Deploying Internet Protocol version 6 (IPv6) over Internet Protocol version 4 (IPv4) tunnel

Conference Paper · February 2002

DOI: 10.1109/SCORED.2002.1033069 · Source: IEEE Xplore

5 authors, including:

Mahmoud Mazhar Samad
Glasgow Caledonian University
7 PUBLICATIONS **21** CITATIONS
SEE PROFILE

Fazuliana Yusuf
Universiti Utara Malaysia
2 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Habibah Hashim
Universiti Teknologi MARA
112 PUBLICATIONS **606** CITATIONS
SEE PROFILE

Md Mahfudz Md Zan
Universiti Teknologi MARA
7 PUBLICATIONS **27** CITATIONS
SEE PROFILE

Deploying Internet Protocol Version 6 (IPv6) Over Internet Protocol Version 4 (IPv4) Tunnel

M. Samad, F.Yusuf, Habibah Hashim and Md Mahfudz Md Zan

Fakulti Kejuruteraan Elektrik
Universiti Teknologi MARA (UiTM)
Shah Alam, Selangor Darul Ehsan, Malaysia
E-mail: mustaffa@elect.itm.edu.my

Abstract - Internet Protocol version 6 (IPv6) or IP Next Generation is the protocol that has been designed to replace the existing Internet Protocol version 4 (IPv4). These two protocols are expected to coexist for a number of years during the transition period. A number of IPv4-to-IPv6 transition tools are available to address the various needs of different networks. The two most basic transition tools available are the hybrid stack mechanism and tunneling.

A hybrid or dual stack host, implements both IPv4 and IPv6, usually in a single stack in which most of the code is shared by the two protocols. Tunneling is the encapsulation of IPv6 traffic within IPv4 packets so they can be sent over an IPv4 infrastructure, allowing IPv6 hosts and routers to communicate without the need to upgrade the IPv4 infrastructure that exists between them. This paper looks at how tunneling can be performed over existing internetwork infrastructure.

Keywords: Internet Protocol, IPv6, IPv4, Transition Tools, Tunneling, Encapsulation.

1. INTRODUCTION

Internet Protocol version 6 (IPv6) or IP Next Generation is the protocol that has been designed to replace the existing Internet Protocol version 4 (IPv4). For more than twenty years, IPv4 has been widely used in Internet activities around the world. IPv6 is expected to gradually replace IPv4 over the next few years. While these gradual changes are taking place, these two protocols are expected to coexist for a number of years during this transition period.

To facilitate this, a number of IPv4-to-IPv6 transition tools are available to address the various needs of different networks. The two most basic IPv4-to-IPv6 transition tools available are the hybrid or dual stack mechanism and IPv6 over IPv4 tunneling.

It started as early as July 1991, when the Internet Engineering Task Force (IETF) began the process of researching the problem, soliciting proposals for solutions, and narrowing in on a conclusion, describing this preliminary process in RFC 1380 [1], published in November 1992. In addition, a new research area, called the Internet Protocol Next Generation, or IPng, Area, was commissioned by the IETF to formally study these issues.

In December 1993, RFC 1550 [2] was distributed, titled "IP: Next Generation (IPng) White Paper Solicitation". This RFC invited any interested party to submit comments regarding any specific requirements for the IPng or any key factors that should be considered during the IPng selection process.

In January 1995, RFC 1752 [3], "The Recommendation for the IP Next Generation Protocol," described four key transition criteria.

The first is incremental upgrade, which allow existing IPv4 hosts to be upgraded at any time without depending on other hosts or routers to be upgraded. The second is incremental deployment, where new IPv6 hosts and routers can be installed at any time without any prerequisites.

The third is easy addressing, which allow existing IPv4 hosts or routers that are upgraded to IPv6, to continue using their existing address, without needing new assigned addresses.

The last of these four criteria is low start-up costs, where little or no preparation work is needed in order to upgrade existing IPv4 systems to IPv6, or to deploy new IPv6 systems.

In April 1996, RFC 1933 [4] titled "Transition Mechanisms for IPv6 Hosts and Routers" described two transition mechanisms, a dual IP layer (stack) and IPv6 over IPv4 tunneling. This paper looks at how these transition mechanisms for IPv6 hosts and routers can be implemented, and the experience of connecting to Malaysian Advanced Network Integrated System (MANIS) Tunnel Broker and configured tunnel.

0-7803-7565-3/02/$17.00 ©2002 IEEE.

2. TRANSITION MECHANISMS

The IETF NGTrans (Next Generation Transition) working group has designed a set of IPv4-to-IPv6 transition tools to address the various needs of different networks [5]. The transition mechanisms provide the ways and means of implementing a transition strategy. The three main mechanisms include dual stack mechanism, IPv6-over-IPv4 tunneling and translation. The two most basic IPv4-to-IPv6 transition tools are the dual stack mechanism and tunneling.

The tunneling mechanisms include using manually configured tunnels, generic routing encapsulation (GRE) tunnels, semi-automatic tunnel mechanisms such as tunnel broker services, and fully automatic tunnel mechanisms. The scope of this study is confined to configured tunneling and tunnel broker. The tunnel broker technique requires a dual stack host at the client's end to be connected to the tunnel broker's facilities.

2.1 Dual Stack Mechanism

A dual stack host, implements both IPv4 and IPv6, usually in a single stack in which most of the code is shared by the two protocols [5]. The host supports both IPv4 and IPv6 stacks, known as IPv6/IPv4 nodes [6]. These nodes have the ability to send and receive both IPv4 and IPv6 packets, communicating IPv4 with IPv4 peers, and IPv6 with IPv6 peers.

When both options are available, the host will usually choose the IPv6 path, which increases the value and power of the IPv6 network by creating more users. Figure 1 illustrates the Dual Stack Mechanism.

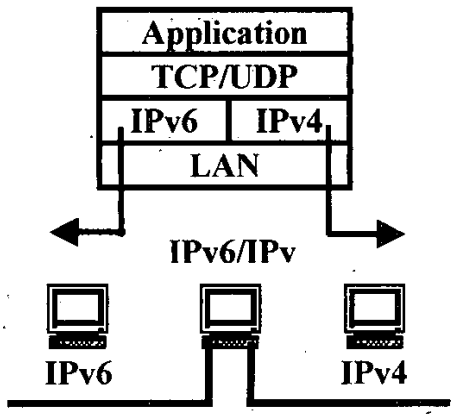

Fig. 1. Dual Stack Mechanism

2.2 Tunneling Mechanism

Tunneling is a process whereby information from one protocol is encapsulated inside the frame or packet of another architecture, thus enabling the original data to be carried over that second architecture [8]. The tunneling mechanism for IPv6/IPv4 is designed to enable an existing IPv4 infrastructure to carry IPv6 packets by encapsulating the IPv6 information inside IPv4 datagrams. Tunneling provides a convenient way for an IPv6 island to connect to other IPv6 islands across an ocean of IPv4 networks [5]. The IETF has drafted several tunneling tools including Configured Tunneling, Automatic Tunneling, Tunnel Broker, 6over4, 6to4, and ISATAP.

The encapsulation process will place the IPv6 information inside IPv4 packets. The dual stack host or router will encapsulate or wrap the IPv6 packet into IPv4 and transmit them over the IPv4 network (tunnel). Figure 2 shows how an IPv6 packet can be encapsulated with-in the payload of an IPv4 packet.

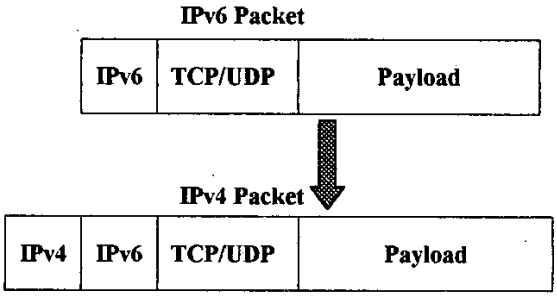

Fig. 2. Encapsulating IPv6 in IPv4

At the receiving end, the dual stack host or router will then decapsulate or unwrap the IPv6 packet from the IPv4 packets. Figure 3 shows how an IPv6 packet can be decapsulated from the IPv4 packet.

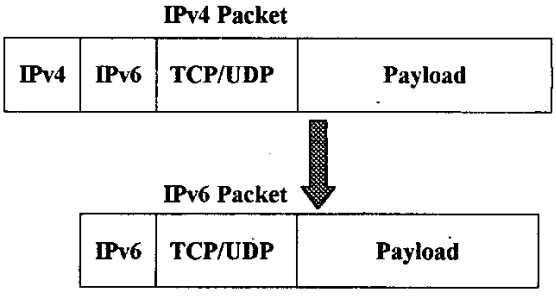

Fig. 3. Decapsulating IPv6 from IPv4

A configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 infrastructure. The main function is for stable connections that require regular secure communication between two dual stack routers or between an end system and a dual stack router, or for connection to remote IPv6 networks such as the 6bone. The routers and end systems, if they are at the end of the tunnel, must be dual-stack implementations. Figure 4 illustrates the tunneling mechanism.

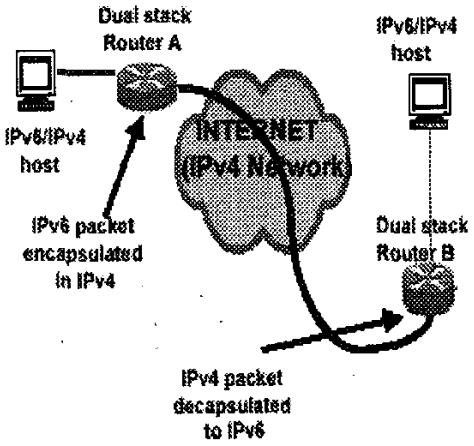

Fig. 4. Tunneling Mechanism.
Courtesy of IPv6 Group (MANIS)

At each end of the tunnel, the IPv4 and IPv6 addresses of the dual-stack router on the tunnel interface are configured, and the source and destination points are identified using IPv4 addresses. Since each tunnel exists between only two routers, adding routers means adding tunnels to cater for all the paths between the routers.

3. CONNECTING TO MANIS NETWORK

The Malaysian Advanced Network Integrated System (MANIS) network is an IPv6 research network, set up to promote IPv6 usage in Malaysia by providing IPv6-over-IPv4 tunnels to interested organizations [6]. The main components of MANIS are IPv6 Router, DNS Server, Web Server, Mail Server and Tunnel Broker. MANIS network provides IPv6 backbone connectivity and is currently connected to more than ten international connections as well at least three local connections [6].

In this study, the two types of IPv6 connections made to MANIS network were the dual stack host to MANIS Tunnel Broker, and dual stack router to MANIS IPv6 router. With these connections to the Tunnel Broker and MANIS router, the dual stack host and router can then be linked to the 6bone network, an experimental network running in parallel with the Internet.

3.1 Tunneling and Dual Stack Router

Fig. 5 illustrates the connection made to MANIS IPv6 router through the IPv6 over IPv4 tunnel. OpenBSD Operating System (OS) was used in the dual stack router as it supports IPv6 and supported by MANIS.

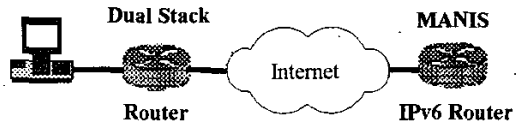

Fig.5 Setting up Dual Stack Router

The dual stack router was then configured. Once the dual stack router has been configured, the tunnel (link) was tested for connectivity and reliability. One of the tests conducted was to "ping" the manis server. Figure 6 shows the result of "pinging" Manis.

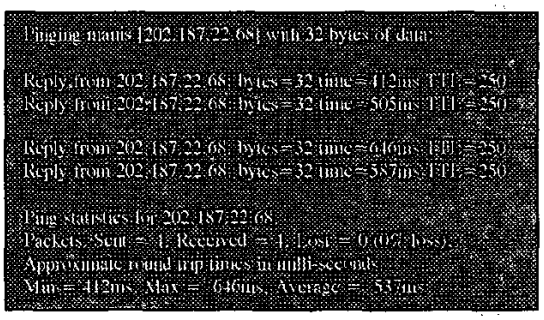

Fig. 6. Ping Statistics for Manis.

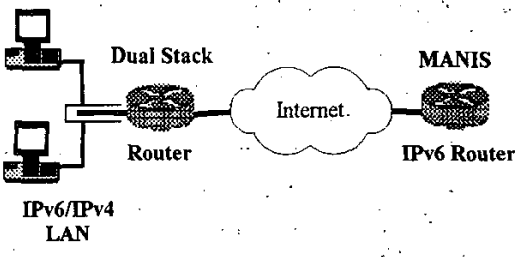

Fig. 7. Connecting Local Area Network to IPv6 Router

An IPv6-and-IPv4 local area network (LAN) test-bed was then set up for the purpose of testing and observing the performance of both IPv6 and IPv4 networks. This was realised using IPv6 and IPv4 capable OS, such as OpenBSD and Windows XP. Figure 7 illustrates the link between the LAN and MANIS IPv6 router, for onward connections to the 6bone network and other (global) IPv6 sites.

3.2 Tunnel Broker

The concept of Tunnel Broker is an alternative approach based on the provision of dedicated servers, called Tunnel Brokers, to automatically manage tunnel requests coming from the users. Idea of Tunnel Broker was first presented at 43rd IETF meeting in December 98 [6]. Two implementations

were demonstrated during the Grenoble IPng & NGtrans interim meeting in February 1999. The Tunnel Broker Internet Draft (April 1999) became the Internet Standard RFC3053 [7] in January 2001. The tunnel broker concept complements the 6over4 approach. This approach was expected to be useful to stimulate the growth of IPv6 interconnected hosts and to allow early IPv6 network providers to provide easy access to their IPv6 networks [7]. The Tunnel Broker fits well for small isolated IPv6 sites, and especially isolated IPv6 hosts on the IPv4 Internet, that requires to be easily connected to an existing IPv6 network. Tunnel brokers can be seen as virtual IPv6 ISPs, providing IPv6 connectivity to users already connected to the IPv4 Internet.

3.3 Tunnel Broker and Dual Stack Host

Figure 8 demonstrates the tunnel broker mechanism. For the purpose of this study, a dual stack host was connected to MANIS Tunnel Broker. OpenBSD OS was used in the dual stack host as it supports IPv6 and supported by MANIS. However the tunnel lifetime is controlled and limited to 30 days only.

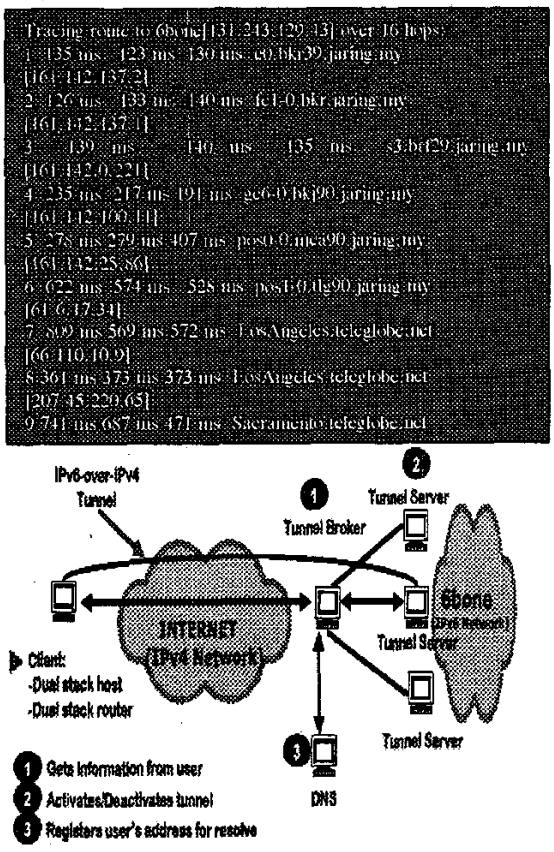

Fig. 8. Tunnel Broker Mechanism
Courtesy of IPv6 Group (MANIS)

Fig. 9. Result of Tracing Route to 6Bone.

Once the tunnel was established, tests were conducted to verify the connectivity and reliability of the link. One of the tests conducted was to trace the route to the 6bone. Figure 9 illustrates the result of this test. The tunnel broker mechanism offers many advantages. It is ready to connect, useful for any isolated user, thus allowing as many users as possible to experiment with IPv6 network. It is also not very costly to run as well as being user friendly, as the tunnel is automatically created between users and Tunnel Broker.

4. SUMMARY

The paper has described the two most basic types of IPv4-to-IPv6 transition tools available, namely the hybrid or dual stack mechanism and IPv6 over IPv4 tunneling. It has also demonstrated the mechanisms of tunneling implemented, utilising dual stack host and Tunnel Broker, and dual stack router connected to MANIS IPv6 network.
Other transition tools include translation. This can be performed at the IP layer, transport layer and application layer. A key part of the IPv6 design is its ability to integrate into and coexist with existing IPv4 networks. Hence the development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the beginning. Transition mechanisms are very important to the successful implementation of IPv6.

5. REFERENCES

[1] P. Gross, and P. Almquist, "IESG Deliberations on Routing and Addressing", RFC 1380, 1992.

[2] S. Bradner, and A. Mankin, "IP: Next Generation (IPng) White Paper Solicitation", RFC 1550, December 1993.

[3] S. Bradner, and A. Mankin, "The Recommendation for the IP Next Generation Protocol", RFC 1752, January 1995.

[4] R. Gilligan, and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 1933, April 1996.

[5] A. Durand, "Deploying IPv6," *IEEE Internet Computing*, Jan-Feb 2001, pp. 79-81.

[6] C. R. Ishak, R. A. Mahmood, S.M.A. Razak, "IPv6 Tunnel Broker Development", 2002.

[7] A. Durand, P. Fasano, I. Guardini, "IPv6 Tunnel Broker", RFC 3053, January 2001.

[8] M. Miller, *Implementing IPv6*, 2nd Edition. M&T Books, CA., 2000.

- Initiate Request for Connection.
- Tunnel Broker (TB) gets user (host) information
- Tunnel Server (TS) gets available IPv6 address
- TS finds available tunnel interface
- TS calculates expiry time
- TS generates script (both for client and TB)
- TS saves user (host) information in database
- TB sends the script to client (host)
- Client (host) downloads the script
- Client (host) runs the script
- Tunnel is established