Network Working Group X. Deng
Internet-Draft
Intended status: Informational M. Boucadair
Expires: December 13, 2014 France Telecom
Q. Zhao
Beijing University of Posts and Telecommunications
J. Huang
C. Zhou
Huawei Technologies
June 11, 2014

Using Port Control Protocol (PCP) to update dynamic DNS
draft-deng-pcp-ddns-06

Abstract

This document focuses on the problems encountered when using dynamic DNS in address sharing contexts (e.g., DS-Lite, NAT64) during IPv6 transition. Both issues and possible solutions are documented in this memo.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

1.1. Problem Statement

Dynamic DNS (DDNS) is a widely deployed service to facilitate hosting servers (e.g., access to a webcam, HTTP server, FTP server, etc.) at customers' premises. There are a number of providers which 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 assigned IP address it automatically sends an update message to the DDNS server. The communication between the DDNS client and the DDNS server is not standardized, varying from one provider to another, although a few standard web-based methods of updating 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

well known port numbers, e.g., port 80 will no longer be available to every web server. It will also require the ability to configure corresponding port forwarding on CGN (Carrier Grade NAT, [RFC6888]) devices, so that incoming communications initiated from Internet can be routed to the appropriate server behind the CGN.

Issues encountered in address sharing are documented in [RFC6269]. This document focuses on the problems encountered when using dynamic DNS in address sharing contexts (e.g., DS-Lite [RFC6333], NAT64 [RFC6146]). Below are listed the main challenges:

Announce and Discover an alternate service port: The DDNS service must be able to maintain an alternative port number instead of the default port number.

Allow for incoming connections: Appropriate means to instantiate port mappings in the address sharing device must be supported.

Detect changes and trigger DDNS updates: 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 (and/ or external port number), the DDNS client must refresh the DNS records otherwise the server won't be reachable from outside. This issue is exacerbated in the DS-Lite context because no public IPv4 address is assigned to the CPE.

1.2. Scope and Goals

This document describes some candidate solutions to resolve the aforementioned issues with a particular focus on DS-Lite. These solutions may also be valid for other address sharing schemes.

This document sketches deployment considerations based on the PCP (Port Control Protocol, [RFC6887]). Note DDNS may be considered as an implementation of the Rendezvous service mentioned in [RFC6887].

Indeed, after creating an explicit mapping for incoming connections using PCP, it is necessary to inform remote hosts about the IP address, protocol, and port number 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 machine hosting a game server 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 [RFC6763] would use DNS Update [RFC2136][RFC3007], etc. 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. An example illustrating how the DDNS server may implement such a service notification functionality if necessary is provided in Section 3.

This document does not specify any protocol extension, but instead it focuses on the elaboration of the problem space and illustrate how existing tools can be re-used to solve the problem for some deployment contexts. Particularly, this document requires no changes to PCP 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 address the forthcoming issues. The current DDNS service providers usually employs a web-based form to maintain DDNS service registration and updates.

Generic deployment considerations for DS-Lite, including B4 remote management and IPv4 connectivity check, can be found in [RFC6908]. This document complements [RFC6908] with deployment considerations related to Rendezvous service maintenance. Additional PCP-related deployment considerations are available at [I-D.boucadair-pcp-deployment-cases].

Solutions relying on DNS-based Service Discovery [RFC6763] or Apple's Back to My Mac (BTMM) Service [RFC6281] are not considered in this document. Moreover, this document does not assume that DDNS service relies on [RFC2136].

IPv4 addresses used in the examples are derived from the IPv4 block reserved for documentation in [RFC6890]. DNS name examples follow [RFC2606].

2. Solution Space

2.1. Locate a Service Port

As listed below, at least two solutions can be used to associate a port number with a service:

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 [RFC2782]. Unfortunately, the majority of browsers do not support this record type.

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

2.2. Create Explicit Mappings for Incoming Connections

PCP is used to install the appropriate mapping(s) in the CGN so that incoming packets can be delivered to the appropriate server.

2.3. Detect Changes

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 several possible ways to address the problems stated in Section 1.1:

1. If the DDNS client is enabled, the host issues periodically (e.g., 60 minutes) 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 accordingly (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., 5 minutes, 30 minutes, 60 minutes). If there is no PCP mapping created by PCP client, 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.

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

Figure 1: Flow Chart

3. Some Deployment Solutions

3.1. Reference Topology

Figure 2 illustrates the topology used for the deployment solutions elaborated in the following sub-sections.

```
   +--------------+   +--------+    +---------+   +--------+   +-------+
   | 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

Figure 2 involves of the following entities:

- Servers: refer to the 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 [RFC6333]. A PCP client together with a DDNS client are running on it. After PCP client establishes a mapping on the AFTR, an end user 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 address and/or port changes to the DDNS server.

- AFTR: Responsible for maintaining mappings between internal IPv4 Address plus port and external IPv4 address plus port [RFC6333].

- DDNS server: Maintains a table that associates 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 announces the updates to DNS servers on behalf of end user. [RFC2136] and [RFC3007] 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: refers to users who want to access services behind an IP address sharing network. They issue standard DNS requests to locate the services, which will lead them to a DDNS server, provided that the requested services have been registered to a DDNS service provider. The DDNS server will then handle the rest in the way as described before.

3.2. For Web Service

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 take into account that external port assigned by AFTR may be any number other than 80, in order to maintain proper mapping between domain names and external IP plus port. By doing such changes, the HTTP request would be redirected to the AFTR which servers the specific end host that are running servers.

Figure 3 depicts how messages are handled in order to be delivered to 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 with 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, 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.

[RFC6763] includes an example of DNS-based solution which allows an application running in the end user's device to retrieve service-related information via DNS SRV/TXT records, and list available services. In a scenario where such application is not applicable, following provides another solution 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 (Fully Qualified Domain Name), which provides users service links. Figure 4 assumes "websrv.example.com" 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.example.com |  update DNS     |                    |
       |   192.0.2.1:2000   | <-------------> |                    |
       |                    |websrv.example.com|                   |
       |                    |   portal's IP   |                    |
       |             +-------------+          |                    |
       |             |update portal|          |                    |
       |             +-------------+          |  DNS resolve for   |
       |                    |                 | <----------------> |
       |                    |                 | websrv.example.com |
       |                    |                 |  get portal's IP   |
       |                    |                 |                    |
       |                    |   visit portal of websrv.example.com |
       |                    | <--------------------------------> |
       |                    |                 |                    |
       |                  visit http://192.0.2.1:2000              |
       | <-------------------------------------------------------->|
       |                    |                 |                    |
```

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 behaves as portal server, it registers its IP address, port number, and user's FQDN to the DNS system, so that visitors can access 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 accesses "websrv.example.com", a DNS query will resolve to portal server's address, port number, and the visitor will see the portal and the available services.

```
     +---------------------------------------------------------------+
     |                                                               |
     |               Portal: websrv.example.com                      |
     |                                                               |
     |     Service1: web server                                      |
     |     Link:     http://192.0.2.1:2000                           |
     |                                                               |
     |     Service2: video                                           |
     |     Link:     rtsp://192.0.2.1:8080/test.sdp                  |
     |                                                               |
     |     ......                                                    |
     |                                                               |
     +---------------------------------------------------------------+
```

Figure 5: An Example of Web Portal

As shown in Figure 5, the web portal shows the service URLs that are available to be accessed. Multiple services are accessible per user's FQDN.

Some applications which are not HTTP-based can also be delivered using this solution. When a user clicks on a link, the registered application in the client OS will be invoked to handle the link. How this can be achieved is out of the scope of this document.

4. Security Considerations

This document does not introduce a new protocol nor specify protocol extensions. Security-related considerations related to PCP [RFC6887] and DS-Lite [RFC6333] should be taken into account.

The protocol between the DDNS client and DDNS server is proprietary in most cases, some extensions may be necessary, which is up to DDNS operators. These operators should enforce security-related policies to avoid that illegitimate users alter records installed by legitimate users or install fake records that would lead to attract illegitimate traffic. Means to protect the DDNS server against DoS (Denial of Service) should be enabled. Note these considerations are not specific to address sharing contexts but are valid for DDNS service in general.

5. IANA Considerations

This document does not require any action from IANA.

6. Contributors

The following individuals contributed text to the document:

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

7. Acknowledgements

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

Many thanks to D. Wing, D. Thaler, and J. Abley for their comments.

8. References

8.1. Normative References

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, August 2011.

[RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, April 2013.

8.2. Informative References

[I-D.boucadair-pcp-deployment-cases]
Boucadair, M., "Port Control Protocol (PCP) Deployment Models", draft-boucadair-pcp-deployment-cases-02 (work in progress), April 2014.

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2606] Eastlake, D. and A. Panitz, "Reserved Top Level DNS Names", BCP 32, RFC 2606, June 1999.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", RFC 6269, June 2011.

[RFC6281] Cheshire, S., Zhu, Z., Wakikawa, R., and L. Zhang, "Understanding Apple's Back to My Mac (BTMM) Service", RFC 6281, June 2011.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

[RFC6888] Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Requirements for Carrier-Grade NATs (CGNs)", BCP 127, RFC 6888, April 2013.

[RFC6890] Cotton, M., Vegoda, L., Bonica, R., and B. Haberman, "Special-Purpose IP Address Registries", BCP 153, RFC 6890, April 2013.

[RFC6908] Lee, Y., Maglione, R., Williams, C., Jacquenet, C., and M. Boucadair, "Deployment Considerations for Dual-Stack Lite", RFC 6908, March 2013.

Authors' Addresses

Xiaohong Deng

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
China

Email: james.huang@huawei.com

Cathy Zhou
Huawei Technologies
China

Email: cathy.zhou@huawei.com