Network Working Group
Internet-Draft
Intended status: Experimental
Expires: August 7, 2016

M. Rosenau

February 4, 2016

IPv4-to-IPv6 translation mechanism with DynDNS
draft-rosenau-dyndns-nat46-00

Abstract

Many devices in private homes can be controlled via Web browser from another computer in the internet. This assumes that the IP address of the device is known and that the private internet access has a public IP address at all.

Due to the IPv4 address shortage many internet providers only provide IPv6 internet access while many internet accesses (and therefore Web browsers) are IPv4-only.

This document describes a method that allows an internet service provider that also provides dynamic DNS to the customers to allow accessing IPv6-only devices from IPv4-only Web browsers.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 7, 2016.

1. Introduction

There are many devices in private homes which can be controlled over the internet. Smart heating installation is one example for this.

In the past users operating such devices used a "dynamic DNS" service because the IPv4 address of the internet access was changing every day. The home router was configured to perform a "port forwarding" so incoming TCP connections on a certain port were forwarded to the device.

Using IPv6 the port forwarding is no longer needed because each device has its own IPv6 address but the "dynamic DNS" service is still required because the IPv6 address prefix of most internet accesses is still changing daily (often for privacy reasons).

Because of the shortage of IPv4 addresses many internet accesses only have a public IPv6 address range and no public IPv4 address while there are still a lot of internet accesses that are IPv4-only. If the internet access at home is IPv6-only and the web browser is connected to an IPv4-only internet access then it is not possible to access the device at home using this web browser.

Some providers of DS-Lite [RFC6333] try to use special protocols that allow customers to forward certain ports to their devices. However this has one major drawback: Because the number of IPv4 addresses of the provider is limited only a limited number of customers can forward a certain port number (such as 80 for HTTP) to their device.

This document describes a method which bases on a NAT46 (IPv4 to IPv6 translation) operated by the internet service provider which does not have such limitations. However this method is limited to certain protocols (for example HTTP and TLS).

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP

14, RFC 2119 [RFC2119] and indicate requirement levels for compliant implementations.

3. System description

3.1. Dynamic domain name service

An essential part of the system is the dynamic domain name service.

The internet service provider provides a dynamic domain name service to the customers. As the customers have IPv6-only internet access they only provide AAAA entries. Example:

```
heater.customer1.example.com AAAA 2001:DB8:1::1234
heater.customer2.example.com AAAA 2001:DB8:2::5678
coffeemachine.customer2.example.com AAAA 2001:DB8:2::9ABC
```

Figure 1: Customer addresses

Let's say the providers AFTR or NAT46 router has the IPv4 address 192.0.2.1. Then the provider adds the DNS entries for the IPv4 addresses: All host names have the IPv4 address of the NAT46 router or AFTR:

```
heater.customer1.example.com IN A 192.0.2.1
heater.customer2.example.com IN A 192.0.2.1
coffeemachine.customer2.example.com IN A 192.0.2.1
```

Figure 2: IPv4 addresses

3.2. Access via IPv6

Since the customers have full IPv6 internet access the devices at home can be accessed directly when the web browser uses IPv6. No NAT46 (IPv4->IPv6) translation is necessary.

3.3. Access via IPv4 - HTTP based

The NAT46 or AFTR is listening on ports 80, 1080 and 8080 which are typically used for HTTP-based connections.

When there is an incoming connection the NAT46/AFTR first receives the HTTP header from the host that initiated the connection.

The NAT46/AFTR evaluates the "Host:" line. Depending on the "Host:" line it creates a connection to the destination host desired, sends the entire HTTP header received to that host and creates a 1:1 NAT connection between the source and the destination host.

In the following example "IPv4" is the IPv4-only host the web browser runs on, "NAT" is the NAT46 or AFTR operated by the internet service provider and "IPv6" is the IPv6-only web server (which may be a device like a smart heater installation):

```
IPv4 -> NAT:   GET /example.file HTTP/1.1<CRLF>
IPv4 -> NAT:   Information: Hello world<CRLF>
IPv4 -> NAT:   Host: heater.customer2.example.com<CR>
IPv4 -> NAT:   (more data received)
-- Now the NAT establishes a connection to the IPv6 host
-- heater.customer2.example.com
NAT -> IPv6:   GET /example.file HTTP/1.1<CRLF>
NAT -> IPv6:   Information: Hello world<CRLF>
NAT -> IPv6:   Host: heater.customer2.example.com<CR>
NAT -> IPv6:   (more data received)
-- Now a 1:1 connection IPv4 <--> IPv6 is established
-- by the NAT.
```

Figure 3: HTTP-Based connection

Note that in this scenario the NAT does not evaluate any other lines but the "Host:" line. It does also not evaluate any responses from the IPv6 host.

When the host name is not known, the IPv6 host refuses the TCP connection or there is no "Host:" line in the HTTP header the NAT sends a response itself:

```
IPv4 -> NAT:   GET /example.file HTTP/1.1<CRLF>
IPv4 -> NAT:   Information: Hello world<CRLF>
IPv4 -> NAT:   Host: heater.customer2.nonexisting.example<CR>
IPv4 -> NAT:   (more data received)
-- Now the NAT tries to establish a connection to the IPv6 host
-- heater.customer2.nonexisting.example
NAT -> IPv4:   HTTP/1.1 502 Unknown host name<SP>
NAT -> IPv4:   heater.customer2.nonexisting.example<CRLFCRLF>
-- Connection is closed by the NAT
```

Figure 4: HTTP-Based connection: Host unreachable

3.4. Access via IPv4 - TLS based

The NAT46 or AFTR is also listening on ports used for protocols that use TLS (443, 563, 565, 636, 989, 990, 992, 993, 995).

Instead of evaluating the "Host:" line in the HTTP request it evaluates the server name extension in the "client hello" packet sent by the TLS client.

In the case of an error (server not available) the NAT sends an "unrecognized_name" error code back to the client.

As for HTTP connections the NAT does not evaluate any other fields of the "client hello" packet but it simply forwards it to the desired TLS server.

4. References

4.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

4.2. Informational References

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", RFC 6333, DOI 10.17487/RFC6333, August 2011, <http://www.rfc-editor.org/info/rfc6333>.

Author's Address

Martin D. J. Rosenau

Email: martin@rosenau-ka.de