Internet Engineering Task Force
Internet Draft
Intended status: Informational
Expires: January 10, 2013

X.Deng
M.Boucadair
France Telecom
X.Wang
BUPT

July 9, 2012

Using PCP to update dynamic DNS
draft-deng-pcp-ddns-01.txt

Abstract

This document focuses on the problems encountered when using dynamic DNS in address sharing contexts (e.g., DS-Lite, NAT64, A+P)during IPv6 transition. Issues, possible solutions and preliminary implementation and validation of one of the solutions are documented in this memo.

Status of this Memo

Copyright Notice

Table of Contents

1. Problem statement

Dynamic DNS (DDNS) is a widely deployed service to facilitate hosting servers (e.g., to host webcam and http server) at home premises. There are a number of providers who offer a DDNS service, working in a client and server mode. DDNS clients are generally implemented in the user's router or computer, which once detects changes to its IP address it automatically sends an update message to the DDNS server. The communication between the client and the server is not standardised, varying from one provider to another, although a few standard web-based methods of updating have emerged over time.

When the network architecture evolves towards an IPv4 sharing architecture during IPv6 transition, the DDNS Client will have to not only inform the IP address updates if any, but also to notify the changes of external port on which the service is listening, because a well know port numbers, e.g. port 80 will no longer be available to every web server. It will also require the ability to configuring corresponding port forwarding on CGN devices, so that incoming communications initiated from outside can be routed to the appropriate server behind the CGN.

This document focuses on the problems encountered when using dynamic DNS in address sharing contexts (e.g., DS-Lite, NAT64, A+P). Below are listed the main challenges to us:

(1)
The DDNS service MUST be able to maintain an alternative port number instead of the default port number.

(2)
Appropriate means to instantiate port mapping in the address sharing device MUST be supported.

(3)
DDNS client MUST be triggered by the change of the external IP address and the port number. Concretely, upon change of the external IP address, the DDNS client MUST refresh the DNS records otherwise the server won't be reachable from outside. This issue is event exacerbated in the DS-Lite context because no IPv4 address is assigned to the CPE.

This document describes solutions to counter the issues listed above in the particular case of DS-Lite.

Note DDNS may be considered as an implementation of the Rendez-vous service mentioned in [I-D.ietf-pcp-base].

"After creating a mapping for incoming connections, it is necessary to inform remote computers about the IP address, protocol, and port for the incoming connection. This is usually done in an application-specific manner. For example, a computer game might use a rendezvous server specific to that game (or specific to that game developer), a SIP phone would use a SIP proxy, and a client using DNS-Based Service Discovery [I-D.cheshire-dnsext-dns-sd] would use DNS Update [RFC2136][RFC3007]. PCP does not provide this rendezvous function. The rendezvous function may support IPv4, IPv6, or both. Depending on that support and the application's support of IPv4 or IPv6, the PCP client may need an IPv4 mapping, an IPv6 mapping, or both."

Dynamic Updates in the standard Domain Name System (DNS UPDATE) (RFC2136) is out of scope of this memo.

2. Solution Space

2.1. Locate a service port

At least two solutions can be used to associate a port number with a service identified:

(1)
Use service URIs (e.g., FTP, SIP, HTTP) which embed an explicit port number. Indeed, Uniform Resource Identifier (URI) defined in

[RFC3986] allows to carry port number in the syntax (e.g., mydomain.example:15687)

(2)
Use SRV records. Unfortunately, the majority of browsers do not support this record type.

DDNS client and server are to be updated so that an alternative port number is also signalled and stored by the server. Requesting remote hosts will be then notified with the IP address and port number to use to reach the server.

2.2. Detect the changes

```
                                       +------------------+
                                       |  DDNS Server     |
                                       |                  |
                                       +------------------+
                                              ^
                                              |
                                              |3. DDNS updates
                                              |  (if any)
                                              |
   +-----------------+                    +-----------------+
   |DDNS Client      |1. PCP MAP request  | CGN/PCP Server  |
   |PCP Client/IWF ON|-------------------->| (PCP mapping for 80:8080   +------+
   |CPE or           |2. PCP MAP response | port forwarding)|<---------|Client|
   |the host itself  |<-------------------|                 |          |      |
   |                 |3. DDNS updates     |                 |          +------+
   |                 |     (if any)       |                 |
   |                 |-------------------->|                 |
   +-----------------+                    +-----------------+
```

Figure 1 : Flow chat

First of all, PCP MUST be used to install the appropriate mapping in the CGN so that incoming packets can be delivered to the appropriate server.

In a network described in figure 1, DDNS Client/ PCP Client can either be running on a Customer Premise Equipment (CPE) or be running on the host that is hosting some services, itself. There are possible ways to address the problems stated in section 1.

(1)

If the DDNS client is enabled, the host issues periodically (e.g., 1h) PCP MAP requests (e.g., messages 1 and 2 in Figure 1) with short lifetime (e.g., 30s) for the purpose of enquiring external IP address and setting. If the purpose is to detect any change of external port, the host must issues a PCP mapping to install a mapping for the internal server. Upon change of the external IP address, the DDNS client updates the records (e.g., message 3 in Figure 1).

(2)

If the DDNS client is enabled, it checks the local mapping table maintained by the PCP client. This process is repeated periodically (e.g., 5mn, 30mn, 1h). If there is no PCP mapping caused by PCP client losing states for example, it issues a PCP MAP request (e.g., messages 1 and 2 in Figure 1) for the purpose of enquiring external IP address and setting up port forwarding mappings for incoming connections. Upon change of the external IP address, the DDNS client updates the records in the DDNS server, e.g., message 3 in Figure 1.

3. Implementation & Validation

So far the topology of network has been implemented as Figure 1. Based on the DS-Lite environment some new roles added into it such as DDNS. It could be implemented by Apache or other applications which has virtual host functions. The DDNS need to be configured as a virtual host and redirect corresponding request to the pointed IPv4 address and port number. It could be validated as Figure 2 shows.

```
  ---------   -----------    -----------   ----------   ----------------
  |User's |   |  DDNS    |    |  CGN&    |   | PCP     |   |Service Server|
  |Host   |---|  Server  |----|  PCP     |---| Client  |---|DDNS client   |
  |       |   |          |    |  Server  |   |         |   |              |
  ---------   -----------    -----------   ----------   ----------------
 Web Visitor     DDNS            AFTR         B4(CPE)       Web Server
```

Figure 2 : Implementation Chart

Web Visitor: Some users who need to access service on the Web Server. They send service request needed to resolve domain name. And the Web response would returned to their hosts as the ways of request reached to the Web Server.

DDNS: Maintaining mappings between domain name and external IPv4 address: port. If a DNS request was sent to it, DDNS server could resolve it to the AFTR which contains that IPv4 address and port number.

AFTR: Responsible for mappings between internal IPv4 Address: port and external IPv4 address: port. It maintains a table to restore these data to keep state of every mapping.

B4 (CPE): An endpoint of IPv4-in-v6 tunnel, and PCP client also runs on it. A package from Web Server is encapsulated into a IPv4-in-v6 one and is sent to the AFTR. A package from AFTR will be decapsulated to a normal IPv4 package and to their destination.

Web Server: Web server was deployed in the DS-Lite network environment. It just has private IPv4 address and with a mapping in AFTR to the public network. Web server may offer Web, FTP, SIP service and so on. And these services may not be set as their specific port. (this also is the reason why introducing DDNS into DS-Lite environment)

If the DDNS client is enabled, the A/AAAA records of DNS (which could be normal one as using on the Internet now) were set to point the DDNS Server. DDNS is responsible for the translation between public IPv4 address (address of DDNS) with specific port (E.g. web with 80 port) and public IPv4 address (outside IPv4 address and port number of mappings). Show as Figure 3.

```
  Web Visitor     DDNS             AFTR          CPE          Web Server

     | HTTP request | public         |encapsulated |               |

     |------------->| address: port  |private      |               |

     |              |--------------->|address: port|               |

     |              |                |------------>| HTTP request  |

     |              |          HTTP response       |-------------->|

     |<-------------|----------------|-------------|---------------|

     |              |                |             |               |
```

Figure 3 : Time Sequence Chart

If a user of another client outside DS-Lite network wants to access a Web Server behind AFTR, the role of DDNS started to become important. Before that the following mappings should had been configured well:

a. PCP mappings: private IPv4 address: port number <--> public IPv4 address: port number

b. DDNS mappings: public IPv4 address: port number <--> domain name

c. DNS Resolution: A/AAAA Records (point to the DDNS server) <--> domain name

A domain resolution request is sent from host of customer who asking service. The request is sent to the DNS server. And DNS server would return a DNS response with A/AAAA records pointing to the DDNS server. If the request is sent to the DDNS directly, it would redirect the request to the pointed IPv4 address and port number which has been configured in the mappings.

After redirection the request is routed to the AFTR. AFTR would translate it from public IPv4 address and port number into private IPv4 address and port. The request finished AFTR translation and is encapsulated into a IPv4-in-IPv6 package until CPE.

At last the request would be decapsulated to an IPv4 package and is sent to the service provider. And the Web response would return to

the customer as requested routine. The whole communication process is finished successfully.

From the view of Web visitor, the location of Web Server is on

DDNS, just like a virtual host. It at least has three advantages.

Firstly, hackers and other attackers couldn't reach the real host and do something bad. The security is assured. Secondly, many domain name or space ISPs also provide service of domain and port mapping. However, some companies may use iframe or 301 redirection technology. Those means could lead to lower speed and affect PR weights to the search engine. Click-through rate and visits was 'stolen'. That could not be introduced into Carrier Scale Network. Hence, generation of DDNS has its unique meaning. Thirdly, DDNS solution could solve the problems of IP address + port mapping almost perfectly. Under DS-Lite network environment normal DNS resolution couldn't point a domain name to a IP address and a port. Because of designing defect of traditional DNS protocol a DNS request just could be resolve to be a A/AAAA record (the services have their own specific port. Such as web is 80 and ftp is 21, etc.). So DDNS as a supplementary was introduced into DS-Lite to play a role of mapping between domain name and IP address and port number.

4. References

4.1. Normative References

[RFC2136]

P. Vixie, et. al." Dynamic Updates in the Domain Name System (DNS UPDATE)", April 1997.

[RFC3007]

B. Wellington, " Secure Domain Name System (DNS) Dynamic Update", November 2000.

[RFC3986]

T. Berners-Lee, et. al. " Uniform Resource Identifier (URI): Generic Syntax", January 2005.

4.2. Informative References

[I-D.ietf-pcp-base]

D. Wing, et. al. " Port Control Protocol (PCP)", June 5, 2012.

5. Authors' Addresses

Xiaohong Deng
France Telecom
Rennes,35000 France

Email: dxhbupt@gmail.com

Mohamed BOUCADAIR
France Telecom
Rennes,35000 France

Email: mohamed.boucadair@orange.com

Xu Wang
Beijing University of Posts and Telecommunications, China
Email: cngesaint@gmail.com