Internet Engineering Task Force
Internet Draft
Intended status: Informational
Expires: January 16, 2014

X.Deng
M.Boucadair
France Telecom
Q.Zhao
BUPT
J.Huang
Huawei

July 15, 2013

Using PCP to update dynamic DNS
draft-deng-pcp-ddns-03.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, which mostly use a web-form based communication. 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 Rendezvous service mentioned in [RFC6887].

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 to reach the services hosted behind a DS-Lite CGN. 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. RFC6281 shows an good example of how to use the DNS-Based Service Discovery to make the service announcement available, in an application manner. 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. In the implementation section, it gives an example how the DDNS server may implement such service notification functionality if they want.

This document requires no changes to PCP protocol or dynamic updates in the standard domain name system [RFC2136], but is rather an operational document to make the current DDNS service providers be aware of the impacts and issues that the IPv6 transitioning and IPv4 address sharing will bring to them, and gives solutions and

implementation examples to address the forthcoming issues. The current DDNS service providers usually employs a web-based form to maintain DDNS service registration and updates. For DNS-based Service Discovery, or DNS-SD and updates, [I-D.cheshire-dnsext-dns-sd] intensively describes how to use DNS resource records and standard DNS queries to facilitate service discovery, and [RFC6281] elaborates an implementation of it with an Apple's Back to My Mac (BTMM) Service.

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 chart

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

3.1. Topology

```
+--------------+   +--------+    +----------+   +--------+   +-------+
| Service      |   |  DDNS  |    |  CGN&    |   | PCP    |   |Servers|
| User         |---|  Server|----|  PCP     |---| Client |---|       |
|              |   |        |    |  Server  |   | /DDNS  |   |       |
|              |   |        |    |          |   | client |   |       |
+--------------+   +--------+    +----------+   +--------+   +-------+
A user             DDNS Server      AFTR           B4(CPE)    A host
From Internet                                                 behind B4
```

Figure 2 : Implementation topology

Servers: Servers that are deployed in the DS-Lite network, or more generally, an IP address sharing environment. They are usually running on a host that has been assigned with a private IPv4 address. Having created a proper mapping via PCP in AFTR, these services have been made available to the internet users. The services may provide Web, FTP, SIP and other services though these ones may not be able to been seen as using a well known port from the outside anymore, in the IP address sharing context.

B4 (CPE): An endpoint of IPv4-in-v6 tunnel. A PCP client together with a DDNS client are running on it. After PCP client establishes a mapping on the AFTR, an end uses may register its domain name and its external IPv4 address plus port number to its DDNS service provider (DDNS server), manually or automatically by DDNS client. Later, likewise, end users may manually or let DDNS client on behalf of it, to automatically announce IP and port changes to the DDNS server.

AFTR: Responsible for maintaining mappings between internal IPv4 Address plus port and external IPv4 address plus port.

DDNS server: Maintains a table linking a registered domain name and a pair of registered host's external IPv4 address plus port number. When being notified IP address and port number changes from DDNS client, DDNS server then announces the updates to DNS servers on behalf of end user. RFC 2136 and RFC 2137 may be used by DDNS server

to send updates to DNS servers. In many current practices, DDNS server provider usually announce its own IP address as the registered Domain names of end users. When Http requests reach the DDNS server, they may employ URL Forwarding or HTTP 301 redirection to redirect the request to a proper registered end user by looking up the maintained link table.

Service users: Users who wants to access services behind an IP address sharing network. They send out standard DNS requires to locate the request services, which, in our case, will lead them to a DDNS server, provided that the requested services have been registered to a DDNS service provider. Then the DDNS server will handle the rest in the way as described before.

3.2. For web service

While the current DDNS server implementations typically assume that the end servers host web server on the default 80 port. In the DS-Lite context, they will have to taken in to account that external port visible assigned by AFTR may be any the other numbers than 80, in order to maintain proper corresponding between domain names and external IP plus port. By doing such changes to implementation, the HTTP request would be redirected to the AFTR which servers the specific end host that are running servers. The following chat shows how the messages reach the right server.

```
   Web Visitor           DDNS server       AFTR          B4(CPE)  Web Server
behind b4

     | HTTP Get*              |                |               |               |
     |----------------------->|                |               |               |
     | ip_DDNS_server         |--------------->|               |               |
     |                        | HTTP 301       |               |               |
     |                        |<---------------|               |               |
     | HTTP Get* ip_aftr:8001                  |               |               |
     |---------------------------------------->|                               |
     |                                         | HTTP Get* ip_websrv:8000      |
     |                                         |------------------------------>|
     |                                         |                               |
     |                       HTTP response     | HTTP response                 |
     |<----------------------------------------|-------------------------------|
```

Figure 3 Http service messages

When a web user sends out a HTTP Get message to DDNS server after a standard DNS query, DDNS server redirects the request to a registered web server, in this case, by responding a HTTP 301 message. Then the HTTP get message will be sent out to the AFTR, which will in turn finds the proper hosts behind it. For simplicity, messages among AFTR, B4 and web server behind b4 are not shown completely, for communications among those nodes, please refer to [RFC6333].

3.3. For Non-web service

For non-web services, as mentioned in Section 2, other means will be needed to inform the users about the service information.

[dns-sd] shows an good example of DNS based solution to do so, in which case an application running in the end user's device will retrieve service information via DNS SRV/TXT records, and list available services. In a scenario where such application is not applicable, following provides another means for a third party, e.g. DDNS service provider, to disclose services to the Internet users.

A web portal can be used to list available services. DDNS server maintains a web portal for each user FQDN, which provides a users service links. In the figure below, it assumes websrv.myip.org is a user's FQDN provided by a DDNS service provider.

```
+-------------+    +-------------+    +----------+ Internet +-------+
|DDNS client /|----|DDNS server /|----|DNS server|----------|Visitor|
|  Web Server |    | web portal  |    |          |          |       |
+-------------+    +-------------+    +----------+          +-------+
    |      register       |                 |                    |
    |<------------------> |                 |                    |
    |   websrv.myip.org   |  update DNS     |                    |
    |   100.1.1.2:2000    | <-------------> |                    |
    |                     | websrv.myip.org |                    |
    |                     |   portal's IP   |                    |
    |              +-------------+          |                    |
    |              |update portal|          |                    |
    |              +-------------+          |  DNS resolve for   |
    |                     |                 | <----------------> |
    |                     |                 |  websrv.myip.org   |
    |                     |                 |  get portal's IP   |
    |                     |                 |                    |
    |                     |   visit portal of websrv.myip.org    |
    |                     | <----------------------------------> |
    |                     |                 |                    |
    |                  visit http://100.1.1.2:2000               |
```

```
      | <-------------------------------------------------------> |
```

```
      |                      |                 |                    |
```

Figure 4 Update Web Portal

The DDNS client registers the servers' information to the DDNS server, including public IP address and port obtained via PCP, user's FQDN and other necessary information. The DDNS server also works as portal server, it registers its IP address and user's FQDN to the DNS system, so that visitors can visit the web portal.

DDNS server also maintains a web portal for each user's FQDN, update the portal according to registered information from DDNS client. When a visitor visits websrv.myip.org, DNS query will resolve to portal server's address, and the visitor will see the portal and the available services.

```
+---------------------------------------------------------------+
|                                                               |
|              Portal of websrv.myip.org                        |
|                                                               |
|    Service1: web server                                       |
|    Link:     http://100.1.1.2:2000                            |
|                                                               |
|    Service2: video                                            |
|    Link:     rtsp://100.1.1.2:8080/test.sdp                   |
|                                                               |
|    ......                                                     |
|                                                               |
+---------------------------------------------------------------+
```

Figure 5 An Example of Web Portal

The web portal in the above figure show service links that are available to be accessed. Multiple services is accessible per user's FQDN. Some applications which are not http based can also be supported via this solution. When user click a link, the registered application in the OS will be invoked to handle the link. How this can be achieved is out of the scope of this document.

4. Additional Authors' Addresses

This work is made available also from additional authors' contribution and work.

Xiaohong Huang

Beijing University of Posts and Telecommunications, China
Email: huangxh@bupt.edu.cn

Yan Ma

Beijing University of Posts and Telecommunications, China
Email: mayan@bupt.edu.cn

5. Acknowledgments

Thanks to Stuart Cheshire for bringing up DNS-Based Service Discovery and RFC6281 where covers DNS-based SD scenario and gives a good example of how the application means of solution to address dynamic DNS update, in this case, apple' BTMM, can be achieved.

6. References

6.1. 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.

[RFC6281]

S. Cheshire, et. Al. " Understanding Apple's Back to My Mac (BTMM) Service", June 2011.

[RFC6333]

A. Durand, et. Al. " Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", August 2011.

6.2. Informative References

[I-D.ietf-pcp-base]

D. Wing, et. al. " Port Control Protocol (PCP)", October 2, 2012.

[I-D.cheshire-dnsext-dns-sd]

S. Cheshire, et. al. " DNS-Based Service Discovery ", Dec

9, 2011

7. 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

Qin Zhao
Beijing University of Posts and Telecommunications, China
Email: zhaoqin.bupt@gmail.com

James Huang
Huawei Technologies
Email:james.huang@huawei.com