IPv6 Rapid Deployment in Taiwan Academic Network (TANet)

Po-Kang CHEN, Chia-Wen LU, Quincy WU

Department of Computer Science and Information Engineering, National Chi Nan University, Taiwan

{s100321526, s99321515, solomon}@ncnu.edu.tw

Abstract— **After the Internet Assigned Numbers Authority (IANA) allocated all the remaining IPv4 address blocks to Regional Internet Registries in February 2011, IPv6 became mandatory to build new Internet networks and services. However, IPv6 networking environment is still not widely constructed and it is conceivably impossible to move from IPv4 to IPv6 with a single stride. Therefore, IPv4/IPv6 transition mechanisms receive great attention since the beginning of IPv6 deployment. Tunneling is one of the transition mechanisms, among which 6to4 tunneling is a popular tunneling mechanism supported by numerous operating systems like Linux, FreeBSD, and Windows. Although theoretically 6to4 is an elegant protocol, there are some limitations that prevent Internet service providers (ISPs) to offer public 6to4 services. To overcome these problems, IPv6 Rapid Deployment (6RD) was proposed in 2007 as an improvement over 6to4 Tunnel.**

This paper illustrates how to deploy 6RD's Border Relay (BR) and Customer Edge (CE) in Taiwan Academic Network (TANet), so that users in IPv6 islands can communicate with the IPv6 Internet via 6RD Tunnels.

Keywords— **6RD, 6to4, IPv6, IPv6 Rapid Deployment, Tunnel**

I. INTRODUCTION

Because of the IPv4 address exhaustion, the Internet Protocol version 6 (IPv6) had been designed. It targets at sufficient IP addresses to ease Internet access. To facilitate moving the Internet environment from IPv4 to IPv6, various transition mechanisms were proposed. According to the suggestions by Internet Engineering Task Force (IETF) [1], the transition mechanisms include three major categories:

A. Dual-stack

The device supports both IPv4 and IPv6 in software approaches. It is thus unnecessary to spend additional hardware cost on dedicated IPv6 devices.

B. Tunneling

If two IPv6 networks were not connected directly, tunnels can encapsulate IPv6 packets into IPv4 headers, and delivery the encapsulated packets to destinations via the existing IPv4 infrastructure.

C. Translation

It can be expected that many years later, after IPv6 is extensively spread, there may be some devices that only support IPv6, while IPv4 protocol stacks are eliminated on them to reduce the production costs. These new devices cannot reach old devices which only support IPv4. At that time the two networks (IPv4 and IPv6) will need a translator to translate IPv4 packets to IPv6, and vice versa.

When the Internet Assigned Numbers Authority (IANA) allocated all the remaining IPv4 address blocks in February 2011[2], it can be foreseen that lots of devices will not obtain IPv4 addresses in the future. In other words, there are more and more devices which must use pure IPv6 to communicate with the Internet. The tunneling mechanism is the most appropriate transition mechanism for this situation – when there are many IPv6 islands surrounded by an IPv4 ocean.

There are many different tunneling approaches, such as 6to4 tunnel [3], ISATAP [4], Teredo [5], etc. In Taiwan, 6to4 tunneling mechanism has been widely adopted. It is the default IPv6 tunnel mechanism in Windows operating systems, so it serves as a convenient automatic tunneling mechanism. However, from the practical operating experience of ISPs, it brings some disadvantages. First, using 6to4 Tunnel prefix makes ISPs difficult to control packets flowing from their customers. Second, because public IP addresses are required, the 6to4 tunnel could not traverse NATs. To overcome these problems, a new tunneling mechanism *IPv6 Rapid Deployment (6RD)* [6] [7] was proposed in 2007 as an improvement over 6to4 Tunnel.

In France, FREE [8] provides the service of 6RD for its customers. In the US, the Comcast Corporation [9] also had a trial for testing 6RD [10]. The remaining sections of this paper will illustrate how we implement 6RD in Taiwan Academic Network (TANet) and share our implementation experience to anyone who is also interested in 6RD.

II. RELATED WORKS (BACKGROUND)

A. 6to4 Features

To appreciate the advantage of 6RD, one must understand the 6to4 tunneling mechanism and related operating issues. The 6to4 Tunnel specifies the IPv6 address of a host to have a common IPv6 prefix (2002::/16), followed by the 32-bits public IPv4 address of the 6to4 host. For example, if a host 192.0.2.1 wants to construct a 6to4 tunnel, it will gain a 6to4 address which starts with 2002:C000:201::/48.

In a 6to4 environment, 6to4 hosts can communicate with each other via 6to4 routers as shown in Figure 1.

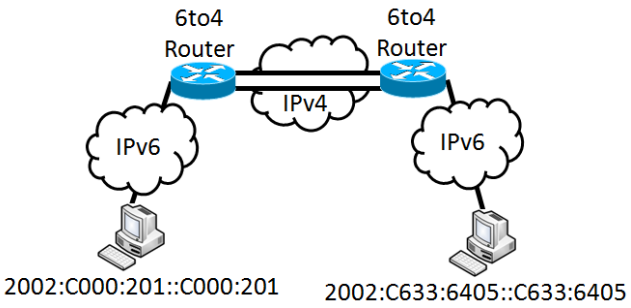

Figure 1. 6to4 communication architecture.

In another case, as shown in Figure 2, if a 6to4 host is going to communicate with a native IPv6 host, they need the assistance of a 6to4 relay router. In order to allow 6to4 hosts to find 6to4 relay routers easily, an IPv4 anycast address 192.88.99.1 is assigned to 6to4 relay routers [11].

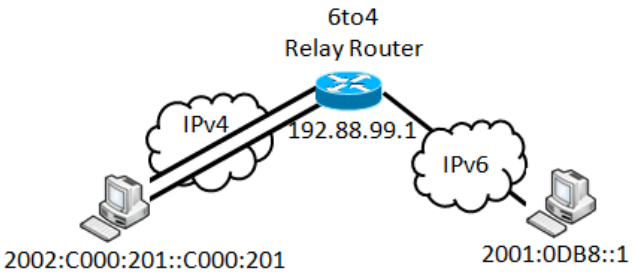

Figure 2. 6to4 host to IPv6 host architecture.

Unfortunately, this convenient feature is not favored by commercial ISPs.

First, if an ISP builds a 6to4 relay router and starts advertising the prefix 2002::/16, this provides open services to all 6to4 hosts, no matter the hosts belong to their own customers or customers of other ISPs. This makes ISPs difficult to control the packets flow. If one ISP tries to filter 6to4 packets which do not come from its customers, the relay router become a black hole to other users. This would break the connectivity of the 6to4 mechanism.

In Figure 3, it shows a regular schema. There is a 6to4 host "Host H1", which is a customer of ISP A. The IPv4 network routes 6to4 tunneling packets of "Host H1" to the relay router "Router R" which is operated by ISP A. The relay router decapsulates the packets and forwards them to the destination in a IPv6 network. When the IPv6 host (Host H2) sends some packets back to "Host H1" with the destination IPv6 address start with 2002::/16. The packets will be routed back to the relay router, encapsulated, and finally reach the "Host H1" without any problem.

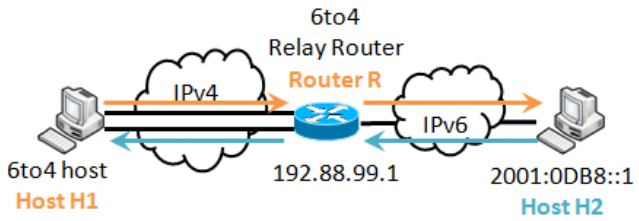

Figure 3. A normal 6to4 tunneling traffic flow.

However, suppose ISP A decided not to serve users all over the world, it may add some rules in its relay router to filter incoming packets. As shown in Figure 4, a 6to4 host "Host H3" belonging to a customer of another ISP B, is near a relay router "Router R" of ISP A. The traffic flows from H3 to the destination; this works fine. When the host H2 in the IPv6 network wants to send responses back to H3, there will be some troubles.

The relay router is advertising a IPv6 prefix 2002::/16. As a result, the packets back from H2 will be faithfully routed to Router R. When the packets go through the relay router R, unfortunately, the relay just drops the packets because ISP A configures the relay router to filter out the packets not belonging to its customers. Therefore, the traffics from the IPv6 network will never reach H2.

According to the routing mechanism, every packets from the IPv6 network to a host with the prefix 2002::/16 near the relay R will be sent to R, but R drops all packets not belonging to its customers. Therefore, relay R becomes a black hole. It absorbs the traffic nearby but do not forward them.

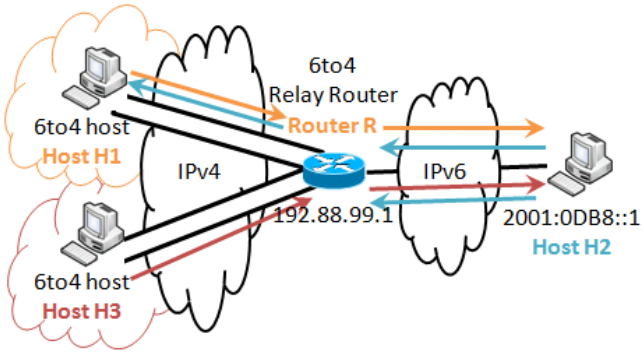

Figure 4. 6to4 Relay Black Hole.

Moreover, it is required that the IPv4 addresses of 6to4 hosts must be public. This implies that the 6to4 tunnel does not work behind NATs. Since NATs are widely deployed in many scenarios, this imposes an unpractical limitation for 6to4 tunneling mechanism.

B. 6RD Features

As an improvement to 6to4, the 6RD architecture (See Figure 5) proposes to connect 6RD hosts to a customized router.

The philosophy of 6RD is using the IPv6 prefix of an ISP (e.g. 2001:288::/32), instead of a common prefix

2002::/16 for all tunnel users. Take Comcast as an example, the IPv6 prefix is 2001:55c::/32. The border router will advertise this prefix to the IPv6 Internet. There should not be any problem for the Internet to route packets back to the tunnel users.

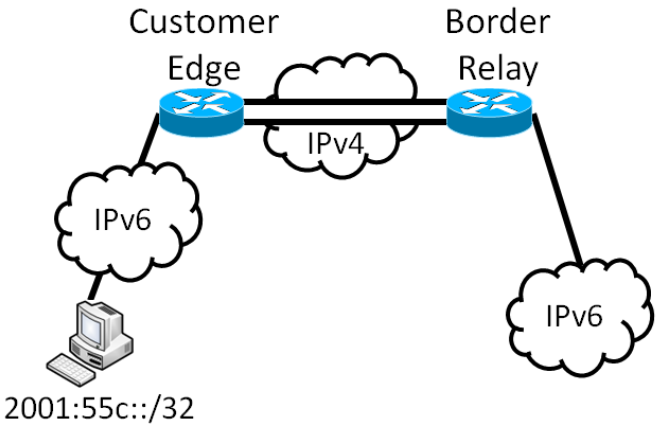

Figure 5. 6RD architecture.

In 6RD architecture, only the routers (Border Relay) need a public IPv4 address, so even if customers were assigned private IPv4 addresses from the ISP, this would not hinder the connectivity of 6RD tunnels. Users can build 6RD tunnels with Border Relays using private IPv4 addresses, so the scale will not be bounded by the number of public IPv4 addresses owned by the ISP. Table 1 shows the comparison between 6RD and 6to4.

TABLE 1. 6RD AND 6TO4 COMPARISON

	6to4	6RD
Prefix	2002::/16	Same as ISP
Scale	Bounded	Unbounded
NAT	Not Allowed	Allow

III. IMPLEMENTATION

The implementation of 6RD can be divided into two parts. In the first part we only focused on the Customer Edge (CE) configuration. After CE is up, we went into the second part, the most important part in 6RD, to build the Border Relay (BR). The following subsections illustrate how we set up the environment in Taiwan Academic Network (TANet).

A. Architecture

Figure 6 shows the architecture for the implementation. We have an IPv4 only CE. Behind the CE is a 6RD host with no IPv4 address (it is a pure IPv6 host which only receives a 6RD tunneling address assigned from the CE). The BR is a dual-stack router, which communicates to the CE through the internal IPv4 network and forwards the tunneling packets in and out. In this architecture, the 6RD hosts can connect to the IPv6 network without any problems. The test environment is deployed in National Chi Nan University (NCNU).

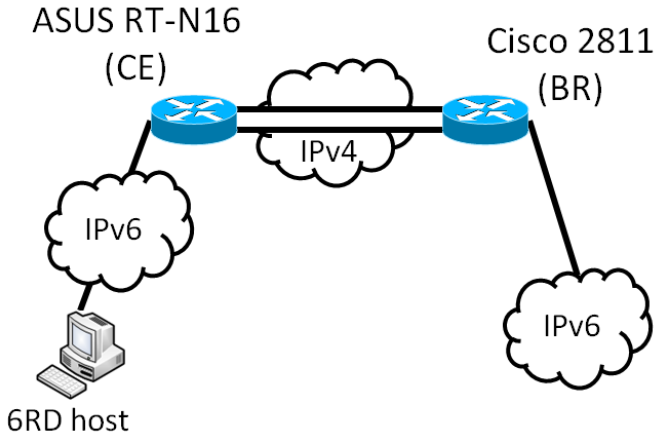

Figure 6. Implementation Architecture

B. 6RD Customer Edge

We adopt an off-the-shelf home router (ASUS RT-N16) as the CE, upgrading the firmware downloaded from the DD-WRT website [12] to support 6RD. Thanks for the Comcast testing 6RD trial, the sample configurations can be easily obtained from the Comcast Corporation. After setting some necessary parameters (6RD prefix to 2001:55c::/32, 6RD BR FQDN, IPv4 mask length as 0), 6RD hosts under our CE could connect to the Internet through the 6RD BR via a tunneling IPv6 address.

However, with a BR located in the US, a packet always need to travel across the Pacific Ocean from Taiwan to America before it arrives at the destination. Therefore, the next step is to build a BR within TANet to shorten the packets delivery delay.

C. 6RD Border Relay

A Cisco 2811 router was chosen to serve as the BR. We upgraded the IOS to version 15.1(3)T1 with 6RD support. We followed the Cisco online document instructions and examples [13] [14] to configure the router. Unfortunately we encountered some unknown problems so that there is no 6RD traffic between our CE and BR. This issue is under investigation by Cisco engineers. As soon as we overcome the problem, the 6RD implementation in TANet will be completed.

IV. FUTURE WORK

A. Security Issue

As RFC 6324 mentioned, there exists vulnerabilities in all IPv6-in-IPv4 automatic tunnels which may cause a loop between the protocol-41 based automatic tunnels [15]. Unfortunately, 6RD is in the list. RFC 6324 had proposed some mitigation measures. Any public 6RD service should implement countermeasures to loop attacks in order to provide a reliable service.

B. Traffic Measuring and Analyzing

Every system should be monitored and analyzed by its utilization, especially an important service. 6RD is a

remarkable mechanism for IPv4/IPv6 transition. The more data we collect, the better we can understand about its behavior, which can help us to constantly improve the protocols.

ACKNOWLE-DGMENT

This work is partly supported by National Science Council in Taiwan under grants NSC 100-2218-E-029 -001.

REFERENCE

[1] E. Nordmark and R. Gilligan, "*Basic transition mechanisms for IPv6 hosts and routers*", IETF RFC 4213, Oct. 2005.
[2] (2011) G. Huston, "*IPv4 address report*." . [online] Available at: http://www.potaroo.net/tools/ipv4/index.html.
[3] B. Carpenter, "*Connection of IPv6 Domains via IPv4 Clouds*", IETF RFC 3056, Feb. 2001.
[4] F. Templin, T. Gleeson, D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", IETF RFC 5214, Mar. 2008.
[5] C. Huitema, "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", IETF RFC 4380, Feb. 2006.
[6] R. Despres, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", IETF RFC 5569, Jan. 2010.
[7] W. Townsley, O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", IETF RFC 5969, Aug. 2010.
[8] (2011) French Internet service provider website. [online] Available at: http://www.free.fr/.
[9] (2011) Comcast Corporation website. [online] Available at: http://www.comcast.com/.
[10] (2011) Comcast 6RD Configuration Instructions for IPv6. [online] Available at: http://www.comcast6.net/6rd-config.php
[11] C. Huitema, "An Anycast Prefix for 6to4 Relay Routers", IETF RFC 3068, Jun. 2001.
[12] (2011) dd-wrt website. [online] Available at: http://www.dd-wrt.com/.
[13] (2011) Implementing Tunneling for IPv6. [online] Available at: http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-tunnel_xe.html.
[14] (2011) 6rd Configuration Example. [online] Available at: http://docwiki.cisco.com/wiki/6rd_Configuration_Example.
[15] G. Nakibly, F. Templin, "Routing Loop Attack Using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations", IETF RFC 6324, Aug. 2011.
.