R6.1	November 8,2 006	Tweaks to existing text throughout the file, all of which are subject to review prior to being “accepted”.
018-R7	November 29, 2006	More review comments incorporated. Added LCP as yet another candidate acquisition protocol.
050-002	December 6, 2006	New baseline document created from all prior work, most recently from 018-R7
050-002-R1	December 7, 2006	Deleted Section 3 (Definitions) by group consensus, which resulted in all section beyond #3 being renumbered, i.e. 4 became 3 etc. Also added some Comments to remind us of intended Action Items, added entries to the Abbreviations, Acronyms, and Symbols table, and alphabetized it, and a few other editorial corrections.
050-002-R2	December 21, 2006	Liaison distribution version

Table of Contents

Table of Figures

2 Introduction/Executive Summary

The NENA VoIP migratory working group defined the i2 network architecture designed to support emergency service calls originating from VoIP services on the Internet. The architecture identifies a network element called the Location Information Server (LIS) that provides location data used for call routing and for display at the PSAP operator terminal.

The i2 specification did not detail the protocol to be used by the LIS for providing location information to the VoIP device or proxy nor the manner in which location should be determined for different Internet access technology types. A separate NENA document [18] defined the requirements for the LIS. NENA requested ATIS/ESIF to provide recommendations for the protocol and implementation specifics of the LIS function for the broadband access and emergency services industry.

This document divides the subject into two areas. The first is “Location Acquisition” which describes the manner in which LIS clients interact with the server to obtain location. Candidate location acquisition protocols (DHCP, LLDP-MED, HELD, and RELO) are compared against the NENA defined requirements. The second area is “Location Determination” which is the manner in which a LIS determines the location of a device in specific access network types. A variety of access technologies are examined and a generic architecture based on access location entities (ALE) providing network parameters to the LIS is described. A protocol called the Flexible LIS-ALE Protocol (FLAP) is described which supports this architecture.

The results of the location acquisition protocol comparison and the description of the LIS-ALE architecture and FLAP protocols are provided as a basis for discussion and decision-making. Input from a range of SDOs in response to this document is to be sought.

2.1 Target Audience

This document is directed to the members of the NGES subcommittee dealing with Issue 50 and tasked with progressing recommendations around policy and standard formulation. It provides a technical overview of the scope of issue and specific terms of reference currently viewed as significant to progress. It is also directed towards those members of third party SDOs who may be in receipt of liaisons from this subcommittee requesting input in the form of opinion, information, or decisions pertinent to the subcommittee’s ability to progress the work associated with the issue.

3 Abbreviations, Acronyms, and Symbols

Term	Brief Definition
ALE	Access Location Entity
ATM :	Asynchronous Transfer Mode
BEEP	Blocks Extensible Exchange Protocol (RFC3080, RFC3081)
BRAS :	Broadband Regional Access Server
BSSLAP	Base Station System Location Assistance Protocol
CMTS :	Cable Modem Termination System
DHCP	Dynamic Host Configuration Protocol (44)
DSL :	Digital Subscriber Line (44)
DSLAM :	DSL Access Module
FLAP	Flexible LIS-ALE Protocol
GGSN :	Gateway GPRS Support Node
GMLC	Gateway Mobile Location Center
GPRS :	General Packet Radio Service
HELD	HTTP Enabled Location Delivery (43)
ISP :	Internet Service Provider
L2TP :	Layer 2 Tunneling Protocol
LIS	Location Information Server
LMU :	Location Measurement Unit
MAC :	Media Access Control
NAS :	Network Access Server
PVC :	Permanent Virtual Circuit
RANP :	Regional Access Network Provider

Term	Brief Definition
RBP :	Regional Broadband Provider
SGSN :	Serving GPRS Support Node
SLP	SUPL Location Platform
SMLC	Serving Mobile Location Center
SNMP :	Simple Network Management Protocol
SUPL	Secure User Plane Location
VESA :	Valid Emergency Service Authority
VPC :	VoIP Positioning Center

1

2

4 NENA i2 and i2 Architecture

Overview description

The NENA i2 initiative [01] was proposed with the intent of addressing the immediate need of providing standard emergency services support to next generation Residential Broadband VoIP phone users. A strong requirement of i2 from the onset was to make little or no change to the existing emergency infrastructure, in particular any solution was to impose no change to PSAPs. The data sets associated with location of an IP device, when investigated further were found to be remarkably similar to location parameters associated in wireless cellular networks. The resulting architecture for i2 therefore closely resembles the architecture created to address the wireless Phase II emergency requirements

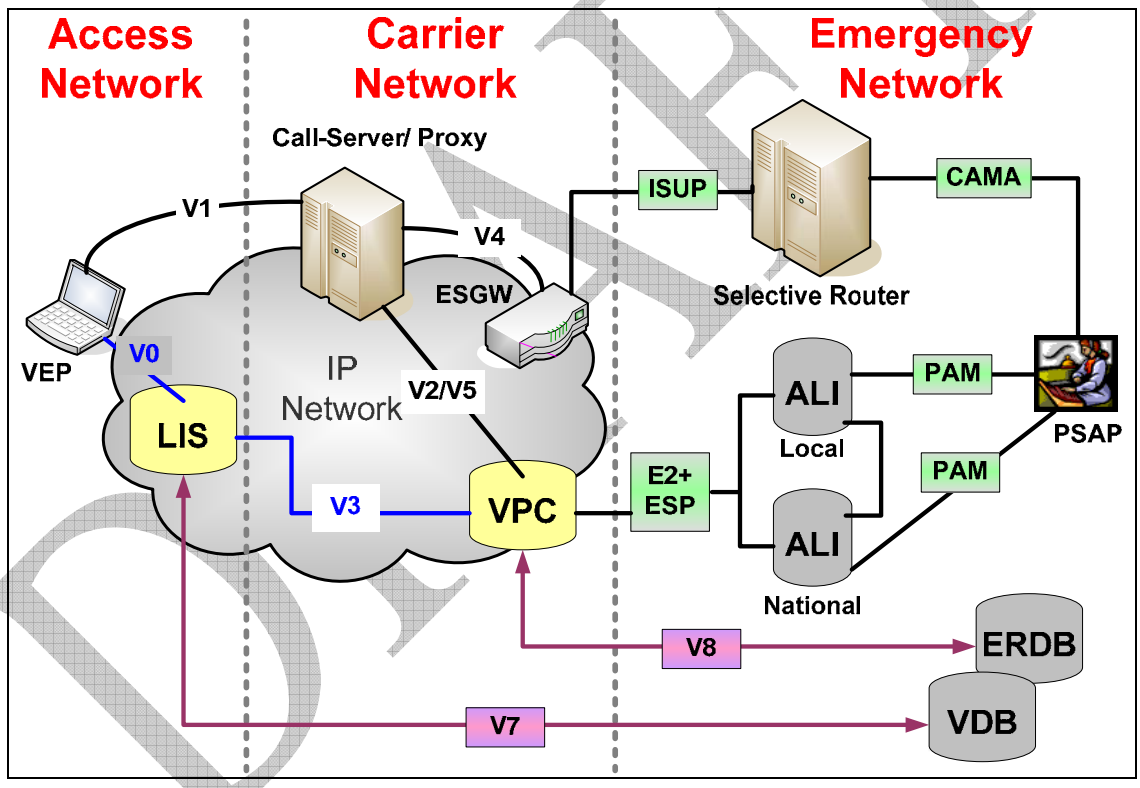


Figure 4-1 NENA i2 architecture

The NENA i2 architecture (see Figure 4-1) identified 5 new network elements, 9 new interfaces, and made minor changes to the E2+ to support VoIP class of service indicators between the new VoIP Positioning Center (VPC) and the existing ALI infrastructure. While the detailed functions of each of the new 5 network elements is defined in the i2 specification, not all of the interfaces between nodes are specified. Specifically, the V0 and V1 interfaces were deemed out of scope for i2.

There are three key components of the i2 architecture that the VoIP service interacts with and which would benefit from global adoption:

- The manner in which the VoIP device obtains and provides location information to the call server (the LIS)
- The manner in which the VoIP call server proffers location information in exchange for routing information and for delivery to the emergency services network (the VPC)
- The manner in which the VoIP call server routes the call out of the Internet and into the emergency network of the destination jurisdiction (the ESGW)

The V2 interface to the VPC is well described and specified in the i2 architecture document. Similarly the function of the ESGW is well understood. By the same token, these elements are the ones which have the most scope for regional variance. In the US, the VPC is queried by the PSAP via the E2 interface. Other jurisdictions may use other protocols such as MLP. In the US, the ESGW provides dedicated trunks to selective routers. In other jurisdictions, the ESGW may route the emergency call onto the PSTN. In addition, the VPC and ESGW are migratory solution constructs. They don't necessarily have a long term role into a future where emergency calling occurs on IP end-to-end between VoIP devices and VoIP enabled emergency call centers.

In contrast to the VPC and ESGW functions, the LIS interfaces (V0 and V1) have the least level of detail in the i2 specification. The V1 interface is recognized to be VoIP-protocol specific so the only requirement cited by i2 is the ability of that interface to convey location in the form of a PIDF-LO or as a reference. The LIS function can and should be consistent on a cross-national jurisdiction basis. This means a device can acquire location information in the same way regardless of the network to which it is attached. The LIS will continue to be relevant in the long term as the need to determine and acquire device location exists regardless of the call being delivered through a legacy infrastructure or on end-to-end IP.

This document focuses on the LIS functionality. It documents considerations and the recommendations of the ESIF NGES WG with respect to the implementation of LIS functionality.

4.1 Summary of LIS Functions in the NENA Architecture

While the i2 architecture did not elaborate on the form of the V0 interface protocol(s) or the manner in which the LIS is expected to determine device location, the i2 working group did provide supporting technical documents describing the requirements for the V0 interface and for the LIS function [18].

The requirements for the LIS were divided into three areas

- Location determination and acquisition (DA)
- Location representation (Rep)
- Location security and dependability (LocSec)

The following section lists these requirements.

4.2 LIS Requirements Prescribed By NENA

The following requirements come from the NENA Requirements for the location information to support emergency services [18].

DA1– The access network shall provide a mechanism for determination and acquisition of location information, and support queries for location.

DA2 – The location estimate used shall be that associated with the physically (wire, fiber, air) connected network.

DA3 – Location may be requested at any time. Location information must be associated with the device at the time the location is requested.

DA4 – Location acquisition should be provided by a consistent method across all network configurations.

DA5 – Location determination and acquisition mechanisms should be applicable to emergency calling; they may also be applicable to a wide range of value-added location-based services.

DA6 – Location determination and acquisition techniques shall support both NENA i2 and i3 network architectures.

DA7 – When measurement-based location determination mechanisms fail, the most accurate location information available should be provided. Examples include: For mobile, the Wireless Service Provider might provide tower/Access Point location, last known fix, etc. For wireline, a LIS might provide a civic location that defines the serving area of an access point, e.g., the State of Texas.

DA8 – Location determination and acquisition must have minimal impact on call setup time in the event that location is not known ahead of time.

DA9 – Where a device is not location aware, the network should have the ability to assert a location estimate on behalf of the device.

DA10 – Location acquisition methods should not require modification of hardware/firmware in home-routers/modems.

DA11 – A location determination method must exist that does not require network hardware replacement in the core network.

DA12 – The location acquisition protocol shall allow the requesting device to specify a response time requirement to the LIS when requesting location information. The response time is expressed as the maximum time that the requesting node is prepared to wait for location information. The LIS is required to provide the most accurate location fix it can within the specified response time.

Rep1– Location information may be provided by-value or by-reference; the form is subject to the nature of the request.

Rep2 – Location determination and acquisition mechanisms must support all location information fields defined within a PIDF-LO.

Rep3 – Location acquisition mechanisms must allow for easy backwards compatibility as the representation of location information evolves.

Rep4 – All representations of location shall include the ability to carry altitude and/or floor designation. This requirement does not imply altitude and/or floor designation is always used or supplied.

LocSec1– Location information shall only be provided to authenticated and authorized network devices. The degree of authentication and authorization required may vary depending on the network.

LocSec2 – Location determination and acquisition methods should preserve privacy of location information, subject to local laws and regulations applicable to the endpoint's geographic location.

LocSec 3 – The location or location estimate of a caller should be dependable.

LocSec4 – The location acquisition protocol must support authentication of the Location Information Server, integrity protection of the Location Information, and protection against replay.

LocSec5 – The location source shall be identified and should be authenticated. This includes manually entered locations.

LocSec6 – Where a location is acquired and cached prior to an emergency call, it SHOULD be refreshed at regular intervals to ensure that it is as current as possible in the event location information cannot be obtained in real time.

LocSec 7 – Where location by-reference is used, the appropriate privacy policies MUST be implemented and enforced by the LIS operator.

4.3 The NENA i2 architecture and global interoperability

The i2 architecture has relevance beyond the North American emergency services infrastructure. In traditional wireline and cellular networks, where the voice service provider and the access provider are the same entity there has been some latitude from one national jurisdiction to another in terms of how emergency calls are processed. In particular, the local network operator had full responsibility for emergency call processing in these traditional networks. As long as the user's device (e.g. GSM phone) was compatible with the dialing of emergency services, the rest of the process could be jurisdiction-specific. VoIP breaks this coupling between access and voice service provision and, in the case of emergency calling, it introduces cross-jurisdictional considerations that have not previously existed. For example, a caller may roam from one national jurisdiction to another but their VoIP service provider does not change. The same VoIP call server will be engaged in the processing of an emergency call regardless of the point of origination of the call. This requires the call server to successfully inter-operate with the emergency calling infrastructure of an arbitrary number of national jurisdictions. Subscribers don't even need to be roaming for this to occur since the subscribers to a VoIP service may be foreign nationals, and foreign-based, to begin with. Being able to support a global subscriber base also creates the requirement for a VoIP provider to inter-operate with the emergency infrastructure of multiple national jurisdictions.

Global inter-operability could be enhanced if the i2 architecture were widely adopted. The two key functions of emergency call routing and the delivery of location information that the i2 architecture provides are actually common to emergency services world-wide. Rather than requiring a call server implementation to adapt to an arbitrary number of systems, protocols, and interfaces, there is a major benefit if all jurisdictions adopt the same approach.

5 Location Determination in Broadband Access Networks

This section describes a range of access technologies and provides examples of how location determination is possible, and the key parameters that need to be captured in order to permit location determination.. The examples provided are illustrative and not comprehensive nor definitive. The descriptions of ADSL, cable, and 3G technologies are accurate in terms of representing actual deployment topologies and signaling scenarios though there is scope for variation in detail in the real world. WiMAX standards are still under definition by the IEEE and references to the types of network parameters that contribute to location determination and the signaling scenarios by which those parameters may be extracted from the network are more speculative.

Note that the term “access location entity” (ALE) is used in various parts of the following descriptions. This term is fully defined in Section 8 and the reader is referred to that section for background on this function. It is included so that the examples are more readily understood in the context of a general location parameter architecture. For the purposes of this section, the term “ALE” is used to identify a logical function and does not refer to a particular product, technology, or standard.

5.1 Example ADSL Network

Asymmetric Digital Subscriber Line (ADSL) is the fastest growing technology used to deliver residential broadband service in the world and boast about 140 million lines world-wide. Recommendations on DSL network configurations and protocols are provided by the DSL forum and these are documented in Technical Reports (TRs) that are freely available from the DSL forum website (www.dslforum.org).

The main DSL network configuration architectures are documented in TR-025 [15] and TR-101 [16] and the example network described in this section will come from one of the architectures described in TR-025. Other examples along with a high-level description of DSL network entities are provided in the NENA location determination TID [20].

5.1.1 DSL Connectivity Over L2TP

The basic DSL network configuration consists of a DSL modem at the customer's premises that transports IP traffic from residence to the Internet. The DSL signals from the modem are carried across copper wires to the local exchange where the DSL broadband signals are extracted from the copper pair and sent to a DSL Access Module, or DSLAM.

The DSLAM has a dedicated circuit path to a central aggregator for each connected line. In many cases this will be an ATM permanent virtual circuit (PVC), but in the case of an Ethernet transport it may be a dedicated Ethernet VLAN identifier.

The central aggregator in this configuration is generally referred to as a broadband regional access server, or BRAS. The BRAS terminates individual DSLAM data streams and redirects them to the end-point/subscriber’s Internet Service Provider (ISP). The BRAS determines which ISP to send any given data stream to, by using data configured directly into the BRAS or by using a RADIUS server as shown in the example below.

The links between a BRAS and an ISP's network access server (NAS) vary from ISP to ISP and BRAS to BRAS. The example network described in this section assumes that a single layer 2 tunnel (L2T) exists between the BRAS and the ISP's NAS, and that each end-point connected to the ISP has a session established inside the BRAS to NAS tunnel.

In this environment tunnel sessions are established dynamically when a connection is made from the end-point to the ISP. ***The inclusion of a dynamic component between the end-point and the ISP means that location cannot be resolved by only provisioning circuit chains from the end-point to the ISP.*** The problem is resolved by taking network parameters that provide a linkage between what the regional access network provider (RANP) knows and what the ISP knows. In other words, the LIS ultimately needs to correlate the IP address of the device with the residential address associated with the DSL connection the device is using. The DSL connection may be correlated with a number of access infrastructure circuit ID parameters finally culminating in the identity of an L2TP tunnel; however, this does not resolve to the IP address of the device. The ISP can provide additional information – specifically a correlation between the L2TP tunnel identity and the IP address of the device – to add to the information available to the access infrastructure provider. Together this information provides a linkage between the IP address of the end-point, the tunnel and session between the NAS and BRAS, and ultimately the circuit information from the BRAS to the DSLAM and the copper pair running to the premises where the end-point is housed.

A general network layout might look something similar to Figure 5-1

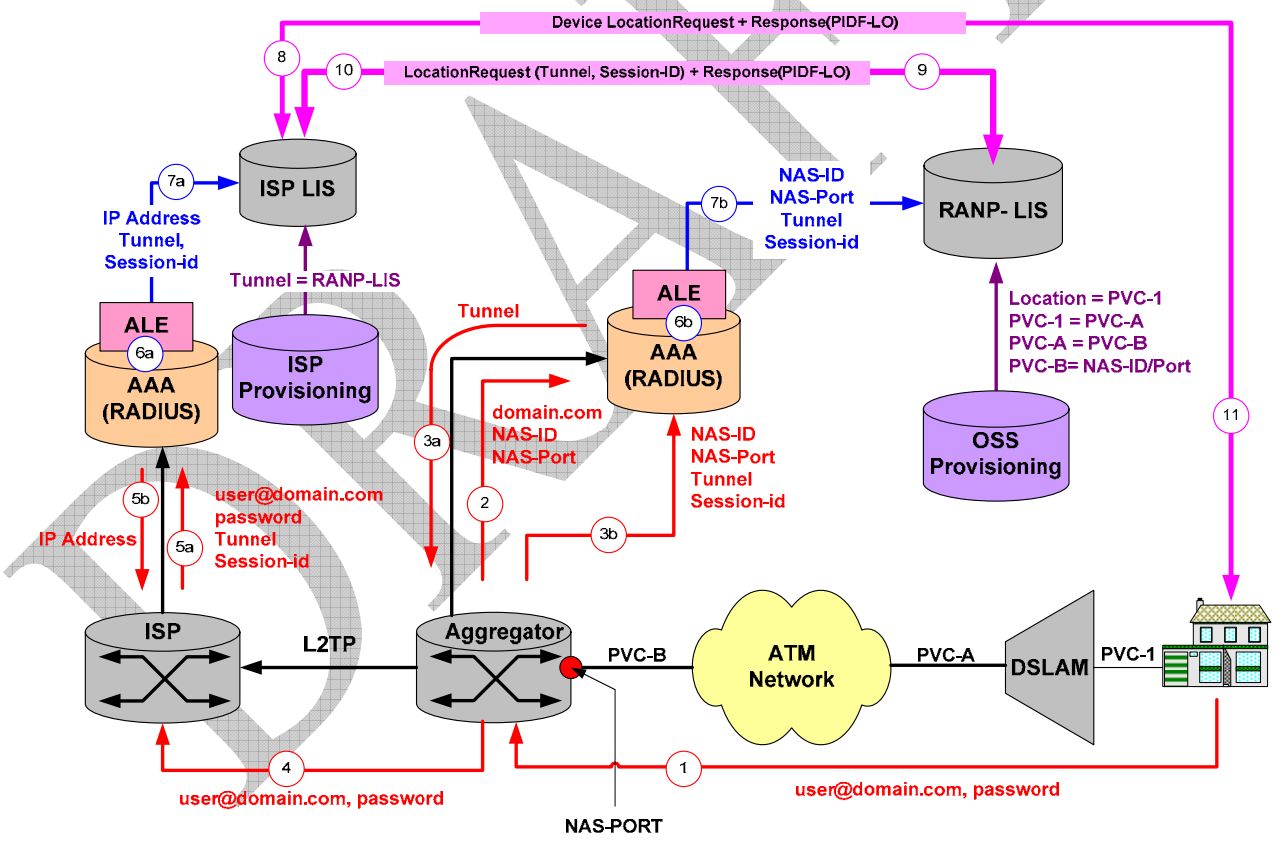


Figure 5-1 DSL Connectivity Using L2TP

In this configuration two LIS's are used, one at the ISP that provides a linkage between IP address and tunnel-session information, and second LIS in the regional access network that provides the mapping from tunnel-session information into a provisioned circuit chain that ultimately yields the location of the end-point. The message flows used in this configuration are provided in Figure 5-2, along with a detailed description of each flow.

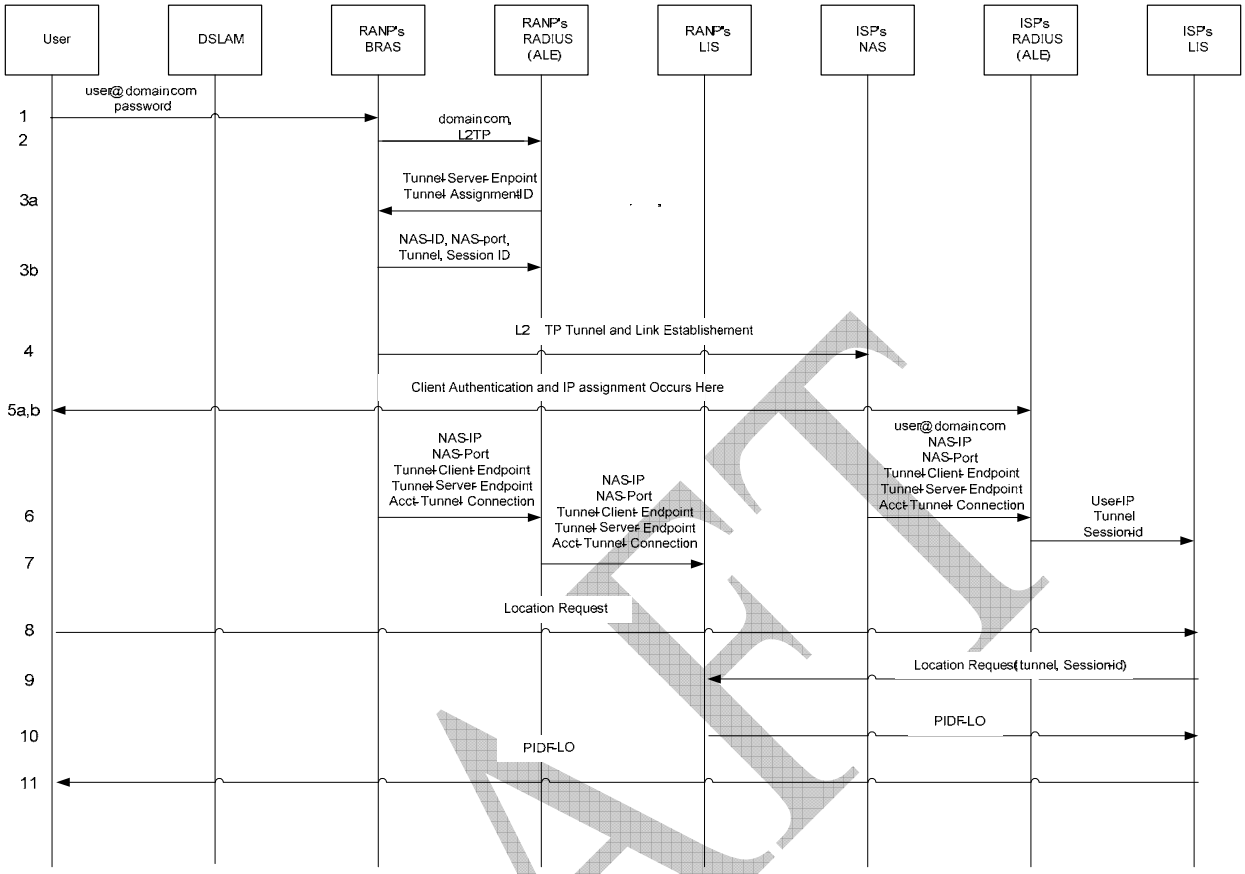


Figure 5-2 DSL L2TP Network Connectivity Message Flows

1. The user or end-point initiates a DSL connection, and passes network credential information to the RANP BRAS.
2. The BRAS requests assistance from a RADIUS server to determine which ISP NAS to send to the end-point data stream to.
3. a) The RADIUS server responds with a tunnel assignment. b) If there is no pre-existing tunnel, it is created and the RADIUS is provided the tunnel identity
4. A new session is created in the tunnel.
5. a) Authentication and authorization between the end-point and the ISP occurs. b) An IP address is provided for the device.
6. (a&b) The RANP BRAS forwards the incoming BRAS port, the BRAS identity, tunnel and tunnel session information to a RADIUS accounting server. This information is also received by the RADIUS ALE and forwarded to the RANP LIS.
7. (a&b) At the same time, the ISP NAS forwards the incoming NAS port, NAS identity tunnel, session and client IP address to a RADIUS accounting server. This information is also received by the RADIUS ALE and forwarded to the ISP LIS.
8. The end-point makes a request for location to the ISP LIS.
9. The ISP LIS uses the end-point IP address to determine the tunnel and session information. The ISP LIS uses the tunnel source information to determine which

RANP LIS to query. The ISP LIS sends a location request to the RANP LIS which includes the tunnel and session information.

10. The RANP LIS receives the location request with the tunnel and session information and this as a key to determine the incoming BRAS and BRAS port information. Once the BRAS and incoming port are identified, the location of the end-point can be determined as the link between BRAS, BRAS port and location is provisioned in the RANP LIS as shown in Figure 5-1. The RANP LIS constructs a PIDF-LO and return this to the ISP LIS.
11. The ISP LIS returns the PIDF-LO to the end-point.

5.2 Example Cable Network

Cable networks are made up of multiple cable modems connected onto a single broadcast cable. The bandwidth in the cable is divided into multiple frequency separated channels, and each channel is comprised of a series of timeslots. Cable modems compete with each other for channel and timeslot availability. A Cable Modem Termination System (CMTS) residing at the head-end of the network is responsible for controlling transmission characteristics such as channel and timeslot allocation for all cable modems in the network.

The CMTS is connected to a router that switches network traffic to an ISP. A cable network can therefore be thought of as a large distributed switched Ethernet network. This type of environment makes it less easy to support multiple ISPs as is done in DSL environments, though not impossible. Many cable network operators therefore either run the ISP themselves or provide exclusive access to a small number of dedicated ISPs, often one.

In most cases the CMTS and other switching devices can learn the MAC address of cable modems connecting to the network. There is a need in cable networks however to be able to associate a modem with a particular subscriber to ensure that the correct services are made available to the end point. This association is generally performed through registration and provisioning systems, which are often web-based, and provides the ISP with a mechanism to link modem MAC address with end-point/modem location.

The tight coupling between cable network providers and ISP and the required modem registration process place cable networks in a position where DHCP location acquisition becomes a viable choice. Problems exist however with the inability of cable operators to unilaterally upgrade subscriber modems or change hosts residing behind firewalls to be compatible with this acquisition method. In addition the inability to provide location dependability and compatibility with other network location solutions may cause cable ISPs to consider an alternate location acquisition solution.

Location determination in a cable network relies on the tie between Ethernet MAC address and physical location that is provisioned at the time the modem is registered to access the network. To use an acquisition protocol may require a mapping between the IP address and physical address, and this is accomplished in a cable network by establishing the binding between the IP address and MAC address. Since the cable network is DHCP based, a binding between MAC address and the IP address is available from the DHCP server, and can be retrieved in a number of ways including using an ALE based around the DHCP lease query protocol RFC4388 [21].

The network configuration to determine and provide location in a cable environment looks similar to Figure 5-3.

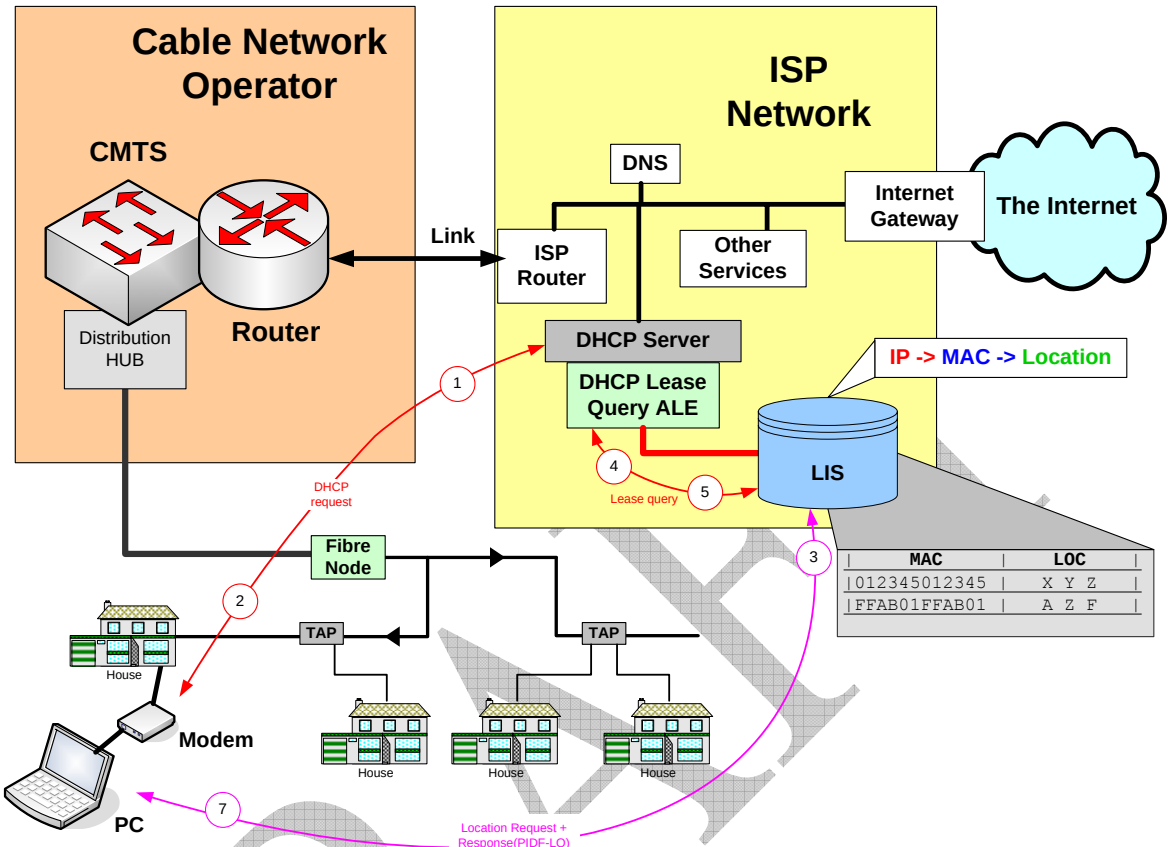
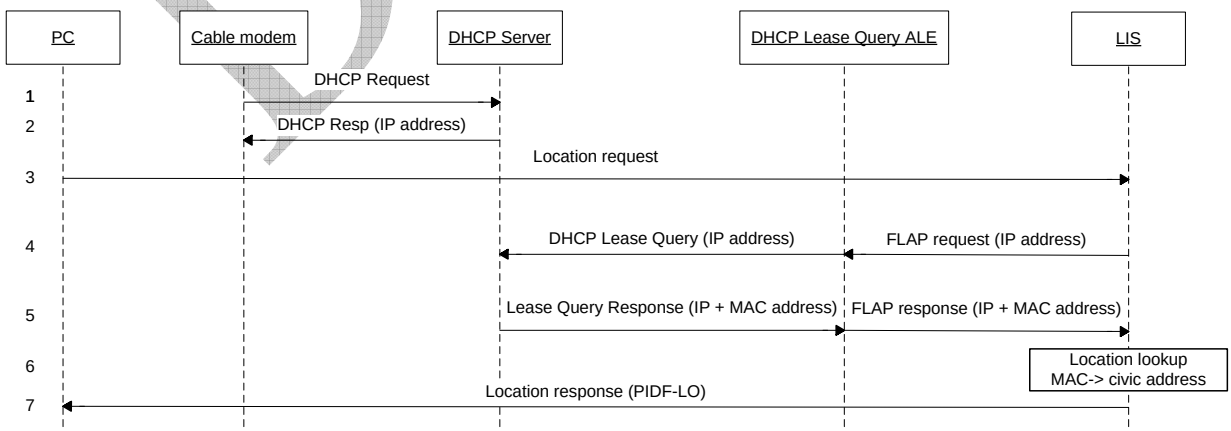


Figure 5-3 LIS In A Cable Network

The message sequence associated with location determination and acquisition in the cable network is shown in the following diagram.



1. The modem requests its IP address from the DHCP server. The DHCP server provides the IP address and caches the association with the modem MAC address. The modem was previously registered with the ISP, and the LIS is provisioned with the MAC address and location of the modem.
2. The client on the PC discovers the LIS and makes a location request.
3. The LIS receives the location request and requests an IP address to MAC address binding from the DHCP lease query ALE.
4. The DHCP lease query ALE receives the request and sends a lease query to the DHCP server.
5. The DHCP server responds with the corresponding MAC address, and the ALE passes this information up to the LIS.
6. The LIS uses the MAC address to look up the provisioned location.
7. The LIS constructs a PIDF-LO and returns this to the client running on the PC.

5.3 Example WiMAX Network

The label “WiMAX” applies to a range of wide area broadband wireless IP access technologies – most specifically related to those defined by IEEE 802.16 and 802.20 specifications. It can be characterized as a public access carrier version of WiFi with metro area coverage associated with a given wireless access point or base station. A WiMAX “cell” can cover an area that is a number of kilometers across. WiMAX may be used to provide fixed wireless access – where the technology is used to provide broadband service to fixed locations such as subscriber residences. It can also be deployed to provide mobile coverage such that users are provided broadband access from portable devices in arbitrary locations and while on the move.

In the fixed wireless deployment model, location can be associated with the wireless modem providing service for that fixed location. In this case WiMAX location service can be implemented in the same way as described for cable broadband in section 5.2. The LIS obtains the MAC address associated with the device from the DHCP server and consults the subscriber data to find the corresponding residential, or other fixed location, address.

In the mobile deployment model, the WiMAX network location determination solutions become more similar to traditional cellular location solutions. In order to determine the location associated with the IP address of a particular device, the LIS will need to find the network parameters that correspond to that device. As a starting point, it will want to determine the base station which the device is currently attached to. This basic information will allow the LIS to associate a geodetic area of uncertainty with the device which is equivalent to the area of coverage of that WiMAX base station. This is the WiMAX equivalent of a cell-based location in traditional cellular networks.

In order to further refine the location associated with the device, the LIS requires additional network parameter values. These include radio parameters such as channel information, signal time of arrival values, and signal strength measurements. Which WiMAX network parameters are pertinent to the calculation of location is a subject for further study and topic for consideration within the IEEE.

Obtaining the value of these parameters requires access parameter conveyance associated with the radio interface. This may be accomplished by native ALE functionality

in the WiMAX network controllers themselves or it may be provided through some overlay facility such as location measurement units (LMUs) as shown in Figure 5-4.

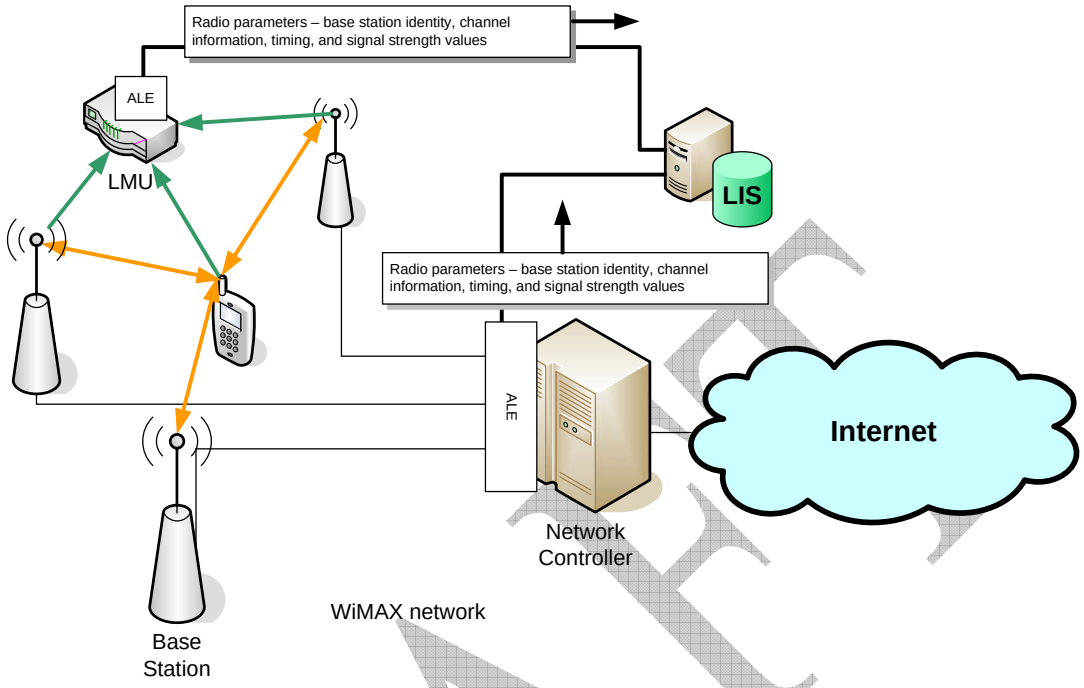


Figure 5-4 WiMAX network

A depiction of obtaining network parameters for the purpose of location determination from the network and location measurement units (LMU)

5.4 Examples of 3G Cellular Networks

In recent years cellular telephone networks have evolved to support high-speed packet data transmission that is used for Internet access. The type of traffic exchanged between the network and handset is separated out at the base station controller, with telephony traffic going to the MSC and packet data going to a packet serving node. This is shown in Figure 5-5.

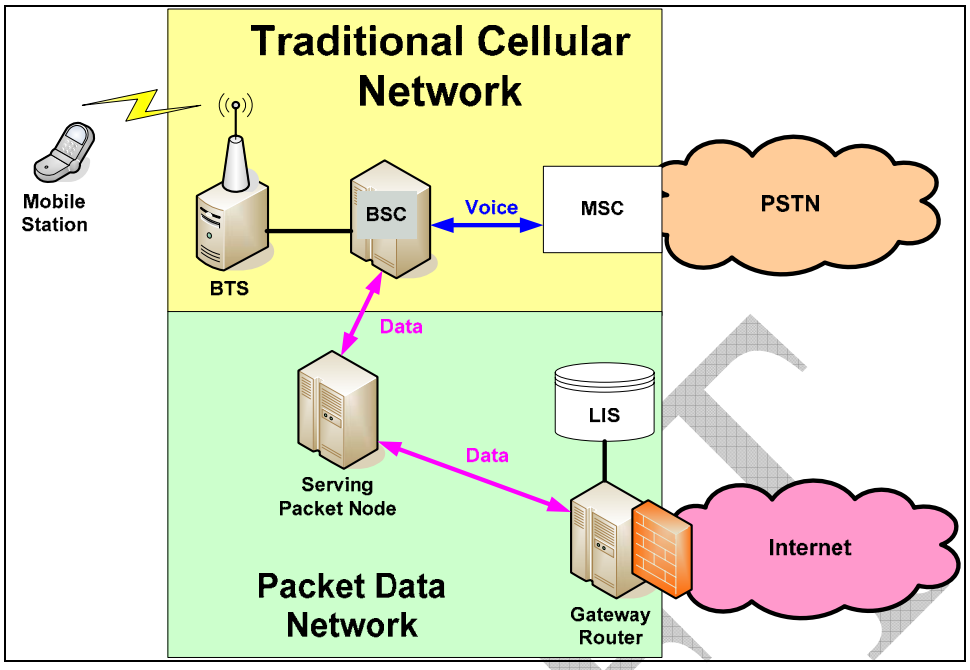


Figure 5-5 Data and Voice Separation In A Cellular Network

5.4.1 3G packet data variants deployed in the United States

The two main 3G packet data variants deployed in the United States are:

- UMTS, based on 3GPP GPRS standards
- 1xEVDO, based on 3GPP2 standards.

In this section we shall examine a GPRS solution, but the principles are also applicable to 1xEVDO. A full description of these networks is provided in [22].

GPRS introduces a number of new nodes to a GSM/UMTS network, the two main ones being the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) – see Figure 5-6.

The SGSN is analogous to a VLR/MSC In the cellular voice world. It is responsible for device authentication, authorization, registration and mobility management functions. The SGSN is also responsible for all protocol conversions that need to occur between the mobile air interface and the protocols used over the carrier's core network. All data sent by or to the mobile device in a GPRS network travels through the SGSN.

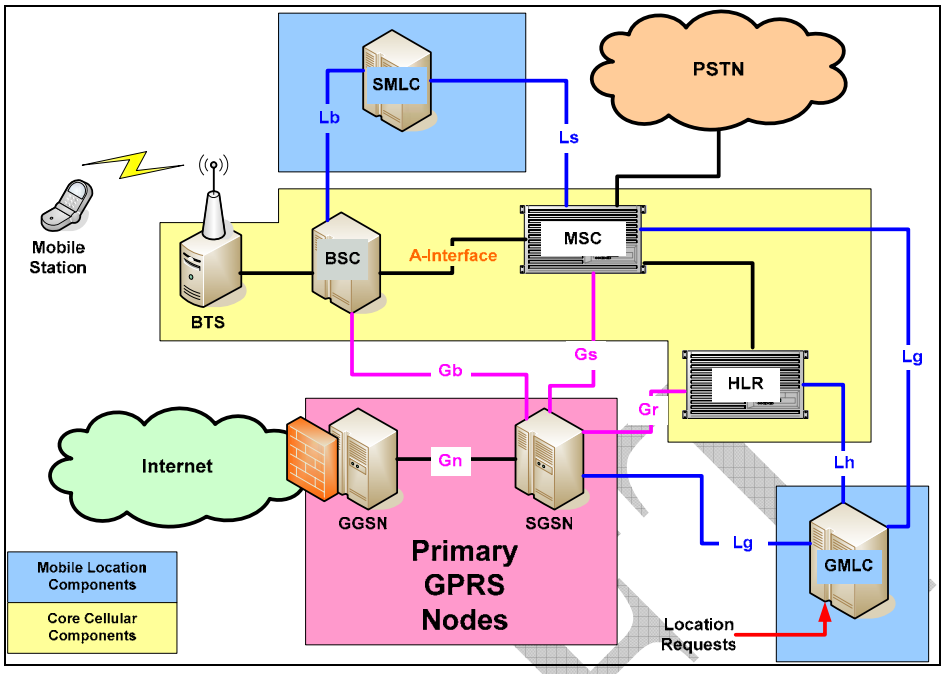


Figure 5-6 GSM-GPRS Network

The GGSN connects the carrier's GPRS network to other networks, such as the Internet, corporate LANs, or third party ISPs. The GGSN may allocate IP addresses itself, it may solicit aid to do this from a RADIUS or DHCP server, or it may broker the request to the Enterprise or ISP to authenticate and assign IP address information. The GGSN is a router and hides visibility of the GPRS network from external entities and networks. In order for the GGSN to be able to route packets between the GPRS network and the external network it maintains a context that associates the mobile to both networks. This context provides a binding between the mobile device using an IMSI and/or MSISDN and the external network identifier, which we assume to be an IP address. A separate context exists for each GPRS to external network association that is required by the mobile.

Figure 5-6 depicts a GSM network with control-plane location elements, the GMLC and SMLC. Where the IMSI or the MSISDN of a mobile is known a request for location can be sent to the GMLC. The GMLC is able to determine where on the network the mobile is located by interrogating the HLR, obtaining the SGSN address and requesting the location of the mobile from the SMLC. In Figure 5-6 a GPRS network however, the external entity requesting location may only know the IP address of the mobile, and while the GMLC can be queried with an IP address, there is no 3GPP MAP mechanism by which a GMLC can perform a location request using only an IP address. Introducing a LIS into this environment (see Figure 5-7) provides a smooth integration between the existing 3G cellular location technologies and associated infrastructure and the packet data network.

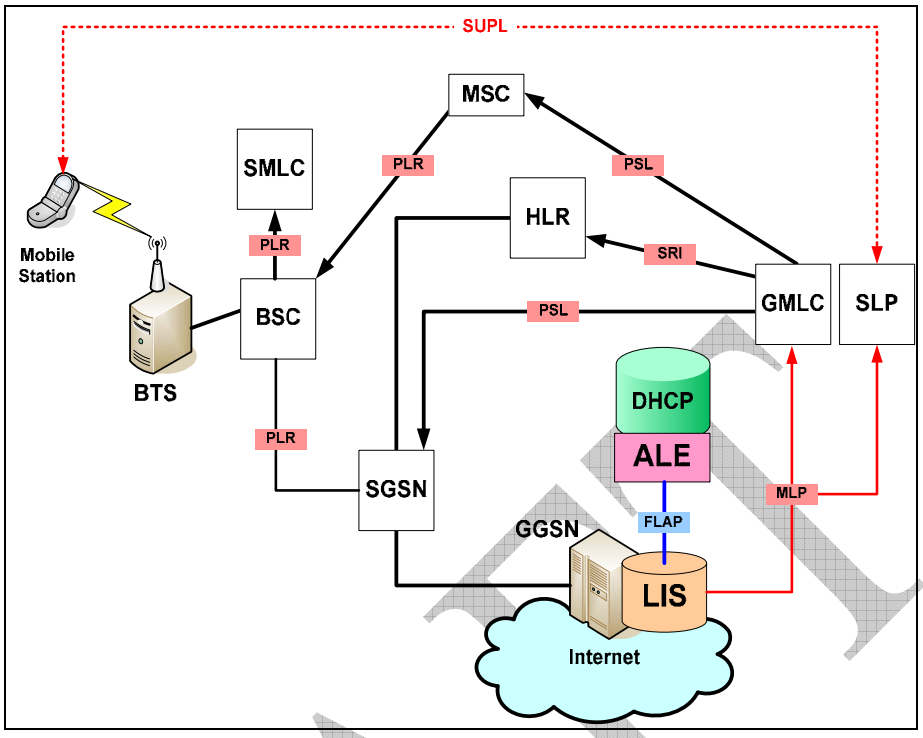


Figure 5-7 LIS in GPRS Network

Introducing a LIS and an ALE into this network assists in two ways. First, it provides a means to obtain the binding between the IP address and IMSI/MSISDN which allows existing GMLC/SMLC and SLP/SUPL deployments to be leveraged easily from the packet data network. Second, it makes a common location acquisition architecture available, allowing mobile devices to request their own location in a standard way, and for applications on the Internet to locate mobile devices in the same way it would for any other device in any other network.

The IP address to IMSI/MSISDN binding is obtained using a DHCP lease query ALE similar to that described in previous sections. In this case the IMSI/MSISDN often forms part of the DHCP client-identifier parameter, and can be extracted by the ALE to provide the necessary information to the LIS. Location requests are then brokered from the LIS to the GMLC or SLP depending on handset capabilities and network configuration.

5.5 Example Enterprise (Ethernet Switch/WiFi) Network

Wired Ethernet and WiFi are the two most common forms of physical Internet access to be found in enterprise environments. They are also found in other environments such as municipal Internet access services and Internet kiosks.

5.5.1 Wired Ethernet

Wired Ethernets are used extensively in enterprise networks and can be configured and connected in a multitude of ways. Networks are constructed to keep inter-switch and inter-network traffic to a minimum so as to optimize network performance. This is done by placing frequently communicating machines (hosts, computers, devices) on the same switch. Where this is not possible, switches may be cascaded together and VLANs introduced to keep different LAN streams on the same switch separated.

Wired Ethernet networks are almost always combined with IP to support more sophisticated addressing and routing functions. IP addresses may be statically configured, or as increasingly the case, provided dynamically using DHCP [06] and a DHCP server. Increasingly DHCP servers are becoming centralized functions requiring DHCP messages to transit several subnets. This requirement poses some problems to hosts requiring dynamically allocated DHCP addresses since broadcast messages are usually blocked by IP routing functions. DHCP relays residing in layer 3 routers which turn IP broadcast traffic into unicast traffic addressed directly to the DHCP server are used to resolve this problem.

DHCP relays are expected to operate and behave in a specified manner, and this is described in [23] and [24]. In addition to providing relay functionality RFC3046 [24] provides a mechanism for the relay to include information about host attachment to the network. This is in the form of the switch identity associated with the relay function and the port on which the DHCP broadcast request was intercepted. The degree of location granularity that can be determined from this information is dependent upon how close the DHCP relay function is to the edge of the network (see Figure 5-8).

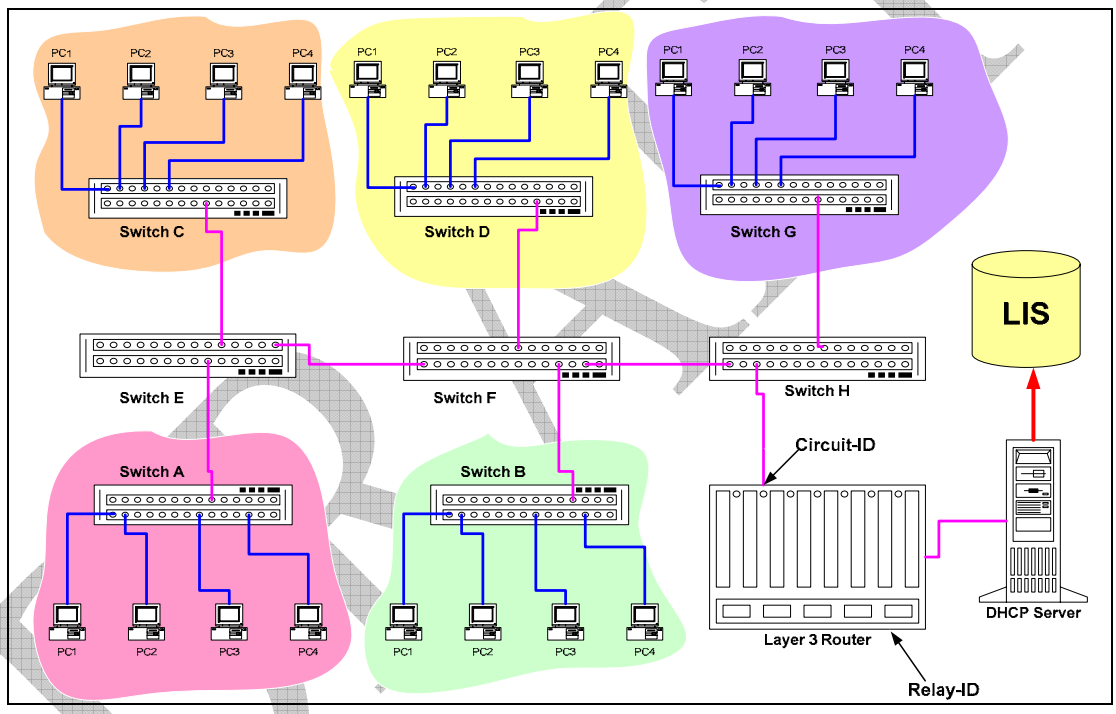


Figure 5-8 Cascaded Switch Network with DHCP Relay

The mechanism of using DHCP relay information forms the basis of location determination and subsequent delivery using the DHCP location acquisition protocol described in RFC3825 [08] and its civic address counterpart [12].

Another mechanism being increasingly deployed in enterprise networks is the use of an ALE-type device that is provisioned with network switch configuration data, and Ethernet MAC addresses it is expecting to see. These systems poll the switches periodically using SNMP and generate reports of MAC address to switch port mappings (See Figure 5-9). This information can then be correlated to determine the location of a physical device. This method of determination is dependent of the edge switches providing SNMP management, and more specifically supporting an implementation of the SNMP Bridge MIB as defined in RFC1493. This MIB provides access to the switch port MAC cache information. The disadvantage is that a substantial amount of configuration data is required in order to

make this type of system work for a large network. MAC address to device binding must also be configured.

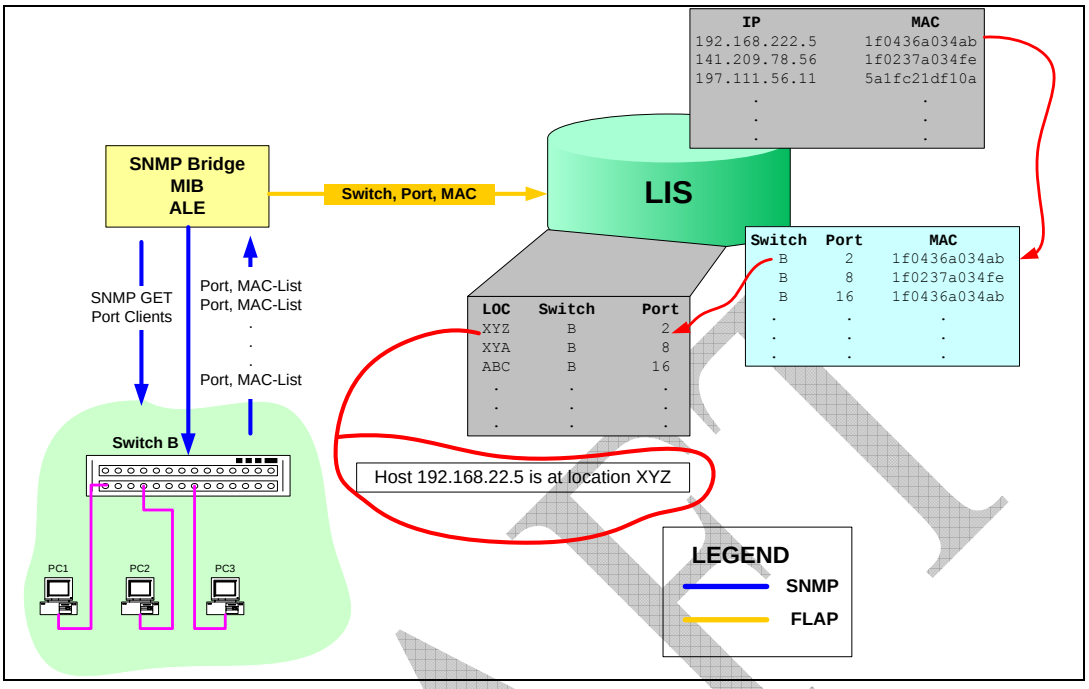


Figure 5-9 SNMP Bridge MIB ALE

The solution described in the previous paragraph can be augmented through the use of a LIS and a DHCP lease query ALE. Here the LIS receives a location request from a specific end-point and keys off the source IP address of the received packet. The LIS uses the DHCP lease query ALE, described in previous sections, to obtain the IP to MAC binding. Once the binding is known, switches can be interrogated to determine the switch and port to which the end-device is attached. To increase search efficiency in a large network, the LIS can be configured with information tying switches to specific subnets. Alternatively DHCP relay information can be obtained from a lease query in addition to the IP to MAC binding, again assisting with switch selection. The advantage of this approach is that no pre-provisioning of MAC addresses is required, allowing deployment in a more dynamic network environment.

The sequence of signaling associated with a LIS that combines ALEs accessing DHCP lease information and SNMP bridge MIB information is shown in Figure 5-10.

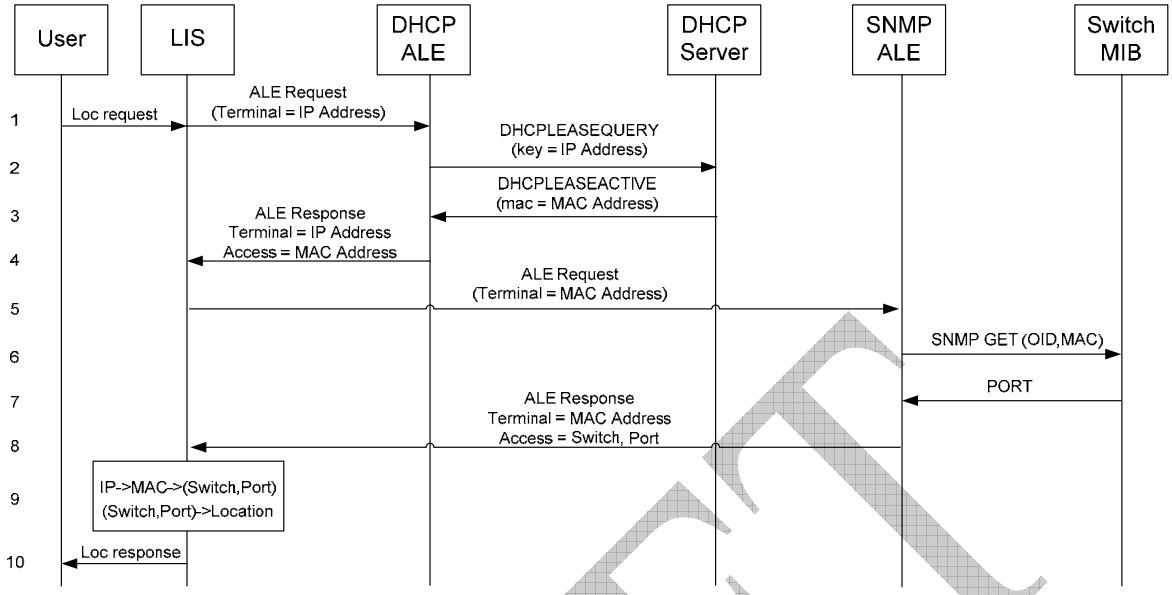


Figure 5-10 ALES Accessing DHCP Lease Information

1. The user device requests location from the LIS which picks up the device IP address from the request.
2. The LIS requests the access location entity to provide the MAC address associated with the IP address.
3. The access location entity utilizes a DHCP lease query request to the network's DHCP server to resolve the MAC address from the proffered IP address.
4. The DHCP server responds with the associated MAC address.
5. The LIS then requests a second (which could be physically implemented as part of the first) access location entity to provide the switch and port identities that the proffered MAC address are associated with.
6. The access location entity utilizes SNMP messaging to query the management information base (MIB) in the network switch(es) to resolve the switch and port identity associated with the MAC address.
7. The MIB on the switch hosting the MAC provides the port information in an SNMP response.
8. The access location entity returns the host switch and port identity to the LIS.
9. The LIS consults an internal wiremap database to resolve the Ethernet cable termination location associated with the host switch and port.
10. The LIS returns this location information to the user device.

5.5.2 Wireless Ethernet

Wireless Ethernet as the same suggests uses RF to communicate between the end-host and the network. There are several flavors of wireless Ethernet LAN or WLAN.

The simplest WLAN consists of wireless access points (WAPs) connected to the ports of a managed switch. End-points attach to the network through a WAP, hand-overs between WAPs occurs when WAP signal strengths reach specific thresholds. Networks built in this

fashion tend to have a relatively flat IP topology with little or no subnetting, allowing hosts to easily move through the network without having to acquire a new IP address to operate in a new subnet or domain.

More complex WLANs are constructed using a wireless network controller (WNC), which controls a cluster of WAPs. In these networks the WNC controls power and client density between WAPs in a similar manner to the way in which a BSC controls cell phone balancing in a Cellular network.

Where the nominal area of coverage of a simple single deployed WiFi access point represents an adequate level of granularity for location determination, then the location of users can be associated with the Ethernet switch port to which the access point is connected. That is, if a simple “cell-based” location is all that is required, then no WiFi specific solution is required. The mechanisms described in section 5.5.1 are all that are required to associate a user with the nominal location covered by the access point which is connected back through an Ethernet switch port.

For more elaborate WiFi networks including mesh deployments involving centralized network controller support, the mechanisms identified in section 5.3 are applicable as there are a number of similarities in the physical characteristics of WiFi and WiMAX. As with WiMAX, there is scope for further study within the IEEE.

6 LIS Operational Considerations

The conceptual role of the LIS is to provide location information (optionally digitally signed) to its clients. This is straightforward from a conceptual perspective but has significant operational implications. The organization that delivers broadband Internet access to users may actually be made up of separate business entities and the relationship between the different entities impacts the practical implementation of the, otherwise logical, LIS function and has a bearing on the specific functionality that a given LIS entity will have.

For example, broadband DSL subscribers establish a commercial relationship with an Internet Service Provider (ISP) who, for the price of the subscription, undertakes to provide the DSL service to that subscriber’s residential address. The ISP, however, may not own the DSL infrastructure, the copper wires and DSLAM equipment that provides the physical connectivity for the subscriber. This infrastructure may be owned by a quite independent Regional Broadband Provider (RBP).

In this situation, the ISP pays the RBP for the physical access on behalf of, and quite transparently to, the subscriber. Moreover, commercial preferences may dictate that the RBP does not want the ISP subscribers and applications having direct connection to, and use of their LIS infrastructure. In such cases the ISP may provide a “gateway” LIS function for the subscribers and applications to query.

The RBP operates the physical access infrastructure from which the location can be determined; i.e. the RBP can determine the physical DSLAM termination and residential address associated with the copper pair on that termination. A practical deployment topology, then, is to have the RBP operate the LIS which actually determines the location. The ISP and the RBP business entities already have a commercial relationship and data interconnection as part of the general provision of Internet access that is the purpose of the relationship. And, in this case, the ISP LIS will also utilize the RBP LIS infrastructure to perform the actual location determination.

The above, is just one example, of how a LIS implementation may be driven by organizational and commercial imperatives. In the example given, the ISP LIS services the client requests but needs to be able to communicate with the RBP LIS in order to resolve actual location information. The same considerations apply for any technology which is wholesaled by an infrastructure operator to an ISP, including wireless technologies such as WiMAX. Just as a standard protocol for LIS-Client communications is critical, the same practical requirement applies to LIS-LIS communication.

The following sections examine some of the practical factors that affect the implementation and deployment of LIS functionality and describe a general model which can be applied in determining the appropriate implementation.

6.1 Types of LIS and LIS Operators

The types of LIS operators (organizational entities that may own and operate a LIS) include, though may not be limited to, the following:

- Access infrastructure providers
  - RBPs for DSL, Cable, 3G, WiMAX etc.
  - Municipal and community WiFi network operators
- Internet Service Providers
  - Providers of Internet access to the public
  - May own or use third party access infrastructure
- Geo-distributed[1] LAN operators
  - Commercial enterprise with broad geographic coverage
  - Government enterprise operator
  - Academic and research network operator
  - Extensive private estate network operator
- Geo-point[2] LAN operator
  - Residential LAN
  - Single access point hotspot

As described in the introductory text, the form and function of the LIS implementation in each of the above cases will vary. They are taken in turn in the following sections.

[1] No hard definition of “geo-distributed” or “broad geographic coverage is offered in this text. To an extent, this will be governed by circumstance and jurisdiction. For example, a LAN operating in a large building covering thousands of square feet may be considered a “geo-distributed” network if either the owner/operator of the building or the jurisdiction in which the building is located consider it necessary to resolve discrete locations within that building – as opposed to just a centroid geodetic location or overall civic address for the building. The owner/operator may use a LIS to track staff or assets within a hot-desk or warehouse environment. The local jurisdictions may require such large buildings to provide a more precise location than just the civic address in the case of emergency calls. If neither imperative exists, then the LAN, despite its actual size, may be regarded as a geo-point network.

[2] As with “geo-distributed”, no hard definition of “geo-point” is provided in this text. Again, the question of whether a hotspot offered by a coffee shop, for example, is considered a geo-point network versus a geo-distributed one depends on circumstances including the question of how big the hotspot coverage actually is.

6.1.1 Access Infrastructure Provider Network

In this case, we are dealing with the operator of the physical infrastructure (wired or wireless) which is used by subscribers to gain access to the public Internet. The LIS in this environment has the key task of determining location from the network parameters related to the device to be located. It may serve the devices themselves when it comes to requests for location, or it may serve a third-party device, such as an ISP LIS, with which the device has a more direct relationship.

In terms of digitally certifying the source of the location information, and for those jurisdictions where the certificate authority only provides certificates to infrastructure providers, the access infrastructure LIS will need to support certificate management and the signing of location information on behalf of ISP operators. The LIS will also support robust authentication and authorization functions to ensure that ISP LIS instances requesting location information for devices are only doing so for their own subscribers.

Therefore, an access infrastructure LIS needs to support all of the generic functions of a LIS including location determination, location acquisition protocol support, assertion, and digital certification of the source of location. It can be labeled as a “general LIS”.

6.1.2 Internet Service Provider

Where the ISP owns and operates its own access infrastructure, then the LIS implementation will be as described for an access infrastructure operator LIS. However, in the quite common circumstance where the ISP purchases access infrastructure wholesale from another operator, the LIS may not actually perform location determination itself. In this case, rather than using network parameters to calculate location, the ISP LIS makes the request, with appropriate device identification parameters, to the infrastructure operator LIS. The ISP LIS supports the location acquisition protocol for subscriber devices and applications but it relies on the infrastructure operator LIS to obtain the location corresponding to those devices.

The protocol used from the ISP LIS to the infrastructure operator LIS may be the standard location acquisition protocol. There is an additional requirement that the ISP LIS has the option to be able to provide authentication to establish the acquisition protocol session. This supports the ability of the infrastructure operator LIS to properly authorize requests by the ISP LIS.

In terms of the certification of location source, the ISP LIS may be equipped with a certificate or it may request the digital certification be done by the infrastructure provider on its behalf.

An ISP LIS, as described in this section, acts as a gateway to a general LIS where location is actually determined. As such, this form of LIS can be labeled as a “gateway LIS”.

6.1.3 Geo-distributed LAN

A Geo-distributed LAN is most often labeled an “enterprise LAN”. A key characteristic of such a network is that it provides access to a closed group of users. It is not typically regarded as a public Internet access provider network, but it does have a connection to the Internet via one or more access infrastructure provider networks. Given such a LAN is connected through an access infrastructure provider, the location of devices on the LAN could be provided by the LIS within that access infrastructure. However, if the LAN is substantially “geo-distributed” then there is a requirement to be able to determine location to discrete areas within that area of LAN coverage. Thus the idea of an enterprise LIS

exists. Such a LIS would be able to determine more precise locations based on LAN parameters associated with the subscriber device.

A large enterprise may actually be regarded as the equivalent of an access infrastructure provider, in that the LIS may support all of the functions of a general LIS with the exception of supporting ISP client LIS connections. However, for enterprises below a given size, it becomes unlikely that a certificate authority could possibly proceed with issuing certificates to the many candidates this would represent. Where a client device or application requests a certified location the enterprise LIS will proxy the request through to the access provider LIS. As such, the LIS operating with a geo-distributed LAN may be labeled a “proxy LIS”.

6.1.4 Geo-point LAN

A typical Geo-point LAN might correspond to a residential home LAN where there is no requirement to refine location to any finer degree than can be determined by the access provider. It is not actually necessary to operate a LIS in such an environment as, with the appropriate discovery mechanism in place, the devices on a Geo-point LAN can query the access provider LIS directly for location information. However, there are some benefits that can be derived from operating a LIS in this LAN environment.

This LIS has no location determination capabilities itself, but it can act as a relay between the devices and the access provider LIS, or it can act as a standalone LIS providing a hard-coded location. Such a LIS can act as a single client to the access provider LIS and apply optimizations such as caching location information to reduce operator LIS load and to provide a backup in the event of an operator LIS outage. Indeed, this type of LIS can be configured with static location information and provide rudimentary location service where the access provider does not offer a LIS.

Since such a LIS primarily acts as a relay to the ISP LIS, it may be labeled a “relay LIS”.

6.1.5 Summary

The form and function that a specific instance of a LIS has will vary depending on the nature of the network it is supporting and the role that the operator of that network plays in the larger picture of Internet access. The specifics of form and function will inevitably be influenced by these aspects and the business and other relationships that exist between network types.

Some variants of LIS implementation that can be identified from these different network scenarios can be labeled as

- General LIS
- Gateway LIS
- Proxy LIS
- Relay LIS

The following diagram (Figure 6-1) shows an overall network topology illustrating the relationships between these types of LIS implementations.

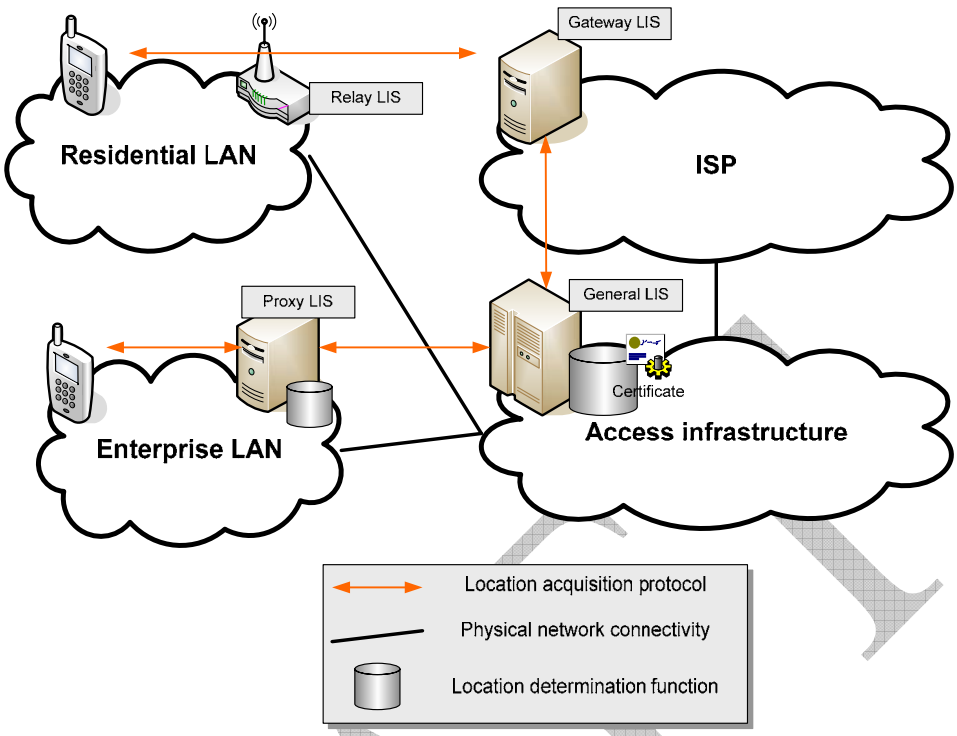


Figure 6-1 LIS Types and associated network types

6.2 Certificate Security and Management

The “certification of location source” has been mentioned several times in the preceding text. The concept behind this term is that location information provided by a LIS may optionally be requested in a digitally “signed” form. The signature provides for the identification of the source of the location information – for example a major access infrastructure provider organization – and provides the means to determine whether the location information has been tampered with (i.e. changed) between the time it was generated by the LIS and the time it is received at the emergency network.

There is no direct connection between the emergency network and the LIS when the location is provided by the user device. In order to deliver the location, and the identity of the source of the location, and still be able to have confidence that they have not been changed in the interim, the information needs to be secured digitally. This is done using digital signatures based on public key encryption mechanisms.

The NENA i2 architecture identifies an agency labeled the Valid Emergency Services Authority (VESA) which will control the generation, issuing, and maintenance of certificates to (among others) LIS operators. It will be critical to the security of the emergency services infrastructure of each jurisdiction implementing the i2 architecture to ensure that the certificates issued by the certificate authority are managed with due care by both the authority and the recipient organizations.

Such security considerations have implications for a LIS operator. For example, the internal organization and procedures associated with the control of access to certificates will need to ensure the data is not compromised. This will likely be best facilitated by physical measures such as equipment supporting FIPS-140 level 3 [26] protection of the certificates.

The use of certificates only guarantees that the location data contained is authentic and originated by the signer. Certificates do not protect against replay attacks, e.g. a miscreant steals a signed location object and attaches it to any emergency call or multiple calls. This attack could result in a PSAP being fooled into responding to what is thought a real emergency as the location data passed the certification test. Emergency calls that contain no location certification and/or a failed location certification also would need careful handling so as to not deny services to a legitimate caller.

6.3 OSS Integration Considerations

Section 4 describes the manner in which the location of devices may be determined in access networks based on a range of technologies. A common requirement in all of these solutions is for the LIS to maintain data records which can be used to associate dynamic network parameter values to information which ultimately indicates the location of the user. Examples, of such records are ATM permanent virtual circuit IDs and the corresponding DSLAM termination and residential address associated with them, or the MAC address of a cable modem and the residential address associated with it.

In practice, there will be considerable effort and infrastructure associated with the collection, grooming, provisioning and ongoing synchronization of such records into an operator LIS. Typically, the necessary data may be stored in a range of back end Operational Support Systems (OSS) ranging from network configuration platforms to subscriber record databases. This aspect of LIS implementation may be the most challenging aspect of LIS ownership. For example, this is already a significant challenge for the operators of location platforms in cellular networks supporting the Phase 2 E9-1-1 requirements of those networks.

Since OSS implementations are often operator specific with little standardization in terms of data schema or provisioning interfaces, it may be that the data provisioning functions of a LIS will need to be dealt with by each individual operator. The situation could be mitigated to some extent with the specification of a standard provisioning protocol for LIS functions. While this does not address the thorny aspect of grooming data from its manifold sources, it would at least allow for a common implementation at the LIS end of the data chain. This document does not describe a common provisioning protocol but it is identified as a potential candidate for further study in an appropriate SDO.

7 Location Acquisition Protocols

The term “location acquisition” refers to the process of a client device or application requesting, and receiving, location information from the LIS. There are a number of approaches and philosophies related to this acquisition process and the protocols that support it. This section looks at various candidates: DHCP, LLDP-MED , HELD, RELO, LREP-SIP and LCP.

7.1 Protocol Descriptions

7.1.1 Dynamic Host Configuration Protocol (DHCP) RFC3825

DHCP delivers network configuration information to an IP device. The intent is to provide the device all the information it needs to utilize the IP network it has connected to;

information such as the IP address allocated to the device, the address of the gateway through which the traffic destined beyond the LAN should be sent, and/or the identity of the domain name service (DNS) that can be requested to translate the names of network hosts into their physical IP addresses in order to talk to them. RFC3825 describes an option on DHCP that allows the device to request and receive a specific form of location information (geodetic or civic).

7.1.2 Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED)

TIA has defined extensions to the link layer discovery protocol (LLDP) to support additional information elements applicable to media endpoint devices. These were termed LLDP-MED and included the ability for those end point devices to be informed of the location associated with, for example, the 802.3 Ethernet switch port to which they are currently attached.

7.1.3 HTTP Enabled Location Delivery (HELD)

HELD is a newly proposed protocol, specifically for the purpose of supporting location acquisition. It uses HTTP as one optional transport/session protocol and can be carried on top of Layer 3 (IP), so the client device and server do not need to be within the same subnet or broadcast domain to communicate. A BEEP binding has also been defined as an optional transport/session protocol. HELD is currently an Internet draft submitted to the IETF [04].

7.1.4 Retrieving End-System LOcation information (RELO)

RELO is another newly proposed protocol and also one aimed at supporting location acquisition interaction above Layer 3. RELO is currently an individual draft submitted to the IETF [28].

7.1.5 A Location Reference Event Package for the Session Initiated Protocol (LREP-SIP)

LREP-SIP is the most recently proposed protocol aimed at supporting location acquisition interaction above Layer 3. It is based on the use of the presence event package for SIP [30] defining a new, locationref, package. It is currently an individual draft submitted to the IETF [29].

7.1.6 Location Configuration Protocol (LCP)

LCP was defined to provide the same functionality as [08] but replacing DHCP with a new IP-based protocol to carry the location request and response. The form of location provided by LCP is defined to be the same as [08]. It is currently an individual draft submitted to the IETF [31].

7.2 Location Protocol Gap Analysis Against NENA i2 Requirements

The following table illustrates the evaluation of various location protocols against NENA i2 Requirements [01] .

NENA Requirement	DHCP	LLDP-MED	HELD	RELO	LREP-SIP	LCP
DA-1 – Mechanism for determining and acquiring location	Yes – the manner in which location is determined is not defined by DHCP	Yes – location associated with the network port is configured directly on the host most commonly using SNMP	Yes - HELD provides acquisition (FLAP provides measurements for determination)	Yes – the manner in which location is determined is not defined by RELO	Yes – the manner in which location is determined is not defined but the protocol supports the provision of network parameters by the device – currently only supports switch chassis/port.	Yes – the manner in whic location is determined is n defined by LCP
DA-2 – Use location estimate	Yes	Yes	Yes	Yes	Yes	Yes
DA-3 – Location requested any time	Yes	Yes	Yes	Yes	Yes	Yes
DA-4 – Consistent method across all network configurations	No Since DHCP is not applicable in all network technologies therefore this acquisition mechanism cannot apply to all access networks.	No Since LLDP-MED is not applicable in all network technologies therefore this acquisition mechanism cannot apply to all access networks.	Yes	Yes	Yes The network identifier types are important to location determination. Currently only supports switch chassis/port.	Yes
DA-5 – Applicable to emergency services	Yes Does not convey uncertainty.	Yes Does not convey uncertainty.	Yes	Yes	Yes	Yes Does not conv uncertainty.
DA-6 – Support i2 and i3	Yes	Yes	Yes	Yes	Yes	Yes
DA-7 – Provide fallback or last known	Non Applicable	Non Applicable	Non Applicable	Non Applicable	Non Applicable	Non Applicable
DA-8 – Minimal call processing impact	Yes	Yes	Yes	Yes	Yes	Yes

NENA Requirement	DHCP	LLDP-MED	HELD	RELO	LREP-SIP	LCP
DA-9 – Assert on behalf of	No	No	Yes (using third party terminal address value – On Behalf Of type request)	No	No	No
DA-10 – No Hardware modification	No	No	Yes	Yes	Yes	Yes
DA-11 – No Hardware replacement	Non Applicable	Non Applicable	Non Applicable	Non Applicable	Non Applicable	Non Applicable
DA-12 – Request response time	No	No	Yes	No	No	No
Rep-1 – Request by reference and by value	Partial, DHCP does not support by-reference	Partial, LLDP-MED does not support by-reference	Yes	Partial, RELO does not support by-reference	Yes	Partial, LCP does not suppo location-by-reference
Rep-2 – Support all fields of PIDF-LO	No Method, presentity, rules, provided-by are not supported.	No Method, presentity, rules, provided-by are not supported.	Yes	No RELO uses opengis GML and pidf civilLoc forms only.	Yes	No Method, presentity, rule provided-by ar not supported.
Rep-3 – Backwards compatibility	No Can only support change through BIS of option or a new option	No Can only support change through BIS of option or a new option	Yes (PIDF-LO definition evolves independently of HELD acquisition protocol)	Yes by indirection to GML and civilLoc forms	Yes (PIDF-LO definition evolves independently of LREP-SIP acquisition protocol)	No Can only supp change throug BIS of [08]
Rep-4 – Provide altitude and floor	Yes	Yes	Yes	Yes	Yes	Yes
LocSec-1 – Provide only to authorized and authenticated devices	Yes Can only provide location to the end-point	Yes Can only provide location to the end-point	Yes	Yes Can only provide location to the end-point	No Protocol forbids the use of authentication for location dereferencing	Yes Can only provi location to the end-point
LocSec-2 – Preserve privacy	Yes (except in transmission since location can only be transferred by-value and not by-reference)	Yes (except in transmission since location can only be transferred by-value and not by-reference)	Yes	Yes (except in transmission since location can only be transferred by-value and not by-reference)	No Protocol does not support the provision of access rules	Yes (except in transmission since location can only be transferred by-value and not b reference)

NENA Requirement	DHCP	LLDP-MED	HELD	RELO	LREP-SIP	LCP
LocSec-3 – Location Dependable	No No dependability mechanism exists for a PIDF-LO crafted by the end-point	No No dependability mechanism exists for a PIDF-LO crafted by the end-point	Yes (through signed location request mechanism with PIDF-LO delivered fully-constituted by the LIS)	No No dependability mechanism exists for a PIDF-LO crafted by the end-point	No There is no support for signed location or for provision of credentials on dereferencing	No No dependabil mechanism exists for a PIDF-LO crafte by the end-poi
LocSec-4 - Authentication of LIS	Partial DHCP can provide integrity through [19], but not secrecy	No	Yes (through encryption of appropriate attributes in creation of location signatures)	No	No	No
LocSec-5 – Source authenticated	No	No	Yes (credentials associated with signed location indicate the source of the location. A user provided location may be "asserted" and subsequently signed by the LIS)	No	No	No
LocSec-6 – Refresh cached location	Yes	Yes	Yes	Yes	Yes	Yes
LocSec-7 – Privacy policies for location by reference	Not applicable DHCP does not support location by-reference	Not applicable LLDP-MED does not support location by-reference	Yes	Not applicable RELO does not support location by-reference	No	Not applicable LCP does not support locatio by-reference

7.3 Findings

Of the 23 NENA provided applicable requirements [18] on location acquisition and determination:

- DHCP provides full support for 10 and partial support for 2, but cannot support the remaining 8. Three requirements are not applicable.
- LLDP-MED provides full support for 10 and partial support for 1, but cannot support the remaining 9. Three requirements are not applicable.
- HELD provides full support for 21, two requirements are not applicable.

- RELO provides full support for 13 and partial support for 1. It does not support 6 and 3 are not applicable.
- LREP-SIP provides support for 13 but does not support 8. Two requirements are not applicable At time of writing, it was not clear whether the user agent identifier exchange is fundamental to location determination or not. The compliance figures assume it is not, or else there would be lower compliance.
- LCP provides support for 12 and partial support for 1. It does not support 7 requirements and 3 are not applicable.

In addition, to support mobile devices requiring a mid-call location update, a location reference is the only practical solution and this mechanism is not supported by DHCP, LLDP-MED, RELO, or LCP.

7.4 HELD Status

HELD has been submitted as an Internet draft over several increments in the 18 month period up until the publication of this TR. It was submitted within the Geopriv working group since that group was defining the location object extensions for the IETF presence information data format. Discussion is currently focused on the question of whether a location acquisition protocol that works above Layer 3 should be defined. A special sub working group (the Layer 7 location protocol group) has been formed to discuss this aspect before further definition of the protocol can progress.

8 Location Parameter Conveyance

Regardless of the location acquisition protocol used to communicate location information to devices and applications, the LIS in a given network needs to be able to determine the location of the device. While the location acquisition protocol is ideally access technology independent, it is necessary to deal with technology dependent specifics in order to determine location in a specific access network. The manner in which the location of a given IP address is determined in a DSL network is, of necessity, different than the manner in which it is determined in a WiMAX network.

When it comes to using the network to determine location, all of the technologies do have one key characteristic in common. They all need to provide the value of some set of network parameters associated with the target IP address in order that the LIS can determine the location for that IP address. Section 4 describes the different sorts of network parameters that may be used (Ethernet switch and port identities, L2TP and ATM circuit identities, modem MAC addresses, wireless network access point identities and radio parameter values being some examples).

To capitalize on this common characteristic, a logical network function called an Access Location Entity (ALE) can be defined. The function of the ALE is to provide the LIS with the set of network parameters pertinent to location determination for the particular type of access network with which the ALE is associated. While the ALE is technology specific, the communication of a “set of network parameters” to the LIS is a common function. For this purpose, the Flexible LIS-ALE Protocol (FLAP) is proposed.

8.1 LIS-ALE Architecture

As indicated above, the ALE is a logical entity dealing with the specific function of extracting and providing the pertinent network parameter values for location determination and sending these parameters to the LIS – see Figure 8-1. The ALE is a logical entity and, as such, the manner in which the ALE is implemented is not prescriptive. However, the ALE abstracts the implementation specifics so the parameters are conveyed in a standard way using FLAP.

A LIS instance provides location services support for users of a specific access network or set of access network technologies. As such, the LIS has a relationship with all the ALE instances supporting the access network(s) for which it provides service.
As part of the ongoing operation of the network;

- the ALE functions may asynchronously report all events pertinent to location determination, with at least some measurements including the IP address of devices against which these parameters can be correlated,
- the LIS may poll the ALE functions for such parameter values on an ongoing basis, or
- the LIS may specifically poll the ALE in response to a client request for location.

The FLAP definition supports all of these modes of operation.

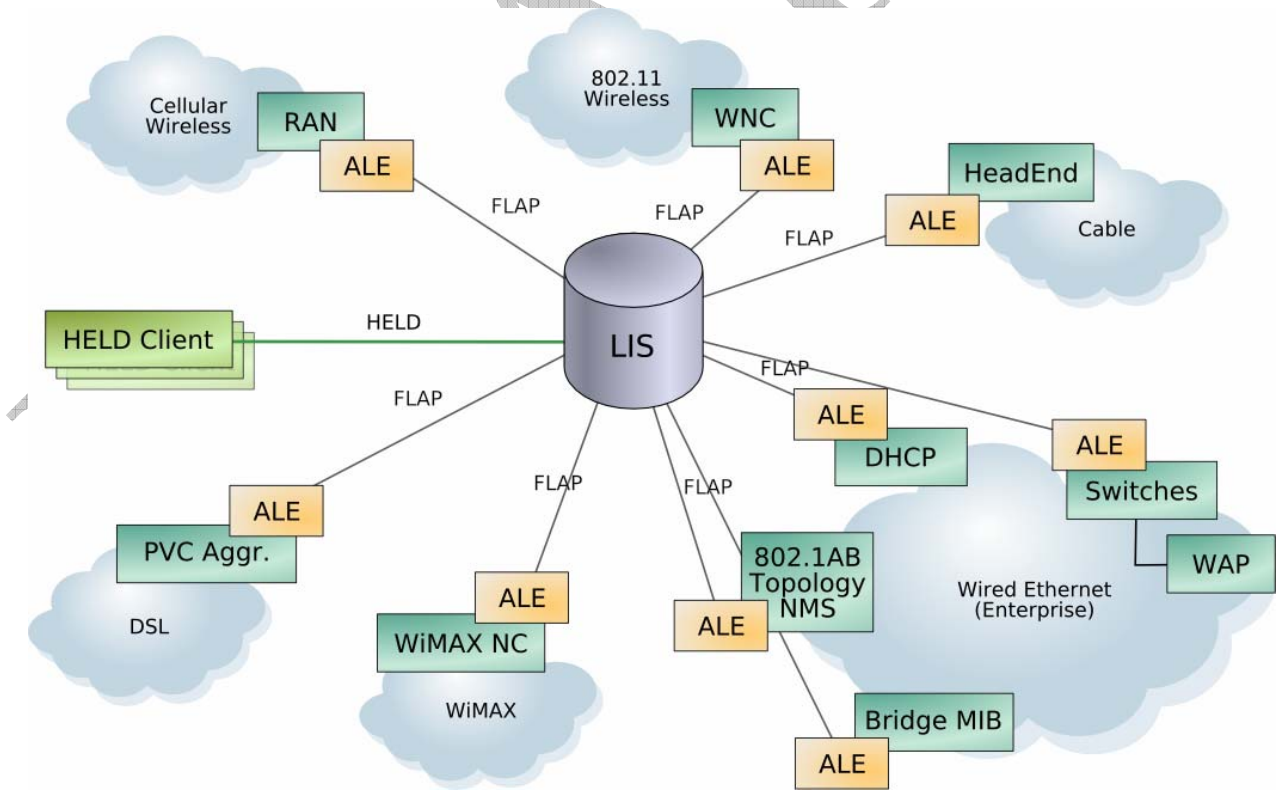


Figure 8-1 The General LIS-ALE Architecture

8.2 FLAP Protocol

The Flexible LIS-ALE Protocol (FLAP) was designed to provide a framework for reporting location measurements.

8.2.1 FLAP Description

It is useful to realize that, at any point along the location determination chain, one piece of information is known and the other is required. FLAP names the known component *terminal* information, that is, the information identifies a particular terminal. The unknown part relates to how the terminal accesses the network, and is called *access* information. The ALE is responsible for providing access information when given terminal information.

For example, if an ALE in an Ethernet switch is queried, it can provide a link between a MAC address and/or IP address (terminal information) and a switch and port (access information).

The distinction between terminal and access information is a simplification that can be thought of as a key-value pair. The link between these values is provided by the ALE. FLAP provides a framework for reporting this link between terminal and access information.

FLAP is defined as a BEEP profile (Blocks Extensible Exchange Protocol) (RFC3080, RFC3081). BEEP is a protocol framework providing bi-directional, asynchronous communication between two entities, in this case a LIS and ALE. BEEP is based on TCP, with support for Transport Layer Security (TLS) where additional security is required.

In order to keep all configuration data centralized, the LIS initiates the BEEP connection. The only configuration that may be required at the ALE is that which permits the authentication of the LIS. Using the Pre-Shared Key Ciphersuites for Transport Layer Security (TLS) (RFC 4279) means that all configuration maintenance effort is kept at the LIS.

By using XML-formatted messages, FLAP can be easily extended to accommodate different access network technologies. The base specification does not proscribe what terminal and access information look like, except to provide start and end times for access information. Terminal and access elements provide a generic container that can be redefined depending on the access network technology. A technology extension defines what information is required for each of *terminal* and *access* for that technology.

Vendor extensions are added on top of technology extensions and allow for enhancements to FLAP that are specific to particular ALEs or networks. Vendor extensions can be used for proprietary methods of improving the speed, accuracy or security of location determination.

Technology and vendor extensions are distinguished by using Namespaces for XML. Each extension is uniquely identified by a URN that is recognized by the LIS.

FLAP allows different ALE types to report location measurements as best suits them. Different FLAP message types, defined in the base FLAP schema, can be used to convey location measurements both asynchronously and synchronously.

8.2.2 Supported FLAP Messages

Notification

The Notification message Figure 8-2 can be generated by the ALE when it detects: a terminal entering the network, a terminal moving within the network, or a terminal leaving the network. This is the recommended approach to ensure an ALE reports location parameters as network circumstances change.

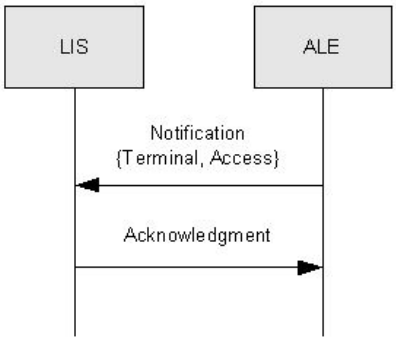


Figure 8-2 The ALE-to-LIS Notification Message Flow

LIS to ALE Notifications (a specific use case)

In some cases, the LIS might detect a particular terminal has moved out of the of network coverage the LIS supports (referred to in this document as the “network sector”) monitored by an ALE before the ALE detects this change. This might be reported to the LIS by another ALE. For instance, DHCP may not always recognize when a terminal has left the network sector. DHCP clients are not obliged to notify the server when they leave the network sector, so many do not.

In this case a LIS to ALE, or downstream, notification message can be sent to the ALE. This message is optional, and is provided as a courtesy to the ALE. The ALE can use this message as a trigger to release any resources it has committed in monitoring that terminal and to update any state it maintains. The downstream notification also prevents the ALE from erroneously reporting the presence of the terminal.

Resynchronization

Network or system outages are inevitable in virtually any system, particularly one that is intended for continuous usage. Resynchronization enhances the robustness and reliability of LIS and ALE communications by providing the LIS a means to quickly determine the current state of the ALE at startup time and after an outage.

Resynchronization uses the BEEP MSG/ANS exchange, which allows for multiple responses to a single request. A Resynchronization Request from a LIS can result in any number of Resynchronization Response messages being sent by the ALE. Each Resynchronization Response contains information about a single terminal and network attachment.

A Resynchronization procedure Figure 8-3 can be used in two ways: a full Resynchronization is used at startup time, or after a long outage; a partial Resynchronization can be used for short outages caused by a transitory fault, or communications error.

When a LIS starts, it will probably not have any useful information about the state of the network. The “full” Resynchronization procedure provides the current state of *all* network attachments the ALE can monitor.

After a short outage in either the LIS or the LIS to ALE link, the LIS can use the partial, or “since”, Resynchronization procedure to request those notifications it might have missed. The partial Resynchronization Request includes a start time, which triggers different behavior at the ALE.

The partial Resynchronization differs from a full Resynchronization because the LIS already has some information about the state of the network – the ALE only needs to provide the changes that have occurred since the indicated time. In effect, the ALE needs to send all the Notifications it would have sent during the request period. This usage differs because responses to this sort of request include terminals leaving the network sector.

Partial Resynchronization is an optimization that reduces the impact of temporary outages. If this mode is not supported, the LIS can purge its current state and use the full Resynchronization.

These messages require that the ALE perform tasks beyond just reporting changes in the network. In order to support these messages, the ALE needs to maintain certain information. For the first usage, the ALE needs to maintain an image of the current state of the network sector. The second usage requires that the ALE also remember a certain number of the most recent Notification messages it has sent, or might have sent.

Alternatively, ALE implementations can avoid storing any additional information, providing they support the Access Query, which can be used by the LIS to build an image of the state of the network sector. However, this option increases the impact of an outage by requiring more messaging to recover state after the outage.

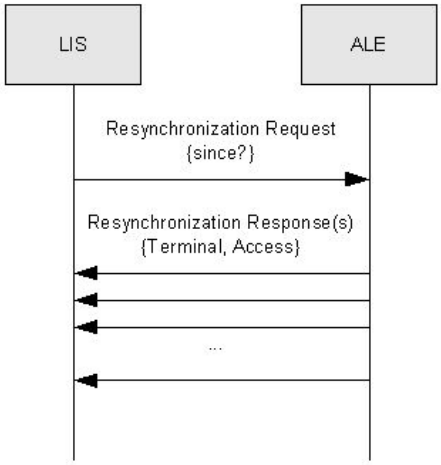


Figure 8-3 The LIS-to-ALE Resynchronization Message Flow

Access Query

The Access Query is a synchronous query that is provided to deal with limitations of ALE implementations. The LIS can make a direct request to the ALE to obtain location parameters. The Access Query is sent by the LIS, and includes terminal information only.

The Access Query procedure Figure 8-4 can be used in a number of ways to address ALEs with limited functionality. Therefore, an Access Query can be used to check that a terminal is still attached to a network sector.

If an ALE does not generate Notification messages, an Access Query can be used to retrieve parameters. The LIS can poll for information from the ALE, or request information on demand. Using Access Query in this fashion can consume a large amount of network resources, and therefore is not recommended.

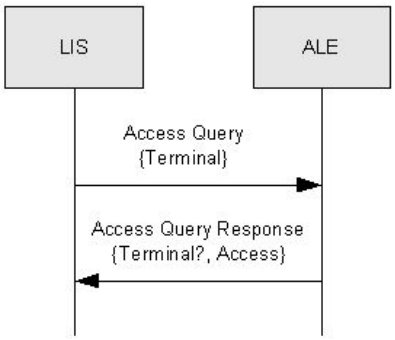


Figure 8-4 The LIS-to-ALE Access Query Message Flow

The set of messages defined in the base FLAP XML schema are designed to provide flexibility. Effective ALE implementations and LIS-ALE inter-working can be set up based on the practicalities surrounding the ALE implementation and the most optimal approach to obtaining location parameter information from specific network types. Most ALEs and LIS implementations would not be expected to utilize all of the defined message types.

8.3 FLAP Examples

The following message uses the Ethernet extension with additional vendor extension parameters to do a notification message:

```
<ntfy xsi:type="enet:ntfy"
    xmlns:vnd1="http://www.example.com/flap/terminal/hw"
    xmlns:vnd2="http://www.example.com/flap/access/skew">
  <enet:terminal
    <ip>192.168.0.1</ip>
    <enet:hwaddr>12:34:56:78:90:ab</enet:hwaddr>
    <vnd1:hw revision="1.2"/>
  </enet:terminal>
  <enet:access time="2005-04-14T10:51:23.000+10:00">
    <enet:switch><ip>192.168.0.1</ip></enet:switch>
    <enet:port>4</enet:port>
```

<vnd2:skew>0.5127</vnd2:skew>
</enet:access>
</ntfy>

The following is an example of an Access Query. It includes information about a particular terminal that location parameters are being requested for:

MSG 1 0 . 63 176
Content-Type: application/xml

<aq xsi:type="dhcp:aq">
<dhcp:terminal>
<ip>192.168.2.10</ip>
<dhcp:hwaddr>01020304050a</dhcp:hwaddr>
</dhcp:terminal>
</aq>
END

The response to this message does not necessarily contain any terminal information:

RPY 1 0 . 801 294
Content-Type: application/xml

<aqr result="200" xsi:type="dhcp:aqr">
<dhcp:access time="2005-04-15T14:02:25.160+10:00"
expires="2005-04-15T16:02:25.160+10:00">
<dhcp:relay>192.168.2.1</dhcp:relay>
<dhcp:circuit-id>03</dhcp:circuit-id>
</dhcp:access>
</aqr>
END

The following is an example of a Resynchronization message sent by the LIS. The ***since*** attribute indicates to the ALE that this is a partial Resynchronization starting at the given time.

MSG 1 0 . 0 108
Content-Type: application/xml

<sync since="2005-04-15T14:51:21.000+10:00"
xsi:type="dhcp:sync"/>

END

The ALE responds to this request by providing a number of responses, each contained in a separate BEEP frame, followed by a NUL frame:

ANS 1 0 . 0 411
Content-Type: application/xml

```
<syncr result="200" xsi:type="dhcp:syncr">
  <dhcp:terminal>
    <ip>192.168.2.11</ip>
    <dhcp:hwaddr>01020304050b</dhcp:hwaddr>
  </dhcp:terminal>
  <dhcp:access time="2005-04-15T15:01:10.991+10:00"
          expires="2005-04-15T17:01:10.991+10:00">
    <dhcp:relay>192.168.2.1</dhcp:relay>
    <dhcp:circuit-id>02</dhcp:circuit-id>
  </dhcp:access>
</syncr>
```

END
ANS 1 0 . 411 253
Content-Type: application/xml

```
<syncr result="201" xsi:type="dhcp:syncr">
  <dhcp:terminal>
    <ip>192.168.2.12</ip>
    <dhcp:hwaddr>01020304050c</dhcp:hwaddr>
  </dhcp:terminal>
  <dhcp:access time="2005-04-15T15:17:57.521+10:00"/>
</syncr>
```

END
NUL 1 0 . 664 0
END

8.4 Considerations of FLAP versus “Technology Specific Solutions”

While FLAP does not address the specifics of how location parameters are identified and extracted from a given access network type, it does provide a consistent framework by which these parameters may be conveyed to a LIS.

Advantages of this approach to delivering location parameters to a LIS compared to implementing technology specific protocols from the access network elements to the LIS include the following:

- FLAP provides a common conceptual framework and language which facilitates the communication of requirements and capabilities between network operators and network equipment vendors.
- Network operators can utilize a common LIS infrastructure supporting multiple access network technology variations without requiring vendor-specific protocol support to handle the delivery of location parameters. The LIS still needs to be able to understand the significance of the parameters delivered by a vendor network ALE.
- The cost associated with LIS implementations and the speed of deployment will be reduced if there is a common LIS-ALE protocol.
- Cross-vendor (LIS-ALE) interoperability will be less complex with a common inter-working protocol.
- Network equipment vendors will be able to highlight product differentiators more readily by documenting the FLAP extensions (and related benefits for location determination) supported by their products.

8.5 Status of FLAP

FLAP is currently only informally documented [27] and has not been specified under the auspices of any SDO. Location measurement has, in the past, typically been done on a technology specific basis.
For example, the Base Station system Application Part- Location Services Extension (BSSAP-LE) and Base Station system (BSSLAP) 3GPP protocols define the messaging used to communicate GERAN related location parameters. FLAP spans an arbitrary set of access technologies and, consequently, is not specific to any particular technology-focused SDO or forum. To provide a definitive specification for FLAP, a general SDO body is most appropriate but there is no value in specifying FLAP unless the technology-focused organizations actually endorse the use of FLAP to support location parameter conveyance for the access technologies they support. ESIF recommends that FLAP be adopted for implementation.

9 References

[01] NENA VoIP-Packet Technical Committee, “Interim VoIP Architecture for Enhanced 9-1-1 Services (i2),” NENA 08-001, Dec 2005.

[02] NENA Technical Committee Chairs, “Implementation of the Wireless Emergency Service Protocol E2 Interface,” NENA 05-001, Dec 2003.

[03] TIA-1057 TIA, “Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED),” TR 41.4

[04] Winterbottom, J., Thomson, M., and B. Stark, “HTTP Enabled Location Delivery (HELD),” draft-winterbottom-http-location-delivery-04 (work in progress), October 2006.

[05] Polk, J. and B. Rosen, "Session Initiation Protocol Location Conveyance," draft-ietf-sip-location-conveyance-05 (work in progress), October 2006.
[06] Droms, R., "Dynamic Host Configuration Protocol," RFC 2131, March 1997 (TXT, HTML, XML).
[07] Patrick, M., "DHCP Relay Agent Information Option," RFC 3046, January 2001.
[08] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information," RFC 3825, July 2004.
[09] Peterson, J., "A Presence-based GEOPRIV Location Object Format," RFC 4119, December 2005.
[10] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for PIDF-LO," (work in progress), April 2006.
[11] Thomson, M., "Geodetic Shapes for the Representation of Uncertainty in PIDF-LO," (work in progress), May 2006.
[12] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information," (work in progress), January 2006.
[13] Winterbottom, J., Tschofenig, H., and M. Thomson, "GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations," (work in progress), May 2006.
[14] Winterbottom, J., Peterson, J., and M. Thomson, "Rationale for Location by Reference," (work in progress), January 2006.
[15] DSL Forum, "Core Network Architecture Recommendations for Access to Legacy Data Networks over ADSL," Technical Report 025.
[16] DSL Forum, "Migration to Ethernet-Based DSL Aggregation," Technical Report 101.
[17] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements," RFC 3693, February 2004.
[18] NENA Requirements for Location Information to Support Emergency Services, 13 November 2006.
[19] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages," RFC 3118, June 2001.
[20] NENA VoIP, Recommended Method(s) for Determining Location to Support Emergency Calling Technical Information Document, Draft 30 May 2006.
[21] Woundy, R. and K. Kinnear, "Dynamic Host Configuration Protocol (DHCP) Leasequery," RFC 4388, February 2006.
[22] "IP Location; Geographic Location Measurement, Delivery and Conveyance", Dawson, Winterbottom , Thomson; Osbourne-McGraw-Hill; ISBN: 007226376
[23] Wimer, W., "Clarifications and Extensions for the Bootstrap Protocol," RFC 1542, October 1993.
[24] Patrick, M., "DHCP Relay Agent Information Option," RFC 3046, January 2001.
[25] Decker, E., Langille, P., Rijsinghani, A., and K. McCloghrie, "Definitions of Managed Objects for Bridges," RFC 1493, July 1993.
[26] National Institute of Standards and Technology (NIST) – Federal Information Processing standard 140 version 140-2, May 2001.
[27] Dawson, Winterbottom, Thomson, "IP Location", McGraw-Hill Publishing, 2006
[28] Schulzrinne, H., "RELO: Retrieving End System Location Information", draft-schulzrinne-geopriv-relo-01.txt, October 22, 2006

[29] Schulzrinne, H., "A Location Reference Event Package for the Session Initiated Protocol (SIP)," draft-schulzrinne-geopriv-locationref-00.txt, October 17, 2006

[30] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol (SIP)," RFC 3856, August 2004.

[31] Linsner, M. Schnizlein, J., "Location Configuration Protocol (LCP)," draft-linsner-geopriv-lcp-01, November 7, 2006