NENA VoIP Recommended Method(s) for Determining Location to Support Emergency Calling Technical Information Document (TID)

DRAFT

NENA Recommended Method(s) for Determining Location to Support Emergency Calling -- Technical Information Document
NENA 08-<to be assigned (tba)>, Issue 0, 2006 — DRAFT 30 May 2006

Prepared by:
National Emergency Number Association (NENA) VoIP Location Working Group

Published by NENA
Printed in USA

One Nation 9-1-1 One Number

NENA
TECHNICAL INFORMATION DOCUMENT

NOTICE

The National Emergency Number Association (NENA) publishes this document as an information source for the designers and manufacturers of systems to be utilized for the purpose of processing emergency calls. It is not intended to provide complete design specifications or parameters or to assure the quality of performance for systems that process emergency calls.

NENA reserves the right to revise this TID for any reason including, but not limited to:

conformity with criteria or standards promulgated by various agencies
utilization of advances in the state of the technical arts
or to reflect changes in the design of network interface or services described herein.

It is possible that certain advances in technology will precede these revisions. Therefore, this TID should not be the only source of information used. NENA recommends that members contact their Telecommunications Carrier representative to ensure compatibility with the 9-1-1 network.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

This document has been prepared solely for the voluntary use of E9-1-1 Service System Providers, network interface and system vendors, participating telephone companies, etc.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA's Technical Committee has developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
4350 North Fairfax Drive, Suite750
Arlington, VA 22203-1695
800-332-3911
or: techdoccomments@nena.org

DRAFT

Acknowledgments:

The National Emergency Number Association (NENA) Technical Committee Chairs developed this document.

NENA recognizes the following industry experts and their companies for their contributions in development of this document.

Members:	**Company**
Nadine Abbott – Working Group Chair	Telcordia
James Winterbottom - Editor	Andrew Corporation
Barbara Stark	Bell South
Guy Caron	Bell Canada
Brian Rosen	Neustar
Patti McCalmont	Intrado
Dave Morris	Verizon
Dick Khan	AT&T
Ed Shrum	Bell South
Tom Anschutz	Bell South
Calvin Chow	Bell Canada
Marc Linsner	Cisco Systems
Roger Marshall	TCS
Marc Berryman	Harris Country
Deb Barclay	Lucent
Ken Maynard	Bexar Metro 9-1-1 Network District
John Cummings	Vonage

DRAFT

TABLE OF CONTENTS

1 EXECUTIVE OVERVIEW 6

1.1 PURPOSE AND SCOPE OF DOCUMENT 6
1.2 REASON FOR ISSUE 6
1.3 REASON FOR REISSUE 6
1.4 RECOMMENDATION FOR STANDARDS DEVELOPMENT WORK 6
1.5 COSTS FACTORS 7
1.6 ACRONYMS/ABBREVIATIONS 7

2 TECHNICAL DESCRIPTION 9

3 TERMS AND DEFINITIONS 9

4 REQUIREMENTS 11

4.1 LOCATION DETERMINATION AND ACQUISITION 11
4.2 LOCATION REPRESENTATION 12
4.3 LOCATION SECURITY AND DEPENDABILITY 12

5 ACCESS TECHNOLOGIES 13

5.1 WIRED ETHERNET 13
5.2 WIFI NETWORKS 14
5.3 WIRELESS MESH 15
5.4 DIGITAL SUBSCRIBER LINE (XDSL) NETWORKS 17
5.4.1 DSL Interfaces and Protocols 20
5.5 FIBER TO THE HOME (FTTH) 22
5.6 CABLE NETWORKS 22
5.7 ATM 22
5.8 3G CELLULAR 22
5.9 OFDM/WIMAX (802.16) 22
5.10 BROADBAND OVER POWER LINES (BPL) 22

6 LOCATION REPRESENTATION AND CHARACTERISTICS AND CALLING TRENDS 22

6.1 LOCATION REPRESENTATION 22
6.2 LOCATION CHARACTERISTICS 22
6.3 CALLING TRENDS 23

7 LOCATION ACQUISITION METHODS 23

7.1 DHCP LOCATION ACQUISITION 23
7.2 LLDP-MED LOCATION ACQUISITION 24
7.3 HELD LOCATION ACQUISITION 24

8 XDSL RESIDENTIAL BROADBAND CONFIGURATIONS 25

8.1 IP CONNECTIVITY OVER THE SERVICE PROVIDER SEGMENT 25
8.2 LAYER 2 FORWARDING OVER THE SERVICE PROVIDER SEGMENT 27
8.3 L2TP OVER THE SERVICE PROVIDER SEGMENT 29
8.4 LIS DISCOVERY IN A DSL ENVIRONMENT 32
8.4.1 IP Address Determination 33
8.4.1.1 Universal Plug and Play (UPnP) 33
8.4.1.2 WEB Report 33
8.4.1.3 STUN 34

DRAFT

8.4.1.4 Recommendation 34
8.4.2 Domain Determination 34
8.4.3 DNS SRV Record LIS Discovery 35
8.4.4 Requirements 35

9 LIS PROVISIONING GUIDELINES 36

10 REFERENCES 37

DRAFT

1 Executive Overview

1.1 Purpose and Scope of Document

This document is the first edition of what will be a comprehensive document addressing many access network configurations. This edition has a narrow solutions focus and will address only the automated mechanisms for the residential broadband market, manually configured location mechanisms for end-points are not discussed. Revised editions of this document will add new sections to address enterprise, hosted and mobile access configurations.

In order to understand the residential broadband market it is important to understand a few things about how these services are delivered. Detailed discussions throughout this document describe the technological and organizational structures that are required to deliver these services, and the impacts that these have on the potential to deliver workable location determination and acquisition solutions.

The document provides a clear set of requirements that the proposed solutions try to satisfy. These requirements are deemed to be desirable characteristics of any solution regardless of the access technology.

1.2 Reason for Issue

This release of the document describes requirements and solutions for automatically determining the location of IP devices inside a residential broadband network. It also provides requirements and recommended solutions to allow the network-determined location to be acquired by nodes needing it in emergency applications.

1.3 Reason for Reissue

This document should be reissued as new location determination and acquisition solutions are identified for residential broadband and other IP access networks. The current scope of this document is restricted to residential broadband networks in an effort to ensure that some solutions are available in a timely manner. This document is expected to be reissued to address enterprise, WiFi (enterprise and community), 3G cellular and WiMAX access networks.

1.4 Recommendation for Standards Development work

Many of the solutions described in this document are already the subject of work by various standards bodies. This is a solutions document, and puts together a series of elements connected by standards-based, or standard-track specifications, however the overall solutions are not covered by any one standards body. It is therefore recommended that the solutions proposed in this document be forwarded to ESIF for consideration as an American National standard. NENA may also forward this document to other industry forums. This will ensure that location determination and acquisition for residential broadband networks is done in a consistent manner allowing the quality and safety of the system to be monitored.

DRAFT

1.5 Costs Factors

Not Applicable

1.6 Acronyms/Abbreviations

This is not a glossary! See NENA 01-002 - NENA Master Glossary of 9-1-1 Terminology located on the NENA web site for a complete listing of terms used in NENA documents.

The following Acronyms are used in this document:	
ADSL	Asymmetric DSL
AIP	Access Infrastructure Provider
ALI	Automatic Location Identification
ANI	Automatic Number Identification
ANSI	American National Standards Institute
ASP	Application Service provider
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
BOOTP	Bootstrap Protocol
BRAS	Broadband Remote Access Server
BPL	Broadband Over Power Lines
CLEC	Competitive Local Exchange Carrier
CPE	Customer Premises Equipment
CSP	Communications Service provider
DHCP	Dynamic Host Configuration Protocol
DN	Directory Number
DSL	Digital Subscriber Line
DSLAM	DSL Access Module
E9-1-1	Enhanced 9-1-1
EFM	Ethernet in the First Mile
ELIN	Emergency Location Identification Number
ERL	Emergency Response Location
FTTA	Fiber To The Access
FTTH	Fiber To The Home
FTTP	Fiber To The Premises
GIS	Geographic Information Systems
GML	Geographic Markup Language
GMLC	Gateway Mobile Location Center
GPS	Global Positioning System
HFC	Hybrid Fiber Coax
ILEC	Incumbent Local Exchange Carrier
IPoE	Internet Protocol over Ethernet
ISP	Internet Service provider

DRAFT

The following Acronyms are used in this document:	
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
LIS	Location Information Server
LLDP-MED	Link Layer Discovery Protocol Media Endpoint Discovery
LO	Location Object
MDF	Main Distribution Frame
MLP	Mobile Location Protocol
MPC	Mobile Positioning Center
MSAG	Master Street Address Guide
NAS	Network Access Server
NID	Network Interface Device
NSP	Network Service Provider
OMA	Open Mobile Alliance
PAN	Personal Area Network
PIDF	Presence Information Data Format
PIDF-LO	Presence Information Data Format – Location Object
PON	Passive Optical Network
POS	Packet Over SONET
PPPoE	Point-to-Point Protocol over Ethernet
PPPoA	Point-to-Point Protocol over ATM
PSAP	Public Safety Answering Point
PSTN	Public Switch Telephone Network
PVC	Permanent Virtual Circuit
RADIUS	Remote Authentication Dial-In User Service
RG	Routing Gateway
SIP	Session Initiation Protocol
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
URI	Uniform Resource Identifier
VCI	Virtual Circuit Identifier
VEP	VoIP End Point
VLAN	Virtual LAN
VoIP	Voice over Internet Protocol
VPC	VoIP Positioning Center
VPN	Virtual Private Network
VPI	Virtual Path Identifier
VSP	VoIP Service Provider
WAP	Wireless Access Point
WNC	Wireless Network Controller

DRAFT

2 Technical Description

The intent of this document is to give operators and access providers alike some recommended ways to provide an automatic location service across a range of access networks. Where recommendations are standards-based, the relevant standards are referenced. Not all recommendations made in this document will have strong standard specifications because the problem domain is relatively new. As stated in the section 1.3, when relevant new solutions or standards become available the document will be re-issued to include reference to them.

3 Terms and Definitions

The IP location domain is new so terms and definitions used in other telephony environments may no longer apply or have the same meaning. This document defines a very clear set of terms for describing key aspects of IP networks to avoid confusion with similar terms that may be used in other contexts.

Access Location Entity (ALE): A network entity or function that provides network measurements to a LIS allowing the LIS to correlate a device with a physical location.

Definitive Civic Address: An address that can be resolved into a local MSAG valid address, will yield a route to the correct PSAP when used to route an emergency call, and is bound to a specific IP end-point.

Enterprise Network: A large, privately owned and run, diverse network connecting major points in a company or other organization.

Fixed/Static: Refers to an IP end-point that cannot move, is always in same location and always accesses a network from the same point.

IP Access Network: The network in which the first IP address is assigned to an end-point. For residential networks the creation and supply of an access network may require the co-operation of several different providers. For example an ISP may lease lines and DSLAM capacity from an existing telephony provider, in such a circumstance both entities are required in the providing of an access network.

Location: The physical position of an IP end-point expressed in either civic or geodetic form.

Location Acquisition: Refers to the way in which a network determined location is provided to the network entity responsible for inserting the location information into the context of an emergency call. Location information may be pushed to the network entity by the LIS, or pulled by the network entity from the LIS. The network entity may be the Target, or it may be some other routing node such as a proxy or call-server.

Location-aware: Used to describe IP endpoint devices that are location-capable and that have acquired location information, either with network assistance or by self-determination.

Location By-Reference: An identifier that when referenced in the correct manner by an authenticated and authorized entity will yield the location of a IP end-point. An example of a location reference is a URI.

Location By-Value: A PIDF-LO containing the location of an IP end-point that can be attributed to a specific point in time.

Location-capable: Used to describe IP devices that are capable of requesting, acquiring, and storing location information as well as including this information in a PIDF-LO when originating an emergency call.

Location Conveyance: Refers to the act of transporting location information with an emergency call.

Location Dependability: Reflects the level of trust that a receiving node has in the quality and authenticity of the location information being provided. A full description of location dependability is provided in Section 6.2.

Location Determination: Act of using measurements taken from the access network to calculate or otherwise discover the physical location of a device.

Location Estimate: The approximate physical position of an IP end-point expressed in either civic or geodetic form usually accompanied by a degree of uncertainty. The degree of uncertainty may be expressed by a reduction in precision. For civic locations this equates to the number of fields specified while for geodetic locations it equates to the definition of an area or volume specified as a shape.

Location-incapable: Used to describe IP devices that are not capable of requesting, acquiring, or storing location information. This includes most current IP devices.

Location Information Server (LIS): The LIS is a network entity that determines the physical location of Targets with in the access network and provides that location information to authenticated and authorized recipients. Location determination is performed with the assistance of network measurements provided by ALEs residing in the access network.

Location Recipient: A location recipient is the consumer of location information. This may be the Target, the PSAP, the VPC or any other node that uses location information when it is provided.

Location-unaware: Used to describe IP devices that are location-capable but that have not been able to successfully acquire location information, either with network assistance or by self-determination.

Location Validation: Refers to the action of ensuring that a civic address can be used to discern a route to a PSAP. Location validation is outside of the scope of this document.

Mobile: A user is said to be mobile if they are able to change access points while preserving all existing sessions and services regardless of who is providing the access network, and their location

DRAFT

may be definitively represented by a geographic co-ordinates but only indicatively represented by a civic address.

Network Location Determination: Refers to the mechanism and data that a network entity can use to ascertain the whereabouts of a terminal in the access network such that the location can be specified in a valid PIDF-LO.

Nomadic: A user is said to be nomadic if they are constrained within an access network such that their location can be represented as a definitive civic address for that network attachment. The user may move from one network attachment to another but cannot maintain a session during that move. If the user is able to move outside the definitive civic address without losing network attachment then the user is considered to be mobile, not nomadic.

Target: The IP endpoint to which location is attributed.

4 Requirements

4.1 Location Determination and Acquisition

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, and 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 (Location 1400-0100 from LTD WG i3 rqmts) – 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 provide minimal impact to 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.

DRAFT

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.

4.2 Location Representation

Rep1 – Location information may be provided by-value or by-reference and 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.

4.3 Location Security and Dependability

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.

LocSec3 – 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 location[1].

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.

LocSec7 – Where location by-reference is used the appropriate privacy policies MUST be implemented and enforced by the LIS operator.

[1] Manual entry is not the preferred method. If the Location Information is configured into the Emergency Caller's Device by manual entry, such entry SHOULD require authentication and authorization of the person providing the entry.

DRAFT

5 Access Technologies

This section provides an overview of a number of different access technologies that can be used to provide an IP access network. The scope of this document is oriented towards residential broadband networks however, having an understanding of other access technologies allows a network builder the choice to select a solution that will address multiple access deployments.

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 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 is increasingly the case, provided dynamically using the Dynamic Host Configuration Protocol (DHCP) [2] 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 as service discovery is performed using IP broadcast messages that are blocked by IP routing functions to prevent network packet storms and worse.

This situation was addressed in the forerunner protocol to DHCP, BOOTP [3], through the use of “Agents”, referred to in the common vernacular as “relay-agents”. A relay-agent generally resides in an IP gateway function, or router, and intercepts DHCP broadcast traffic. The relay-agent directs the intercepted traffic to the DHCP server on behalf-of the requesting node using unicast IP. That is the relay-agent knows the IP address of the DHCP server and is inherently trusted by the DHCP server; a DHCP client has no visibility as to the presence of the relay-agent. The functionality that a relay-agent can provide has grown over time; the foundation for most of the functionality is defined in the IETF DHCP Relay Information Option [4].

DRAFT

Figure 5-1 Wired Ethernet Network

Wired Ethernet networks are considered further in this document, though the concepts of DHCP and its associated relay functions are described in more detail in a later section.

5.2 WiFi Networks

The 802.11 suite of protocols (a,b,g), collectively referred to as WiFi, provide wireless connectivity to a LAN. Speeds and QoS options vary from type to type with 802.11g being commonly deployed and providing an access bandwidth of 54Mb. WiFi networks can be configured and rolled out in a number of ways. Standalone Wireless Access Points (WAP) and Wireless Network Controller (WNC) configurations will be discussed first. Wireless mesh networks are addressed in a subsequent section.

The simplest form of WiFi network consists of one or more WAPs connected to a standard Ethernet switch, which in turn is connected to an intranet containing a DHCP server and other layer 3 routing infrastructure. In this configuration, the switch is aware of the MAC addresses that it is serving down a specific port, and the IP address is delivered from a centralized DHCP server. If a user "roams" from one access point to an adjacent one, then its IP address becomes associated with a new port in the switch and its packets are sent to the new serving WAP.

Figure 5-2 Basic WiFi Network

A more sophisticated approach to enabling WiFi networks introduces the notion of a wireless network controller (WNC) which manages a group of WAPs. In this type of network the WNC is able to control WAP hand-overs etc… to improve the overall performance of the network.

Figure 5-3 WNC Based Network

WiFi networks are not considered further in this version of the document.

5.3 Wireless Mesh

In Mesh networks, each WAP communicates with its neighbors over a wireless link, with a view that eventually one or more connections back to a core network element will be established. There are two basic types of wireless mesh network. The first variety, referred to as infrastructure-mesh networks, consists of a group of wireless access points wired into the core network, and a radio link

is established between these nodes to provide an additional backhaul in the event that a node's direct connection is lost.

Figure 5-4 Infrastructure-Mesh Network

The second variety of mesh network is referred to as client-mesh or ad-hoc-mesh. In this type of network each wireless device participates in the communication, and each client may become a repeater or router in the network thereby extending the reach of the network. This type of network is becoming increasing popular in community-based networks as the nodes are relatively inexpensive and require little infrastructure to install.

Radio link

Figure 5-5 Client-Mesh Network

ore
ode

Such a network is extremely resilient to element failures, but determining the message originating node from a central point can be problematic. The complexity in wireless client-mesh networks cannot be over stated, as each client in a mesh network has the potential to host other clients and thereby extend the reach the network making it even more difficult to determine the ultimate location of an end-point.

Wireless mesh networks are not considered further in this version of the document.

5.4 Digital Subscriber Line (xDSL) Networks

xDSL is a technology that allows high-speed broadband services to be delivered to residential premises over existing twisted pair copper lines. It allows transmission of high-speed internet traffic and existing telephony services down the same pair of wires at the same time, with signal separation occurring at the local telephone exchange. xDSL signals are passed to a DSL Access Module (DSLAM) which ultimately passes traffic on to the subscriber's Internet Service Provider and on to the Internet.

Figure 5-6 ADSL Concepts

Most DSL services require the cooperation of several parties and organizations in order to provide an access service. This cooperation is necessary because different aspects and functions reside in different organizations and all are required for the connection to be established. The DSL forum is an internationally recognized body that provides guidance and recommendations on how to build and provide service to DSL networks.

Fax **Telephone**

`

Filter

DSL
Modem

Figure 5-7 shows the main organizational entities identified by the DSL forum as being required to provide a DSL access solution.

DRAFT

Figure 5-7 DSL Forum Defined Access Entities

The responsibilities for each of the operating entities are defined below:

The Loop Provider:

Regional Network Provider

A

Provides a physical loop from the Local Network equipment to the customer's premises

Is responsible for the integrity of the physical loop and its repair

May also provide the Access Network Provider aggregated access to remotely deployed DSL equipment owned, operated, and maintained by the Loop Provider

NSP Network

Regional Network

Access Node

The Access Network Provider:

Provides digital connectivity to the customer via the physical Loop

Is responsible for the performance and repair of the access transmission equipment

The Regional Network Provider:

Provides appropriate connectivity between the Access Network, Network Service Providers and the Application Service Providers (not shown).

Is responsible for Regional Network performance and repair

May perform aggregation services to Network Service Providers or Application Service Providers and/or may provide any-to-any connectivity within the Regional Broadband Network on behalf of the Network/Application Service Provider.

The Regional/Access Network Provider (RANP):

The Regional and Access Networks aggregate subscriber traffic and provide routing or forwarding of this traffic at various levels. In the framework described in TR-058 [12], these are considered as a combined network because new functionality must be coordinated between both networks. Among other important functions, the Regional Access/Network provides aggregation of subscriber traffic to

DRAFT

different service providers and IP address allocation and network authentication for subscribers that desire to connect to NSPs and ASPs. If these functions are provided by separate entities, the relevant functions are as described previously.

The Network Service Provider (NSP):

Includes Internet Service Providers (ISPs) and Corporate Service Providers

Is responsible for overall service assurance

May provide CPE, or software to run on customer-owned CPE, to support a given service

Provides the customer contact point for any and all customer related problems associated with the provision of this service

Authenticates access and provides and manages the IP address to the subscribers

5.4.1 DSL Interfaces and Protocols

A DSL network can be thought of as being made up of 3 primary segments that link various functions of the work.

Figure 5-8 DSL Network Segments

The Loop segment runs between the RG (the DSL modem) and the DSLAM. At the time of writing this may take one of two forms: DSL using an ATM transport or an Ethernet transport (EFM). The DSL forum refers to this segment as the U-Interface.

DRAFT

Figure 5-9 DSL Forum U-Interface

The access segment, or V-Interface as it is officially referred to, defines connectivity between the Access Node/DSLAM and the aggregator and is usually provided on ATM, or Ethernet; however, Frame-Relay and Packet Over SONET (POS) can also be used. The aggregator uses the incoming port identifier and some message content information to determine the destination Network Service Provider.

The Service Provider segment transports traffic between the Aggregator/Regional Network and the Network Service provider (ISP) and is termed the A10-Interface within DSL forum specifications.

Figure 5-10 DSL A10-Interface

DSL networks are one of the principle ways in which residential broadband networks are provided. DSL networks and in particular the various interface segments are examined in some depth in subsequent sections to provide an understanding of how location determination can be performed in these networks.

5.5 Fiber To The Home (FTTH)

<TDB>

5.6 Cable Networks

<TDB>

5.7 ATM

ATM has been listed here to point out that it was not unintentionally missed. ATM is not being considered as a standalone access technology used by endpoints to connect to a larger networks. While the working group accepts that there may be isolated cases where such situations do occur, they are not considered to be widespread; consequently, no specific description or solution for these networks will be discussed in this paper. ATM as a transport for ADSL and other broadband access techniques is addressed specifically in sections relating to those access technologies.

5.8 3G Cellular

<TBD>

5.9 OFDM/WiMax (802.16)

<TDB>

5.10 Broadband Over power Lines (BPL)

<TDB>

6 Location Representation and Characteristics and Calling Trends

6.1 Location Representation

The form adopted for location representation in both i2 and i3 is the PIDF-LO [1]. The PIDF-LO allows representation of location in two general forms, geodetic and civic [21]. The geodetic form was originally left open to use the GML 3.0 feature namespace which made shape definition hard. A recent internet draft [20] defines an easy-to-use set of shapes that is largely compatible with those defined in the OMA MLP specification.

Care must be taken however when expressing location in geodetic form when that location is also to be displayed at a PSAP. This is particularly true with i2 solutions as location is communicated to the PSAP over the V-E2 interface, based on the NENA E2 specification [22] which supports only a very small set of shapes. Restricting the geodetic representation to this subset is recommended if conversion and error is to be avoided.

6.2 Location Characteristics

For location information to be useful to a recipient it requires three key characteristics:

DRAFT

1. It must be attributed to the Target that the recipient wishes to locate
2. It must be in a form and to a suitable precision to be of use to the recipient
3. It must have characteristics 1 and 2 at the time it is provided to the recipient

The level of trust that a location recipient has in the location information accurately exhibiting all three of these characteristics is referred to as location dependability. While the need for location dependability is still argued in some circles, it is widely accepted that it can be provided using either digital signatures or location references. It is also widely accepted that a dependability component to location would provide facilities for PSAP policy-based routing, though a requirement to support this function is yet to be agreed upon.

6.3 Calling Trends

Calling trends world-wide as well as in North America are towards mobile. Half of all emergency calls in the USA through 2005 originated from a mobile service, while 60% of all long distance calls originated from mobiles. These figures indicate that wireless is no longer a minority case, but the dominant traffic base and this should be taken into account when looking at location determination and acquisition techniques. Designing two infrastructures-one for wireless and one for wireline-is not a desirable outcome particularly when an infrastructure designed to support wireless can easily accommodate wireline service. The pros and cons for implementing location by-reference versus location by-value conveyance should be re-examined in this context. A comparison of some of these characteristics can be found in [19].

7 Location Acquisition Methods

Location determination is the act of using measurements taken from the access network to calculate or compute the physical location of a device. The computations may be relatively simple, such as looking up switch and port values in a database, or they may be algorithmically complex, such as computing location based on angle of arrival radio signals. Location determination is, by its very nature, a process that is dependent on the context of the access network (refer to Section 8 for an example).

Location acquisition is the act of obtaining location information once location has been determined. Location information is acquired by accessing a network service, a LIS, and is done without requiring specific knowledge about the type of access network.

Three methods for location acquisition are described in the following subsections.

7.1 DHCP Location Acquisition

The DHCP location acquisition mechanism treats physical location information as host configuration data, in the same manner that it treats DNS server IP addresses for example, consequently it delivers location to the End-Point in the same manner, as a DHCP option. Two IETF specifications exist for obtaining location information over DHCP. RFC-3825, [16] provides a

format for delivering binary geodetic location information to the VEP, while draft-ietf-geopriv-dhcp-civil [17] is concerned with providing the End-Point with civic location information.

One advantage of the DHCP acquisition mechanism is that many networks already have DHCP servers, service discovery for DHCP is well understood, and implementations are widely available.

In both DHCP options however, the End-Point must take the location provided and structure it in a form suitable for representation in a PIDF-LO. Some fields pertinent to a PIDF-LO are not provided in these options, so they are not available in the PIDF-LO, or the End-Point must make assumptions as to the correct values. In addition only location by-value can be provided; there is no support for a location by-reference mechanism using DHCP.

Care must be taken when using the DHCP geodetic representation because the resulting shape is a 2D polygon, or 3D prism. Neither provides geodetic locations suitable for routing in the i2 architecture. The primary reason for this is that the VE2 interface in i2 is only capable of supporting point; point and radius; and point radius and altitude shape types. A conversion from a 2D rectangle to a circle will introduce additional uncertainly and a potential loss of precision. In addition to this, location provided to the VPC and used for routing would not be the same as the location provided to the PSAP.

7.2 LLDP-MED Location Acquisition

The Link Layer Discovery Protocol (802.1AB) is designed to allow stations connected to an 802 LAN segment to advertise their capabilities and functions to other stations connected to the same LAN segment. This information can then be collated and represented in a standard Management Information Base (MIB) and subsequently transferred to a centralized network management system (NMS) using SNMP or other similar network management protocol. Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP-MED) [14], specifies extensions to the base LLDP protocol which includes location delivery to the end-point from an LLDP-MED enabled switch. The location representations available in LLDP-MED are replications of those offered through DHCP and provide a geodetic zone encoded in the same manner as described in [16] and [17].

Since LLDP and hence LLDP-MED are targeted at enterprise environments they will not be addressed further in this version of the document.

7.3 HELD Location Acquisition

The HELD protocol is an application layer location acquisition protocol defined in draft-winterbottom-geopriv-held-sighting [18]. The HELD protocol is designed to support acquiring location by-value or by-reference over a range of IP access networks. The HELD protocol is an XML webservices-based protocol with an HTTP binding. It can provide a very simple request (HTTP GET) and response mechanism for location requests or more complex application-based requests for location information in specific forms.

A key premise of the HELD protocol is that a device can be uniquely identified by its IP address and that the LIS can use this information to provide location. How the LIS uses the IP address to

determine the location of the device is outside of the scope of the HELD protocol, but location determination sections later in the document will show some ways that this is possible.

Where location is requested using the HELD protocol, the LIS will return location in PIDF-LO form, so any location representations possible in a PIDF-LO can be supported by the HELD protocol. Additionally, all parameters pertinent to the location, such as provided-by and method can be returned in the PIDF-LO with no assumptions being required on the part of the recipient.

8 xDSL Residential Broadband Configurations

This section details on how to support location determination and location acquisition in a variety of DSL-based networks. The solution list is not exhaustive, but it is representative. Only the HELD location acquisition protocol is considered at the time of writing; no workable DHCP location determination and acquisition mechanism has yet been proposed[2].

As was described in Section 7.3, the HELD protocol relies on the IP address of a device being unique within the domain of the LIS, and it uses this IP address as the key to providing location. A LIS is responsible for determining and providing location for devices within its domain. Therefore, in order to use the HELD protocol, a LIS needs to gather sufficient measurements from the network to allow it to link an IP address to location. These network measurements are provided by an access location entity (ALE) and will differ for each access network type. In the networks described in the following subsections two ALE types are described; an ALE based around RADIUS messages (described in [6], [7], [8], [9] and [10]) and a second based on DHCP relay information (described in [4]).

Point-to-Point Protocol (PPP) solutions in DSL networks are popular for a number of reasons. One of the major reasons is that it greatly simplifies provisioning for the region access provider as initial destinations are determined based on domain names included in the PPP authentication data. As was described in Section 5.4.1, much of the difference in DSL networks occurs in data that is transferred from the regional access aggregator (BRAS) to the ISP's network access server (NAS), i.e. over the A-Interface. In the subsections that follow we will look at three A-Interface types, IP-based routing, Layer 2 forwarding and Layer 2 Tunnelling Protocol (L2TP).

8.1 IP Connectivity over the Service Provider Segment

In this configuration, traffic is directed from the Aggregator to the ISP using conventional IP routing.

[2] However, it should be noted that the DSL Forum has begun work that would require new DSL Aggregation Modules (DSLAMs) to support the DHCP relay options, data from which could be used to aid location determination.

One Nation 9-1-1 One Number

Figure 8-1 IP Connectivity

1. A DSL modem is connected to PVC-1 and tries to connect to the ISP using PPP.
2. The DSL modem forwards the PPP authentication credentials to the network.
3. The Aggregator receives the PPP connection and passes the authentication message, along with the Aggregator ID (NAS-ID) and Aggregator port (NAS Port) to the regional access network provider's (RANP's) RADIUS server.
4. The RADIUS server proxies the request to the ISP RADIUS server.
5. The ISP's RADIUS server authenticates the user and returns an IP address to the RANP's RADIUS server. An ALE at the ISP's RADIUS server forwards the IP address and RANP-ID to the ISP's LIS.
6. An ALE at the RANP's RADIUS server forwards the NAS-ID, NAS-Port and IP-Address to the RANP LIS.
7. The RANP's RADIUS server returns the IP address to the Aggregator and back to the DSL modem.

The RANP LIS must be able to link the NAS-ID and NAS-Port to the incoming PVC (PVC-1) on the DSLAM and this will need to be done through the co-operation and provisioning of OSS systems.

A location request from a device attached to the DSL modem will go the ISP LIS. The ISP LIS will look up the IP address to determine which RANP is providing the access. The ISP LIS will then make a request to the RANP LIS for the location associated with the IP address. So the chain to determine location is as follows:

IP → RANP-LIS → NAS-ID,NAS-Port → PVC-B → PVC-A → PVC-1 → Location

8.2 Layer 2 Forwarding over the Service Provider Segment

Where Layer 2 forwarding is employed the connectivity is over ATM or Ethernet. Where ATM is used, the RANP LIS maintains a mapping between the incoming vpi/vci to the BRAS and the outbound vpi/vci to the Service Provider. This mapping provides the necessary associations for the RANP LIS to determine location. Association back to an IP address is dependent on the ISP providing IP address to incoming vpi/vci information.

Figure 8-2 ATM Based Layer 2 Forwarding

Ethernet configurations generally stem back to the Access Node (AN or DSLAM) and can further be broken down into 1:1 VLAN and N:1 VLAN configurations. 1:1 VLAN configurations use a combination of two VLAN tags, referred to as double tagging, to uniquely identify a data stream. Traffic coming in on a specific DSLAM port is tagged with a VLAN-ID tag referred to as the C-TAG, traffic exiting a DSLAM bound for the Aggregator is tagged with a second VLAN-ID referred to as the S-TAG. The combination of S-TAG and C-TAG uniquely identify a DSLAM and port in the DSL network.

Figure 8-3 1:1 VLAN Layer 2 Fowarding

In N:1 VLAN configurations the DSLAM combines multiple data streams bound for the Aggregator under a single VLAN. End-Points acquire IP addresses through the aid of relay-agents (PPP/RADIUS or DHCP) in the DSLAM, and the Aggregator builds ARP tables for devices attached to each DSLAM to facilitate the correct routing of traffic. A centralized Relay/Server function in the RANP can then be used to generate the required associations to a LIS enabling location determination.

DRAFT

Figure 8-4 N:1 VLAN Layer 2 Forwarding

In all three of these configurations a location is requested in the same manner. A device attached to the DSL modem (CPE in the diagram) will request location from the ISP LIS. The ISP LIS will look up the IP address to determine which RANP is providing the access. The ISP LIS will then make a request to the RANP LIS for the location associated with the IP address; the query will contain any RADIUS attributes that were received from the RADIUS-ALE. The location is then returned from the RANP-LIS to the ISP-LIS to the requesting node.

8.3 L2TP over the Service Provider Segment

In this configuration one or more tunnels exist between the RANP's BRAS and the ISP's NAS, and each tunnel is made up of several sessions. L2TP is described in detail in [5].

Figure 8-5 L2TP Access Segment

1. A DSL modem connects to the DSLAM over PVC-1, through an ATM cloud and on to the Regional Access Network Provider's (RANP) Aggregator.
2. The DSL modem attempts to establish a PPP connection, and sends user@domain.com and password.
3. The Aggregator intercepts the connection establishment message and sends the domain information to the RADIUS server in an Access-Request message. This behavior is specified in [28] section 4.1.2.3. The Access-Request message may also contain the NAS-IP, NAS-ID, NAS-Port or NAS-Port-Id fields.
4. The RANP's RADIUS server determines the tunnel down which the Aggregator must direct traffic. This is the Tunnel-Server-Endpoint, which is assumed to be an IP address, and the Tunnel-Assignment-Id which is a string describing the local name for the tunnel. Both of these attributes are described in [9]. These are returned to the Aggregator in an Access-Response message from the RADIUS server.
5. If the Aggregator does not have an existing tunnel called Tunnel-Assignment-Id open with the Tunnel-Server-Endpoint (the ISP's NAS) then it will create one; otherwise it will use the existing tunnel.
6. Once a tunnel exists between the Aggregator and the ISP's NAS, a link is created in the tunnel. Both the Aggregator and the ISP's NAS independently send accounting records identifying this association to their respective RADIUS servers. The most common way to uniquely identify a link within a given L2TP tunnel (as defined in [5]) is to use the Tunnel-

DRAFT

One Nation 9-1-1 One Number

Client-Endpoint (in this case the Aggregator), the Tunnel-Server-Endpoint (in this case the ISP's NAS) and a call-serial-number, a unique 32 bit number.

The accounting record from the Aggregator will consist of the parameters defined in section 3.4 of [8] with the following parameters specifically being used to assist with location determination:

NAS-IP-Address

NAS-Port (32 bit integer) or NAS-Port-ID (string). When a NAS-Port-ID is used, convention seems to be in the form atm <slot>/<port>:<vpi>.<vci>

Tunnel-Type

Tunnel-Medium

Tunnel-Client-Endpoint (the RANP's end of the tunnel)

Tunnel-Server-Endpoint (the ISP's end of the tunnel)

Acct-Tunnel-Connection (the 32 bit call-serial-number)

The accounting record from the ISP's NAS will be similarly constructed but will also contain the username.

7. The RANP's RADIUS server sends the NAS-ID, NAS-Port, Tunnel-Client-Endpoint, Tunnel-Server-Endpoint and Acct-Tunnel-Connection information on to the RANP's LIS. The RANP's LIS is able to associate NAS-ID and NAS-Port to a specific DSLAM port, and hence a physical location. The RANP's LIS keys this location against the Tunnel-Client-Endpoint, Tunnel-Server-Endpoint and Acct-Tunnel-Connection triplet.
8. The ISP's RADIUS server sends IP address, Tunnel-Client-Endpoint, Tunnel-Server-Endpoint and Acct-Tunnel-Connection to the ISP's LIS.
9. A subsequent location request from the ISP LIS to the RANP LIS must include the Tunnel-Client-Endpoint, Tunnel-Server-Endpoint and Acct-Tunnel-Connection triplet to find the location record.

DRAFT

Figure 8-6 L2TP over the Service Provider Segment Message Flow

8.4 LIS Discovery in a DSL Environment

In order to request location from a LIS and IP endpoint must first learn the identity of the LIS. This may be done either by manually provisioning the URL for the LIS into the IP endpoint or by the IP endpoint using a mechanism to dynamically discover the address of the LIS. This section proposes one way in which an IP endpoint can dynamically discover a LIS through DNS records. This mechanism requires knowledge of the domain name of the access provider serving the IP endpoint. The domain name of the access provider in many circumstances is available directly from the home router via DHCP (Option 15 see [23]), and in many cases this domain name is adopted for use with the home computers and networks. In some cases however it is not. For example, when a laptop is taken home from work it often maintains the domain name of the company owning the laptop, e.g. andrew.com. In this latter situation more complex access domain name discovery techniques are required and ways of achieving this are described in following subsections.

Knowing the domain name of the serving access network allows a Device to query the local DNS server and perform service discovery for the LIS. The discovery technique described is based around conventional DNS SRV records detailed in Section 8.4.3.

8.4.1 IP Address Determination

Figure 8-7 shows the domain discovery problem as it relates to a typical residential broadband network. The home-router runs an internal DHCP server that provides IP addresses from a private address range. The home-router itself is provided an externally routable IP address from the ISP and performs NAT between the internal and external networks. The externally routable IP address is associated with the domain name belonging to the ISP, “my.isp.net” (Figure 8-7). To discover the local access domain name a client must first determine the external IP-address of the home-router; three mechanisms for discovering this IP-address are described.

Figure 8-7 Address Discovery Problem

8.4.1.1 Universal Plug and Play (UPnP)

This mechanism makes use of the UPnP Internet Gateway Device (IGD) specification which is supported in many home-routers to allow PC applications and the like to operate seamlessly through the router’s NAT function. The HELD-Client in this case acts as a UPnP Control Point (CP) and requests the external IP address of the router using the “GetExternalIPAddress” action defined in [26].

This mechanism has the advantage that UPnP is a SOAP-based protocol running on top of HTTP, making it easy to implement as the HELD-Client is also built on top of HTTP.

8.4.1.2 WEB Report

To use this mechanism a VSP or other trusted network entity establishes a website, that when accessed returns the IP address of the requesting node. A variety of clients that support this function are listed at the website detailed in [27].

8.4.1.3 STUN

One way to determine the external IP address of the home-router is to use STUN. STUN [24] defines a mechanism that is able to determine the IP address on the public side of a NAT. STUN is a simple client-server based protocol and as such requires a STUN server. Because of the way STUN works, it not necessary for the STUN server to reside in the same access network as the Device, but it is necessary that the STUN server be reachable by the Device.

The recommendation here is that the Voice Service Provider (VSP) provide the STUN server to assist the VSP's customers in gaining access to a service from any access network. The rationale is that the Device must already have a trust relationship with the VSP; consequently the various identity and integrity recommendations for STUN can be easily satisfied.

This document will not go into a full working description of STUN which is described in [24]. The expectation is that a STUN-client be associated with the HELD-client and that it issues a STUN binding request to the STUN-server at the VSP. The STUN-server will respond with a MAPPED-ADDRESS message indicating the external IP address of the home-router gateway.

8.4.1.4 Recommendation

Three mechanisms for dynamically determining the external IP address of a home-router have been described; each has its advantages and disadvantages. An alternative mechanism to dynamically determining the external IP address is to have this address manually configured into the IP endpoint. Such a mechanism is possible where the address is known ahead of time and never changes.

Different network /service providers are likely to offer and implement services that best suit them. It is therefore necessary that HELD-Clients implement all mechanisms for determining the external IP-address of the home router. The recommended order in which to try these is:

a) UPnP
b) WEB Report
c) STUN
d) Manually configured

8.4.2 Domain Determination

Where the domain is not known, it must be determined. Once the Device knows its external IP address it can determine its access domain name by performing a reverse DNS lookup. This requires the ISP to populate `in-addr.arpa` records into its DNS for all IP addresses so that the resolution can occur. The generally accepted format for the resulting fully-qualified domain name (FQDN) would be `ip-address.my.isp.net`.

The HELD client MUST use the entire domain name trailing the IP address. For example, `205.188.192.203.my.isp.net` would yield `my.isp.net` as the domain on which to query.

Where the access provider has a DNS that services multiple zones under the `isp.net` domain, for example `my.isp.net` and `your.isp.net` and `their.isp.net`, the access provider MUST ensure that a LIS resolving record for each zone is provisioned, even if they point ultimately to the same LIS.

DRAFT

8.4.3 DNS SRV Record LIS Discovery

This is the first of two LIS discovery techniques; it is dependent on knowing the domain name of the access provider. The ISP must provision a DNS SRV record in the following form:

```
_locserv+https._tcp SRV 1 0 <port> <Hostname of LIS>
```

In response to a query for the _locserv+http._tcp service the DNS will return the FQDN and port for the LIS service. The client will assume that all HELD requests are made against the root URI on the returned host.

For example if the DNS were to return: `held.lis.my.isp.net` with a port of `10001` then the client may obtain location from that service with the following:

https://held.lis.my.isp.net:10001/

Figure 8-8 shows the message flow between nodes when the DNS SRV LIS discovery mechanism is used. The figure shows STUN being used as example for external IP discovery.

Figure 8-8 DNS SRV LIS Discovery

8.4.4 Requirements

If LIS discovery using DNS is to be successful, the following requirements must be taken into account

1) Where fixed devices are used, the LIS URL should be configured into the device ahead of time, either manually or by the manufacturer.

One Nation 9-1-1 One Number

DRAFT

2) A VSP SHOULD supply a STUN server or WEB IP discovery service
3) A HELD-client MUST support UPnP-CP functionality, HTTP IP determination client and a STUN-client.
4) An ISP must support `in-addr.arpa` for local IP addresses to support reverse DNS lookup
5) An ISP must support _locserv+https._tcp SRV record

In the future there may be other LIS discovery protocols and techniques and these should be adopted where necessary.

9 LIS Provisioning Guidelines

This section provides guidance about what information should be provisioned into a LIS, and how to structure that information into a PIDF-LO. Routing calls based on location, specifically civic location, puts constraints on that location extending to representation, interpretation and sources of information.

The PIDF-LO profile draft [29] describes mechanisms for producing and interpreting the contents of PIDF-LO documents. The PID-LO profile draft also describes the acceptable geodetic shapes that may be used for emergency call routing. The PIDF-LO profile draft [29] does not however discuss the notion of location validation or which civic fields are required for civic location-based emergency call routing. This is largely because these are national/local concerns and consequently for North America need to be described in national standards. For i2, the corresponding PIDF-LO to VE2 field mappings are defined in the i2 specification and at this point in time, it is anticipated that at least these same fields will be required for civic routing in an i3 environment.

To route an emergency call based on civic location, it is necessary that the civic location can be mapped to yield a valid route to a PSAP; whether the resulting PSAP address is a URI, or an ESRN/ESQK pair is immaterial. Therefore the LIS operator must ensure that all civic address information in the LIS is valid and that the civic location is in a form that can be used to determine the correct PSAP to route the emergency call to.

Provisioning constraints are not restricted to civic formats. As mentioned the PIDF-LO profile draft makes recommendations on acceptable geodetic shapes for emergency routing applications. Specifically this draft indicates that in some countries, such as the United States VoIP migratory standards are being deployed that make use of existing cellular interfaces to convey location to PSAPs. Reusing these interfaces, in particular the E2 interface, imposes some restrictions on acceptable shape types for emergency usage. At the time of writing these restrictions confine geodetic shape representation to a point, circle or sphere as defined in the GeoShape specification [20].

Where a LIS operator intends to use DHCP as a means to provide geodetic location information for use in emergency routing, extreme care should be taken to avoid the pitfalls outlined in Appendix A of the PIDF-LO profile draft. The severe nature of the errors induced by the DHCP geodetic encoding scheme for uncertainty make this mechanism unsuitable for specifying areas for emergency location representation. However, if location must be provided in geodetic form over DHCP by a LIS provider then the IP endpoint MUST interpret the location as literal point rather than attempting to apply uncertainty as specified through bit resolution in RFC-3825.

10 References

The references used throughout this document are detailed in this section.

[1] **RFC-4119**, A Presence-based GEOPRIV Location Object Format, J. Peterson December 2005
[2] **RFC-2131**, Dynamic Host Configuration Protocol, R. Droms March 1997
[3] **RFC-951**, Bootstrap Protocol (BOOTP), B. Croft, J. Gilmore September 1985
[4] **RFC-3046**, DHCP Relay Agent Information Option, M. Patrick January 2001
[5] **RFC-2661**, Layer Two Tunneling Protocol (L2TP), W. Townsley, A. Velcia, A. Rubens, G. Pall, G. Zorn, B. Palter, August 1999
[6] **RFC-2865**, Remote Authentication Dial In User Service (RADIUS), C. Rigney, S. Willens, A. Rubens, W. Simpson, June 2000
[7] **RFC-2866**, RADIUS Accounting, C. Rigney, June 2000
[8] **RFC-2867**, RADIUS Accounting Modification for Tunnel Protocol Support, G. Zorn, B. Aboba, D. Mitton, June 2000
[9] **RFC-2868**, RADIUS Attributes for Tunnel Protocol Support, G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret, June 2000
[10] **RFC-2869**, RADIUS Extensions, C. Rigney, W. Willats, P. Calhoun, June 2000
[11] **TR-101**, Technical Report DSL Forum TR-101, Migration to Ethernet-Based DSL Aggregation, April 2006.
[12] **TR-058**, Technical Report DSL Forum TR-058, Multi-Service Architecture & Framework Requirements, September 2003.
[13] **TR-059**, Technical Report DSL Forum TR-059, DSL Evolution – Architecture Requirements for the Support of QoS-Enabled IP Services, September 2003.
[14] **TIA-1057 (TR-41.1)**, Link Layer Discovery Protocol for Media Endpoint Devices
[15] **TR-069**, Technical Report DSL Forum TR-069, CPE WAN Management Protocol, May 2004.
[16] **RFC-3825**, Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information, J. Polk, J. Schnizlein, M. Linsner July 2004
[17] **draft-ietf-geopriv-dhcp-civil-09**, Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Address Configuration Information, H. Schulzrinne January 2006
[18] **draft-winterbottom-geopriv-held-sighting-00**, HTTP Enabled Location Delivery (HELD)-Sighting, J. Winterbottom M. Thomson B. Stark January 2006
[19] **draft-winterbottom-location-uri-01**, Rationale for Location by Reference, J. Winterbottom M. Thomson J. Peterson January 2006
[20] **draft-thomson-geopriv-geo-shape-01**, Geodetic Shapes for the Representation of Uncertainty in PIDF-LO, M. Thomson January 2006
[21] **draft-ietf-geopriv-revised-civic-lo-02**, Revised Civic Location Format for PIDF-LO, M. Thomson J. Winterbottom January 2006
[22] **NENA-05-001** December 2003, NENA Standard for the Implementation of the Wireless Emergency Service Protocol E2 Interface
[23] **RFC-2132**, DHCP Options and BOOTP Vendor Extensions
[24] **RFC-3489**, STUN, Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
[25] **RFC-3958**, Domain-Based Application Service Location Using SRV RRs and the Dynamic Delegation Discovery Service (DDDS)

[26] WANIPConnection:1 **Service Template Version 1.01 For UPnP™ Version 1.0**, Status: Standardized DCP, Date: November 12, 2001

[27] http://www.snapfiles.com/freeware/network/fwip.html

[28] **RFC-2809**, Implementation of L2TP compulsory Tunneling via RADIUS, B. Aboba G. Zorn April 2000

[29] **draft-ietf-geopriv-pdif-lo-profile-04**, GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations, J. Winterbottom, M. Thomson, H. Tschofenig, March 2006.

DRAFT