International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 6 (2017) pp. 894-897
© Research India Publications. http://www.ripublication.com

Analysis and Comparison of Tunneling based IPv6 Transition Mechanisms

Pyung Soo Kim
System Software Solution Lab.,
Department of Electronic Engineering, Korea Polytechnic University,
237 Sangidaehak-ro, Siheung-si, Gyeonggi-do, 429-793, Korea.

ORCID: 000-0002-9589-446X

Abstract

In this paper, a number of tunneling based IPv6 transition mechanisms are surveyed, analyzed and compared. Firstly, the standards development organization to standardize tunneling based IPv6 transition mechanisms is introduced. Secondly, various tunneling based mechanisms are analyzed. Thirdly, these mechanisms are compared from a variety of views.

Keywords: IPv4, IPv6, Transition, Tunneling.

INTRODUCTION

Although IPv4 has been the most dominant internet protocol, the recent exponential growth of Internet-enabled devices, such as smart phones, tablets, laptops, industrial technologies, appliances, and their increasing requirement of IP addresses cannot be fulfilled because of the limited number of IP addresses offered by the IPv4 address space. This has led to the new version of the Internet Protocol (IPv6). IPv6 is considered the most suitable technology for all the emerging Internet-enabled devices, since it spreads the addressing space and offers scalability, flexibility, tested, extended, ubiquitous, open, and end-to-end connectivity[1]-[3].

However, although the transition to IPv6 is inevitable, it seems to take so much time because IPv4 and IPv6 networks are not directly interoperable for long time. Over the last few decades, a number of IPv6 transition mechanisms have been researched for migration to IPv6 from the existing IPv4 based network infrastructure. These IPv6 transition mechanisms can be classified commonly in three different types : dual-stack, tunneling and address translation[4]-[7].

This paper deals with tunneling based IPv6 transition. Tunneling enables IPv6 connectivity across an IPv4 network and vice versa[8]-[10]. Tunneling operations include encapsulation, decapsulation, and tunnel endpoint signaling, with no upper-layer operation required. A number of tunneling based IPv6 transition mechanisms are surveyed, analyzed and compared. Firstly, the standards development organization, IETF Softwares Working Group, is introduced. Secondly, various tunneling based mechanisms are analyzed. Finally, these mechanisms are compared from a variety of views such as deployment time, CPE change, IPv4 continuity, access network, address mapping, end-to-end transparency, scalability, NAT required.

STANDARDS DEVELOPMENT ORGANIZATION FOR TUNNELING BASED IPV6 TRANSITION MECHANISMS

The IETF (Internet Engineering Task Force) is the body that defines standard Internet operating protocols such as TCP/IP. The Internet Engineering Task Force (IETF) is a global community of volunteers that develops standards used billions of times by companies, organizations, and individuals every day around the world, including those that provide a foundation for email, domain names, and the Web. Standards are expressed in the form of Requests for Comments (RFCs).

The Softwires Working Group, called the softwire WG in IETF is just set up to define a standard way to specify the standardization of discovery, control and encapsulation methods for connecting IPv4 networks across IPv6 networks and IPv6 networks across IPv4 networks in a way that will encourage multiple, inter-operable implementations. In computer networking, a softwire protocol is a type of tunneling protocol that creates a virtual “wire” that transparently encapsulates another protocol as if it was an anonymous point-to-point low-level link. Softwires are used for various purposes, one of which is to carry IPv4 traffic over IPv6 and vice versa, in order to support IPv6 transition mechanisms. For various reasons (financial or political), native IPv4 and/or IPv6 transport may not be available in all cases, and there is need to tunnel IPv4 in IPv6 or IPv6 in IPv4 to cross a part of the network which is not IPv4 or IPv6 capable. Configured tunnels or softwires are suited for the inter-networking job. Table 1 shows standards for tunneling transition mechanisms that have been developed in IETF softwire WG[8].

Table 1. IETF standards for tunneling transition mechanisms

Transition Mechanism	Standard	Title
6in4	RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers
6to4	RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
4over6	RFC 5747	4over6 Transit Solution Using IP Encapsulation and MP-BGP Extensions

Public 4over6	RFC 7040	Public IPv4 over IPv6 Access Network
4rd	RFC 7600	IPv4 Residual Deployment via IPv6 - A Stateless Solution (4rd)
CGN	RFC 6264	An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition
Dual-Stack Lite (DS-Lite)	RFC 6333	Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
Lightweight 4over6 (Lw4o6)	RFC 7596	Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture
6rd	RFC 5969	IPv6 Rapid Deployment on IPv4 Infrastructures

ANALYSIS OF TUNNELING BASED TRANSITION MECHANISMS

To minimize any dependencies during the transition, all the routers in the path between two IPv6 nodes do not need to support IPv6. This mechanism is called tunneling. Tunneling is used to achieve heterogeneous traversing. Basically, IPv6 packets are placed inside IPv4 packets, which are routed through the IPv4 routers. Actually, the concept behind tunneling is not new; many people use tunneling daily, but just use it for other reasons. For example, many companies use IPsec or Secure Sockets Layer (SSL) tunnels to secure information when it is being transmitted over an untrusted network. Diverse tunneling mechanisms are available[8]-[10].

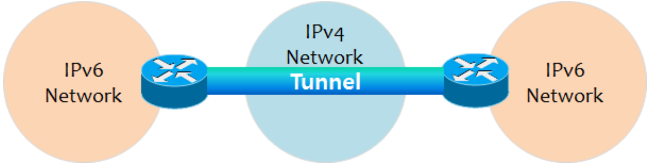

Figure 1. Basic concept of tunneling based transition

A. 6in4

6in4 is an Internet transition mechanism for migrating from Internet Protocol version 4 (IPv4) to IPv6. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links as defined in IETF RFC 4213. The 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP protocol number set to 41. This protocol number is specifically designated for IPv6 encapsulation. In 6in4, the IPv4 packet header is immediately followed by the IPv6 packet being carried. This means that the encapsulation overhead is simply the size of the IPv4 header of 20 bytes. With an Ethernet Maximum Transmission Unit (MTU) of 1500 bytes, one can thus send IPv6 packets of 1480 bytes without fragmentation. 6in4 tunneling is also referred to as proto-41 static because the endpoints are configured statically.

The disadvantage of the 6in4 technology is the higher administrative effort. You must be registered with and login to the tunnel broker. In addition, the tunnel endpoints must be statically configured. Where a dynamic IPv4 address is used, the relevant data must be updated regularly. This can be automated by running a script on a router. 6in4 is a relatively secure and stable technology for providing IPv6 Internet access. This technology is thus suitable for operating web servers that are to be accessed over IPv6. The only drawback is the increased effort in administration. This technology is also suitable for professional use.

B. 6to4

6to4 is an IPv4 tunnel-based transition mechanism defined in IETF RFC 3056. It was designed to allow different IPv6 domains communicate with other IPv6 domains through IPv4 clouds without explicit IPv4 tunnels. 6to4 is used to transfer IPv6 packets over an IPv4 infrastructure, typically the IPv4 Internet. The 6to4 mechanism was created to support coexistence of both versions during the transition to IPv6, which is expected to take years. With 6to4 there is no need to establish the tunnel on the server side, so the only configuration is done on the host side. The 6to4 router (server side) will accept all the 6to4-encapsultated packets coming from any host. A 6in4 router (server side) only accepts 6in4-encapsulated packets of active tunnels.

As consequence, with 6in4 tunnels all the outgoing traffic and incoming traffic follow always the same path between the host and the server side (both ends of the tunnel). However, as illustrated in the figure, with 6to4 the outgoing traffic (from the host point of view) is sent always to the same 6to4 router, but the incoming traffic might be received from different 6to4 router/relays depending on which 6to4 relay is the nearest one to the IPv6 network that the 6to4 host is willing to contact.

C. 4over6

The 4over6 is defined in IETF RFC 5747. This mechanism concerns two aspects: the control plane and the data plane. The control plane needs to address the problem of how to set up an IPv4-over-IPv6 tunnel in an automatic and scalable fashion between a large number of edge routers.

D. Public 4over6

Public 4over6 is providing IPv4 connectivity over a native IPv6-only access network. This mechanism is defined in IETF RFC 7040. It is intended as a mechanism for Internet Service Providers to provide uninterrupted IPv4 services to users, like Internet Content Providers (ICPs), etc., while an operator makes the access network transition to an IPv6-only access network. Public 4over6 is designed to provide IPv4 Internet connectivity over an IPv6 access network using global IPv4 addresses. Future deployments of similar scenarios should use Lightweight 4over6. Public 4over6 follows the Hub and Spoke softwire model and uses an IPv4-in-IPv6 tunnel to forward IPv4 packets over an IPv6 access network.

E. 4rd

IPv4 Residual Deployment (4rd), defined in IETF RFC 7600, is an IPv6 transition mechanism for Internet service providers for deployment of IPv6, while maintaining IPv4 service to customers. 4rd facilitates residual deployment of the IPv4 service across IPv6 networks. Like 6rd, it uses stateless address mappings between IPv6 and IPv4. It supports an extension of IPv4 address based on transport-layer ports. This is a stateless variant of the A+P model. IPv4 Residual Deployment has three main features: mesh topology, shared IPv4 addresses and stateless operation.

F. Carrier Grade NAT (CGN)

Carrier Grade NAT (CGN) is also referred to as the Large Scale NAT (LSN) and defined in IETF RFC 6264. The CGN greatly improves the features of the common NAT including concurrent user capacity, performance, and source tracing. The CGN enables large-scale commercial deployment, resolves IPv4 address exhaustion, and can be deployed in multiple scenarios such as NAT444 and DS-Lite.

CGN is a combined transition mechanism that minimizes the network's structural change that occurs in IPv4 to IPv6 transition. CGN uses both Dual-Stack home gateway and Dual-Stack CGN, which can both be reused during different transition periods. Thus, in this transition period, CGN can be operated through the whole transition solely with upgrades or reboots, without the need to change the device. The early stage of transition uses CGN, which is later replaced by DS-Lite CGN. CGN, having all the NAT's functions and the automatic tunneling characteristics that can be found in 6rd, aids for the recently facing shortage of IPv4 addresses and faster applications of IPv6

G. Dual-Stack Lite(DS-Lite)

As defined in IETF RFC 6333, Dual-Stack Lite (DS-Lite) defines a model for providing IPv4 access over an IPv6 network and aims to better align the costs and benefits of deploying IPv6 in operator's networks. That is, DS-Lite is a technology that enables Internet service providers to move to an IPv6 network while simultaneously handling IPv4 address depletion. IPv4 addresses are becoming depleted; therefore, broadband service providers (DSL, cable, and mobile) need new addresses to support new users. Providing IPv6 addresses alone is often not workable because most of the systems that make up the public Internet are still enabled and support only IPv4, and many users' systems do not yet fully support IPv6.

DS-Lite allows service providers to migrate to an IPv6 access network without changing end-user software. The device that accesses the Internet remains the same, thus allowing IPv4 users to continue accessing IPv4 internet content with minimum disruption to their home networks, while enabling IPv6 users to access IPv6 content.

H. Lightweight 4over6 (Lw4o6)

As defined in IETF RFC 7596, Lightweight 4over6 (Lw4o6) is an optimization of DS-Lite that aims to reduce the NAPT states in the operator's network. The underlying idea of Lw4o6 is to relocate the NAPT function from the Tunnel Concentrator (lwAFTR) to Initiators (lwB4s). The lwB4 element is provisioned with a public IP address and a port set. In this way, the lwAFTR can be transformed into a simple router.

I. 6rd

IPv6 Rapid Deployment(6rd), defined in IETF RFC 5969, is a stateless tunneling mechanism which allows an Service Provider to rapidly deploy IPv6 in a lightweight and secure manner without requiring upgrades to existing IPv4 access network infrastructure. While there are a number of methods for carrying IPv6 over IPv4, 6rd has been particularly successful due to its stateless mode of operation which is lightweight and naturally scalable, resilient, and simple to provision. The service provided by 6rd is production quality, it "Looks smells and feels like native IPv6" to the customer and the Internet at large.

COMPARISON OF TUNNELING BASED TRANSITION MECHANISMS

In this section, tunneling based IPv6 transition mechanisms are classified according to IPv4-IPv6 coexistence scenarios and network configurations as shown in Table 2 and 3, In addition, as shown in Table 4, tunneling based IPv6 transition mechanisms, CGN, DS-Lite, Lw4o6, 6rd, are compared them from a variety of views such as

- Deployment time
- CPE change
- IPv4 continuity
- Access network
- Address mapping
- End-to-end transparency
- Scalability
- NAT required

Table 2. Transition mechanisms according to IPv4-IPv6 coexistence scenarios

IPv4-IPv6 Coexistence Scenario	Mechanism
IPv4 Connectivity	CGN
IPv4 Connectivity over IPv6 Network	DS-Lite, Lw4o6
Rapid IPv6 Deployment	6RD
Wide IPv6 Deployment	*Translation based[7]*

Table 3. Transition mechanisms according to network configurations

Terminal Node	Access Network	Destination Network	Mechanism
IPv4	IPv4	IPv4 Internet	CGN, Dual-stack
IPv4	IPv6	IPv4 Internet	DS-Lite, Lw4o6
IPv6	IPv6	IPv4 Internet	*Translation based[7]*
IPv6	IPv4	IPv6 Internet	6RD
IPv6	IPv6	IPv6 Internet	Dual-stack

Table 4. Comparison of tunneling based transition mechanisms

	CGN	DS-Lite, Lw4o6	6rd
Deployment time	Short-term solution	Long-term solution	Mid-term solution
CPE's change	Not required	Required	Required
IPv4 continuity	Possible	Possible	CGN Optional
Access network	IPv4/IPv6	IPv6	IPv4
Address mapping	Stateful	Stateful	Stateless
Transparency	Limited	Limited	Not limited
Scalability	High	High	Very High
NAT	Required	Required	Not required

CONCLUSION

This paper has focused on tunneling based IPv6 transition. A number of tunneling based IPv6 transition mechanisms have been surveyed, analyzed and compared. Firstly, the standards development organization, IETF Softwares Working Group, has been introduced. Secondly, various tunneling based mechanisms have been analyzed. Finally, these mechanisms have been compared from a variety of views such as deployment time, CPE change, IPv4 continuity, access network, address mapping, end-to-end transparency, scalability, NAT required.

REFERENCES

[1] W. Stallings, "IPv6: The New Internet Protocol", IEEE Communication Magazine, Vol. 34, No. 7, pp. 96~108, 1996.

[2] A. Vallejo, J. Ruiz, J. Abella, A. Zaballos, and J.M. Selga, "State of the Art of IPv6 Conformance and Interoperability Testing", IEEE Communication Magazine, Vol. 45, No. 10, pp. 140~146, 1996.

[3] A. J. Jara, L. Ladid, and A Skarmeta, "The Internet of Everything through IPv6: An analysis of challenges, solutions and opportunities," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 4, no. 3, pp. 97–118, 2013.

[4] P. Wu, Y. Cui, J. Wu, J. Liu, C. Metz, "Transition from IPv4 to IPv6: A State-of-the-Art Survey," IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, 2013, pp. 1407~1424.

[5] S. Savita, Monalisa, "Comparison analysis of various transition mechanism from IPv4 to IPv6," International Journal of Engineering and Computer Science, Vol. 2, No. 6, 2013, pp. 2006~2611.

[6] P. S. Kim, "Comparison and analysis of IPv4/IPv6 transition technologies," Telecommunication Review, vol. 24, no. 3, pp. 419–432, 2014.

[7] P. S. Kim, "Analysis and comparison of address translation based IPv6 transition mechanism," ICIC Express Letters, vol. 9, no. 12, pp. 3162–3170, 2015.

[8] IETF Softwires Working Group, https://datatracker.ietf.org/wg/softwire/documents/

[9] Y. Cui, J. Dong, P. Wu, J. Wu, C. Metz, Y. L. Lee, A. Durand, "Tunnel-Based IPv6 Trasnsition," IEEE Internet Computing, vol. 17, no. 2, pp. 62–68, 2013.

[10] S. Steffann, I. van Beijnum, R. van Rein, "A Comparison of IPv6-over-IPv4 tunnel mechanisms," IETF RFC 7059, November 2013.