Network Working Group H. Tschofenig
Internet-Draft Nokia Siemens Networks
Intended status: Informational H. Schulzrinne
Expires: October 8, 2007 Columbia U.
April 6, 2007

GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements

draft-ietf-geopriv-l7-lcp-ps-01.txt

Status of this Memo

Copyright Notice

Abstract

This document provides a problem statement, lists requirements and captures discussions for a GEOPRIV Layer 7 Location Configuration Protocol (LCP). This protocol aims to allow an end host to obtain location information, by value or by reference, from a Location Server (LS) that is located in the access network. The obtained location information can then be used for a variety of different protocols and purposes. For example, it can be used as input to the Location-to-Service Translation Protocol (LoST) or to convey location within SIP to other entities.

Table of Contents

1. Introduction

This document provides a problem statement, lists requirements and captures discussions for a GEOPRIV Layer 7 Location Configuration Protocol (LCP). The protocol has two purposes:

- It is used to obtain location information from a special node, called the Location Server (LS).

- It enables the end host to obtain a reference to location information. This reference can take the form of a subscription URI, such as a SIP presence URI, an HTTP/HTTPS URI, or any others. The requirements related to the task of obtaining such a reference are described in a separate document, see [4].

The need for these two functions can be derived from the scenarios presented in Section 3.

For this document we assume that the GEOPRIV Layer 7 LCP runs between the end host (i.e., the Target in [1] terminology) acting as the LCP client and the Location Server acting as an LCP server.

This document splits the problem space into separate parts and discusses them in separate subsections. Section 4 discusses the challenge of discovering the Location Information Server in the access network. Section 5 compares different types of identifiers that can be used to retrieve location information. A list of requirements for the GEOPRIV Layer 7 Location Configuration Protocol can be found in Section 6.

This document does not describe how the access network provider determines the location of the end host since this is largely a matter of the capabilities of specific link layer technologies.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [2], with the qualification that unless otherwise stated these words apply to the design of the GEOPRIV Layer 7 Location Configuration Protocol.

We also use terminology from [1] and [3].

3. Scenarios

This section describes a few network scenarios where the GEOPRIV Layer 7 Location Configuration Protocol may be used. Note that this section does not aim to list all possible deployment environments exhaustively. We focus on the description of the following environments:

- o DSL/Cable networks, WiMax-like fixed access

- o Airport, City, Campus Wireless Networks, such as 802.11a/b/g, 802.16e/Wimax

- o 3G networks

- o Enterprise networks

We illustrate a few examples below.

3.1. Fixed Wired Environment

The following figure shows a DSL network scenario with the Access

Network Provider and the customer premises. The Access Network Provider operates link and network layer devices (represented as Node) and the Location Server (LS).


```
+---------------------------+
|                           |
|  Access Network Provider  |
|                           |
|   +---------+             |
|   | Node    |             |
|   +---------+ +-----------+ |
|       |  |   | LS        | |
|       |  +---|           | |
|       |      +-----------+ |
|       |                   |
+-------+-------------------+
        | Wired Network
<----------------> Access Network Provider demarc
        |
```

```
+-------+-------------------+
|       |                   |
|   +--------------+        |
|   | NTE          |        |
|   +--------------+        |
|       |                   |
|       |                   |
|   +---------------+       |
|   | Device with   | Home  |
|   | NAPT and      | Router|
|   | DHCP server   |       |
|   +---------------+       |
|       |                   |
|       |                   |
|    +-------+              |
|    | End   |              |
|    | Host  |              |
|    +-------+              |
|                           |
|Customer Premises Network  |
|                           |
+---------------------------+
```

Figure 1: DSL Scenario

The customer premises consists of a router with a Network Address Translator with Port Address Translation (NAPT) and a DHCP server as used in most Customer Premises Networks (CPN) and the Network Termination Equipment (NTE) where Layer 1 and sometimes Layer 2 protocols are terminated. The router in the home network (e.g., broadband router, cable or DSL router) typically runs a NAPT and a DHCP server. The NTE is a legacy device and in many cases cannot be modified for the purpose of delivering location information to the

end host. The same is true of the device with the NAPT and DHCP server.

It is possible for the NTE and the home router to physically be in the same box, or for there to be no home router, or for the NTE and end host to be in the same physical box (with no home router). An example of this last case is where Ethernet service is delivered to customers' homes, and the Ethernet NIC in their PC serves as the NTE.

Current Customer Premises Network (CPN) deployments frequently show the following characteristics:

1. CPE = Single PC

    1. with Ethernet NIC [PPPoE or DHCP on PC]; there may be a bridged DSL or cable modem as NTE, or the Ethernet NIC might be the NTE

    2. with USB DSL or cable modem [PPPoA, PPPoE, or DHCP on PC]

    Note that the device with NAPT and DHCP of Figure 1 is not present in such a scenario.

2. One or more hosts with at least one router [DHCP Client or PPPoE, DHCP server in router; VoIP can be soft client on PC, stand-alone VoIP device, or Analog Terminal Adaptor (ATA) function embedded in router]

    1. combined router and NTE

    2. separate router with NTE in bridged mode

    3. separate router with NTE [NTE/router does PPPoE or DHCP to WAN, router provides DHCP server for hosts in LAN; double NAT

The majority of fixed access broadband customers use a router. The placement of the VoIP client is mentioned to describe what sorts of hosts may need to be able to request location information. Soft clients on PCs are frequently not launched until long after bootstrap is complete, and are not able to control any options that may be specified during bootstrap. They also cannot control whether a VPN client is operating on the PC.

3.2. Moving Network

An example of a moving network is a "WIMAX-like fixed wireless" scenario that is offered in several cities, like New Orleans, Biloxi, etc., where much of the communications infrastructure was destroyed

due to a natural disaster. The customer-side antenna for this service is rather small (about the size of a mass market paperback book) and can be run off battery power. The output of this little antenna is a RJ-45 Ethernet jack. A laptop can be plugged into this Ethernet jack. The user would then run a PPPoE client to connect to the network. Once the network connection is established, the user can run a SIP client on the laptop.

The network-side antenna is, for example, connected through ATM to the core network, and from there to the same BRASs that serve regular DSL customers. These Broadband Remote Access Servers (BRASs) terminate the PPPoE sessions, just like they do for regular DSL.

The laptop and SIP client are, in this case, unaware that they are "mobile". All they see is an Ethernet connection, and the IP address they get from PPPoE does not change over the coverage area. Only the user and the network are aware of the laptop's mobility.

Further examples of moving networks can be found in busses, trains, airplanes.

Figure 2 shows an example topology for a moving network.

```
+---------------------------+
| Wireless                  |
| Access Network Provider   |
|                           |
|              +-----------+|
|      +-------+ LS        ||
|      |       |           ||
|  +---+----+  +-----------+|
|  | Node   |               |
|  |        |               |
|  +---+----+               |
|      |                    |
+------+--------------------+
       | Wireless Interface
       |
+------+--------------------+
|      |    Moving Network  |
|  +---+----+               |
|  | NTE    |   +---------+ |
|  |        +---+ Host    | |
|  +-+-----++   |  B      | |
|    |     \    +---------+ |
|    |      \               |
|+---+----+  \  +---+----+  |
|| Host   |   \ | Host    | |
||  A     |    \+  B      | |
|+--------+     +---------+ |
+---------------------------+
```

Figure 2: Moving Network

3.3. Wireless Access

Figure 3 shows a wireless access network where a moving end host obtains location information or references to location information from the LS. The access equipment uses, in many cases, link layer devices. This figure represents a hotspot network found in hotels, airports, coffee shops. For editorial reasons we only describe a single access point and do not depict how the LS obtains location information since this is very deployment specific.

```
   +--------------------------+
   | Access Network Provider  |
   |                          |
   |              +----------+|
   |      +-------| LS       ||
   |      |       |          ||
   |  +--------+  +----------+|
   |  | Access |              |
   |  | Point  |              |
   |  +--------+              |
   |      |                   |
   +------+-------------------+
          |
        +------+
        | End  |
        | Host |
        +------+
```

Figure 3: Wireless Access Scenario

4. Discovery of the Location Information Server

When an end host wants to retrieve location information from the LS it first needs to discover it. Based on the problem statement of determining the location of the end host, which is known best by entities close to the end host itself, we assume that the LS is located in the access network. Several procedures have been investigated that aim to discovery the LS in such an access network.

DHCP-based Discovery:

In some environments the Dynamic Host Configuration Protocol might be a good choice for discovering the FQDN or the IP address of the LS. In environments where DHCP can be used it is also possible to use the already defined location extensions. In environments with legacy devices, such as the one shown in Section 3.1, a DHCP based discovery solution is not possible.

DNS-based Discovery:

With this idea the end host obtains its public IP address (e.g., via STUN [5]) in order to obtain its domain name (via the usual reverse DNS lookup). Then, the SRV or NAPTR record for that domain is retrieved. This relies on the user's public IP address having a DNS entry.

Redirect Rule:

A redirect rule at a device in the access network, for example at the AAA client, will be used to redirect the Geopriv-L7 signalling messages (destined to a specific port) to the LS. The end host could then discover the LS by sending a packet to almost any address (as long as it is not in the local network). The packet would be redirected to the respective LS being configured. The same procedure is used by captive portals whereby any HTTP traffic is intercepted and redirected.

Multicast Query:

An end node could also discover a LS by sending a multicast request to a well-known address. An example of such a mechanism is multicast DNS (see [6] and [7]).

The LS discovery procedure raises deployment and security issues. When an end host discovers a LS,

1. it does not talk to a man-in-the-middle adversary, and

2. it needs to ensure that the discovered entity is indeed an authorized LS.

5. Identifier for Location Determination

The LS returns location information to the end host when it receives a request. Some form of identifier is therefore needed to allow the LS to determine the current location of the target or a good approximation of it.

The chosen identifier needs to have the following properties:

Ability for end host to learn or know the identifier:

The end host MUST know or MUST be able to learn the identifier (explicitly or implicitly) in order to send it to the LS. Implicitly refers to the situation where a device along the path between the end host and the LS modifies the identifier, as it is done by a NAT when an IP address based identifier is used.

Ability to use the identifier for location determination:

The LS MUST be able to use the identifier (directly or indirectly) for location determination. Indirectly refers to the case where the LS uses other identifiers locally within the access network, in addition to the one provided by the end host, for location determination.

Security properties of the identifier:

Misuse needs to be minimized whereby off-path adversary MUST NOT be able to obtain location information of other hosts. A on-path adversary in the same subnet SHOULD NOT be able to spoof the identifier of another host in the same subnet.

The problem is further complicated by the requirement that the end host should not be aware of the network topology and the LS must be placed in such a way that it can determine location information with the available information. As shown in Figure 1 the host behind the NTE/NAPT-DHCP device is not visible to the access network and the LS itself. In the DSL network environment some identifier used at the NTE is observable for by the LS/access network.

The following list discusses frequently mentioned identifiers and their properties:

Host MAC address:

The host MAC address is known to the end system, but not carried over an IP hop.

ATM VCI/VPI:

The VPI/VCI is generally only seen by the DSL modem. Almost all routers in the US use 1 of 2 VPI/VCI value pairs: 0/35 and 8/35. This VC is terminated at the DSLAM, which uses a different VPI/VCI (per end customer) to connect to the ATM switch. Only the network provider is able to map VPI/VCI values through its network. With the arrival of VDSL, ATM will slowly be phased out in favor of Ethernet.

Switch/Port Number:

This identifier is available only in certain networks, such as enterprise networks, typically available via proprietary protocols like CDP or, in the future, 802.1ab.

Cell ID:

This identifier is available in cellular data networks and the cell ID might not be visible to the end host.

Authenticated User Identity:

In DSL networks the user credentials are, in many cases, only known by the router and not to the end host. To the network, the authenticated user identity is only available if a network access authentication procedure is executed. In case of roaming it still might not be available to the access network since security protocols might provide user identity confidentiality and thereby hide the real identity of the user allowing the access network to only see a pseudonym or a randomized string.

Host Identifier:

The Host Identifier introduced by the Host Identity Protocol [8] allows identification of a particular host. Unfortunately, the network can only use this identifier for location determination if the operator already stores an mapping of host identities to

location information. Furthermore, there is a deployment problem since the host identities are not used in todays networks.

Cryptographically Generated Address (CGA):

The concept of a Cryptographically Generated Address (CGA) was introduced by [9]. The basic idea is to put the truncated hash of a public key into the interface identifier part of an IPv6 address. In addition to the properties of an IP address it allows a proof of ownership. Hence, a return routability check can be omitted.

Network Access Identifiers:

A Network Access Identifier [10] is only used during the network access authentication procedure in RADIUS [11] or Diameter [12]. Furthermore, in a roaming scenario it does not help the access network to make meaningful decisions since the username part might be a pseudonym and there is no relationship to the end host's location.

Unique Client Identifier

The DSL Forum has defined that all devices that expect to be managed by the TR-069 interface be able to generate an identifier as described in DSL Forum TR-069v2 Section 3.4.4. It also has a requirement that routers that use DHCP to the WAN use RFC 4361 [13] to provide the DHCP server with a unique client identifier. This identifier is, however, not visible to the end host with the assumption of a legacy device like the NTE. If we assume that the LTE can be modified then a number of solutions come to mind including DHCP based location delivery.

IP Address:

The end host's IP address may be used for location determination. This IP address is not visible to the LS if the end host is behind one or multipel NATs. This is, however, not a problem since the location of a host that is located behind a NAT cannot be determined by the access network. The LS would in this case only see the public IP address of the NAT binding allocated by the NAT, which is the correct behavior. The property of the IP address for a return routability check is attractive as well to return location information only to a device that transmitted the request. The LS receives the request and provides location information back to the same IP address. If an adversary wants to learn location information from an IP address other than its own IP address then it would not see the response message (unless he is on the subnetwork or at a router along the path towards the LS) since the LS would return the message to the address where it came from.

On a shared medium an adversary could ask for location information of another host using its IP address. The adversary would be able to see the response message since he is sniffing on the shared medium unless security mechanisms (such as link layer encryption) is in place. With a network deployment as shown in Section 3.1 with multiple hosts in the Customer Premise being behind a NAT the LS is unable to differentiate the individual end points. For WLAN deployments as found in hotels, as shown in as shown in Section 3.3, it is possible for an adversary to eavesdrop data traffic and subsequently to spoof the IP address in a query to the LS to learn more detailed location information (e.g., specific room numbers). Such an attack might, for example, compromise the privacy of hotel guests. Note that DHCP would suffer from the same problem here unless each node uses link layer security mechanism.

Return routability checks are useful only if the adversary does not see the response message and if the goal is to delay state establishment. If the adversary is in a broadcast network then a return routability check alone is not sufficient to prevent the above attack since the adversary will observe the response.

6. Requirements

The following requirements and assumptions have been identified:

Requirement L7-1: Identifier Choice

The LS MUST be presented with a unique identifier of its own addressing realm associated directly or indirectly (i.e., linked through other identifiers) with the physical location of the end host.

An identifier is only appropriate if it is from the same realm as the one for which the location information service maintains identifier to location mapping.

Requirement L7-2: Mobility Support

The GEOPRIV Layer 7 Location Configuration Protocol MUST support a broad range of mobility from devices that can only move between reboots, to devices that can change attachment points with the impact that their IP address is changed, to devices that do not change their IP address while roaming, to devices that continuously move by being attached to the same network attachment point.

Requirement L7-3: Layer 7 and Layer 2/3 Provider Relationship

The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST NOT assume a business or trust relationship between the provider of application layer (e.g., SIP, XMPP, H.323) provider and the access network provider operating the LS.

Requirement L7-4: Layer 2 and Layer 3 Provider Relationship

The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST assume that there is a trust and business relationship between the L2 and the L3 provider. The L3 provider operates the

LS and needs to obtain location information from the L2 provider since this one is closest to the end host. If the L2 and L3 provider for the same host are different entities, they cooperate for the purposes needed to determine end system locations.

Requirement L7-5: Legacy Device Considerations

The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST consider legacy residential NAT devices and NTEs in an DSL environment that cannot be upgraded to support additional protocols, for example to pass additional information through DHCP.

Requirement L7-6: VPN Awareness

The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST assume that at least one end of a VPN is aware of the VPN functionality. In an enterprise scenario, the enterprise side will provide the LS used by the client and can thereby detect whether the LS request was initiated through a VPN tunnel.

Requirement L7-7: Network Access Authentication

The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST NOT assume prior network access authentication.

Requirement L7-8: Network Topology Unawareness

The design of the GEOPRIV Layer 7 Location Configuration Protocol MUST NOT assume end systems being aware of the access network topology. End systems are, however, able to determine their public IP address(es) via mechanisms such as STUN [5] or NSIS NATFW NSLP [14] .

Requirement L7-9: Discovery Mechanism

The GEOPRIV Layer 7 Location Configuration Protocol MUST provide a mandatory-to-implement discovery mechanism.

7. Security Considerations

This document addresses security aspect throughout the document.

8. IANA Considerations

This document does not require actions by IANA.

9. Contributors

This contribution is a joint effort of the GEOPRIV Layer 7 Location Configuration Requirements Design Team of the IETF GEOPRIV Working Group. The contributors include Henning Schulzrinne, Barbara Stark, Marc Linsner, Andrew Newton, James Winterbottom, Martin Thomson, Rohan Mahy, Brian Rosen, Jon Peterson and Hannes Tschofenig.

The design team members can be reached at:

Marc Linsner: mlinsner@cisco.com

Rohan Mahy: rohan@ekabal.com

Andrew Newton: andy@hxr.us

Jon Peterson: jon.peterson@neustar.biz

Brian Rosen: br@brianrosen.net

Henning Schulzrinne: hgs@cs.columbia.edu

Barbara Stark: Barbara.Stark@bellsouth.com

Martin Thomson: Martin.Thomson@andrew.com

Hannes Tschofenig: Hannes.Tschofenig@siemens.com

James Winterbottom: James.Winterbottom@andrew.com

10. Acknowledgements

We would like to thank the IETF GEOPRIV working group chairs, Andy Newton, Allison Mankin and Randall Gellens, for creating this design team. Furthermore, we would like thank Andy Newton for his support during the design team mailing list, for setting up Jabber chat conferences and for participating in the phone conference discussions.

We would also like to thank Murugaraj Shanmugam, Ted Hardie, Martin Dawson, Richard Barnes, James Winterbottom, Tom Taylor, Otmar Lendl, Marc Linsner, Brian Rosen, Roger Marshall, Guy Caron, Doug Stuard, Eric Arolick, Dan Romascanu, Jerome Grenier, Martin Thomson, Barbara Stark, Michael Haberler for their WGLC review comments.

11. References

11.1. Normative References

[1] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.

[3] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", draft-ietf-ecrit-requirements-13 (work in progress), March 2007.

11.2. Informative References

[4] Marshall, R., "Requirements for a Location-by-Reference Mechanism used in Location Configuration and Conveyance", draft-marshall-geopriv-lbyr-requirements-01 (work in progress), March 2007.

[5] Rosenberg, J., Weinberger, J., Huitema, C., and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[6] Aboba, B., "Link-local Multicast Name Resolution (LLMNR)", draft-ietf-dnsext-mdns-47 (work in progress), August 2006.

[7] Cheshire, S. and M. Krochmal, "Multicast DNS", draft-cheshire-dnsext-multicastdns-06 (work in progress), August 2006.

[8] Moskowitz, R., "Host Identity Protocol", draft-ietf-hip-base-07 (work in progress), February 2007.

[9] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[10] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[11] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[12] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[13] Lemon, T. and B. Sommerfeld, "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", RFC 4361, February 2006.

[14] Stiemerling, M., "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", draft-ietf-nsis-nslp-natfw-14 (work in progress), March 2007.

[15] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[16] Hardie, T., "LoST: A Location-to-Service Translation Protocol", draft-ietf-ecrit-lost-05 (work in progress), March 2007.

[17] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-sip-identity-06 (work in progress), October 2005.

[18] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

Authors' Addresses

Hannes Tschofenig
Nokia Siemens Networks
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Phone: +49 89 636 40390
Email: Hannes.Tschofenig@siemens.com
URI: http://www.tschofenig.com

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7004
Email: hgs+ecrit@cs.columbia.edu
URI: http://www.cs.columbia.edu

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).