Internet Migration and Underlying Security Issues

Yvette E. Gelogo[1] and Sunguk Lee[2*]

[1]*Society of Science and Engineering Research Support, Korea*
vette_mis@yahoo.com

[2]*Research Institute of Industrial Science and Technology*
Pohang, Korea
sunguk@rist.re.kr
**Correspondent Author: Sunguk Lee* (sunguk@rist.re.kr)*

Abstract

Internet Protocol version 6 is a revision of the Internet Protocol (IP) developed by the Internet Engineering Task Force (IETF). IPv6 is intended to succeed IPv4, which is the dominant communications protocol for most Internet traffic as of 2012. IPv6 was developed to deal with the long-anticipated problem of IPv4 running out of addresses. IPv6 implements a new addressing system that allows for far more addresses to be assigned than with IPv4. Transition technologies were developed to support the transition from the IPv4-based Internet to IPv6-based Internet. This paper discusses the transition mechanisms that will allow both traditional IPv4-based Internet end-user sites and new IPv6- only Internet sites to utilize IPv6 and operate successfully over the existing IPv4-based Internet routing infrastructure. This paper also outlines the security issues brought about by the connectivity and interoperability of IPv6 toIPv4 domains.

Keywords: *IPv4, IPv6, Tunneling, Transition, Dual-Stack*

1. Introduction

The current Internet protocol, version 4, known as IPv4, poses several problems such as impending exhaustion of its address space, configuration and complexities due to rapid growth of the Internet and emerging new technologies. As a result, IETF developed the next generation IP, called IPv6, to not only eliminate the shortcomings of IPV4 but also deliver new features and services. IPv4 uses a 32-bit address space, in which can accommodate about 4 billion unique addresses. While that sounds substantial, the practical number of usable addresses is actually much lower. The current Internet has grown much bigger than was anticipated. There are several problems such as impending exhaustion of the IPv4 address space, configuration and complexities and poor security at the IP level [1].

It will use a 128-bit address space. In the other hand, it would support unique addresses well beyond the trillions. It can support 340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456 unique addresses. It will not only eliminate the shortcomings of IPv4, but also unlock new features and services [1].

When IPv6 becomes widely deployed on the Internet, a number of different communication scenarios between IPv6 and IPv4 nodes will exist. It is important to

ensure that such scenarios will work in a manner that is seamless to users and requires minimal effort by operators. Otherwise, deployment will seem cumbersome and will be delayed. Mobility will add a new dimension to the deployment problems and therefore should be carefully considered. While we cannot be certain about the way IPv6 will be introduced and certainly cannot claim a "one size fits all" policy, we can anticipate the most likely ways of introducing IPv6 and try to make these scenarios as easy to manage as possible [2]. The problem in the IPv6 deployment is incompatibility, the inability of IPv4 nodes to understand the IPv6 header also, hosts with only IPv4 implementation cannot communicate with others using IPv6 because they will not be able to parse the IPv6 header [2]. Also, along with the existence of IPv6 and the challenges how to make it possible for both protocols to communicate, the security issues also need to be consider. In this paper, we discussed about the comparison of IPv4 and IPv6 in certain category, the mechanisms that are used to make both protocols to communicate and be compatible and the security issues that followed with this transition.

2. IPv6 and IPv4 Comparison

In this section, we compare IPv4 and IPv6 in terms of some categories.

Table 1. Comparison of IPv4 and IPv6 [1]

Category	IPv4	IPv6	IPv6 Advantages
Address Space	4 Billion Addresses	2^128	79 Octillion times the IPv4 address space
Configuration	Manual or use DHCP	Universal Plug and Play (UPnP) with or without DHCP	Lower Operation Expenses and reduce error
Broadcast / Multicast	Uses both	No broadcast and has different forms of multicast	Better bandwidth efficiency
Security	Uses IPsec for Data packet protection	IPsec becomes the key technology to protect data and control packets	Unified framework for security and more secure computing environment
QoS support	ToS using DIFFServ	Flow classes and flow labels	More Granular control of QoS
Network Configuration	Mostly manual and labor intensive	Facilitate the re-numbering of hosts and routers	Lower operation expenses and facilitate migration
Mobility	Uses Mobile IPv4	Mobile IPv6 provides fast handover, better router optimization and hierarchical mobility	Better efficiency and scalability; Work with latest 3G mobile technologies and beyond.

Table 1 show that IPv6 brought many improvements in Internet protocol stacks, from IPv4 to IPv6.

3. Connectivity of IPv6 to IPv4

The goal for a successful connectivity is to allow IPv6 and IPv4 hosts to interoperate. Another goal is to allow IPv6 hosts and routers to be deployed in the Internet in a highly diffuse and incremental fashion, with few interdependencies. Lastly, easy transition for end- users, system administrators, and network operators is also aimed.

The IPv6 transition mechanisms are a set of protocol mechanisms implemented in hosts and routers, with some operational guidelines for addressing and deployment, designed to make the transition to work with as little disruption as possible. These will ensure that IPv6 hosts can interoperate with IPv4 hosts in the Internet up until the time when IPv4 addresses run out.

There are number of IPv6-to-IPv4 transition technologies are introduced to overcome the interoperability between IPv6 and IPv4 issues.
The following focused on specific implementation:

- *Tunneling*

Tunneling is a method which encapsulates the IPv6 packets produced by an upgraded system with IPv4 headers. This allows you to send these packets over an IPv4 network. When an IPv6 packet is encapsulated into an IPv4 header, only the outer (IPV4) header is visible to intermediate routers, hence, eliminating possible problems resulting from IPv4 routers being unable to forward IPv6 packets. Tunneling can be useful when two IPv6 hosts to communicate over an IPv4 Internet, which is likely to be very common scenario in the short and medium terms. Tunneling can be done on an end-to-end basis, with the tunnel entry point being the host originating packets and tunnel exit point being the ultimate destination, or between intermediate routers, or between a host and a router.

- *Translation*

  IPv6 transition mechanisms are technologies that facilitate the transitioning of the Internet from its initial (and current) IPv4 infrastructure to the successor addressing and routing system of Internet Protocol Version 6 (IPv6). As IPv4 and IPv6 networks are not directly interoperable, these technologies are designed to permit hosts on either network to participate in networking with the opposing network.

- *Dual-stack*

  Dual Stack Transition Mechanism was designed to allow operators to deploy an IPv6-only routing infrastructure. Hosts on the other hand can be IPv4 and IPv6- enables to allow them to communicate with any host on the Internet without the need for translation [2].
  A common dual-stack migration strategy is to make the transition from the core to the edge. This involves enabling two TCP/IP protocol stacks on the WAN core routers, then perimeter routers and firewalls, then the server-farm routers and finally the desktop access routers. After the network supports IPv6 and IPv4 protocols, the process will enable dual protocol stacks on the servers and then the edge computer systems.

4. Network Infrastructure

For reaching the IPv6 networks the border routers have to perform a simple routing process. To ensure that the IPv4 hosts are reachable from the outer world NAT-PT has to be taken out. Like the classical Network Address Translation (NAT) NATPT could be configured in a static (fixed map between IPv4- and IPv6-address) as well as in a dynamic way (virtual IPv6 address will be assigned out of an address pool). Since the

global network is logical based on pure IPv6 the DNS server is located in the IPv6 network. Because commercial IPv6- firewalls are not available on the market today only the IPv4-networks are protected by this kind of equipment. It has to be investigated which additional mechanisms have the ability to secure the pure IPv6 networks. Following NAT-PT restrictions will be investigated and their impact on security issues discussed. This should not affect IPv6 to IPv6 communication [5].The NAT-PT translation method has some limitations that are similar to the classical NAT. For instance it is mandatory that all requests and responses pertaining to a session have to be routed via the same NAT-PT router. One way to guarantee this would be to have NAT-PT based on a border router that is unique to a stub domain, where all IP packets are either originated from the domain or destined to the domain [5]. This point is reflected in the chosen topology where NAT-PT is performed on the border routers. In the future when IPv6 will be widespread deployed it is expected to have NAT-PT routers only at the borders of IPv4 islands.

5. Technology and Threat Differences

In IPv6 the basic function of mitigating access to other IP devices based on policy is still implemented with firewalling and ACLs on end hosts and internetworking devices. However, numerous significant differences between the IPv6 and IPv4 headers may change how an administrator deploys these technologies.

IPsec:

IPsec has similar impacts on the administrator's ability to enforce security policy with the IP header information when implementing with IPv4 or IPv6. Because of the cryptographic protections, if IPsec encryption is implemented from end to end, current firewalling technology is effective only in applying policy based on Layer 3 information. If IPv6 uses only the authentication header, it is conceivable that IPv6-capable firewalls could inspect the upper-layer protocols within the authentication-header (AH) encapsulation and permit or deny access to the packet based on that information [6].

Extension Headers:

The IP options in IPv4 are replaced with extension headers in IPv6. Because of this replacement, extension headers may be used in an attempt to circumvent security policy. For example, all IPv6 endpoints are required to accept IPv6 packets with a routing header. It is possible that in addition to accepting IPv6 packets with routing headers, end hosts also process routing headers and forward the packet. With this possibility, routing headers can be used to circumvent security policy implemented on filtering devices such as firewalls [6].

To avoid this possibility, the network manager should designate the specific set of nodes that are to act as MIPv6 home agents (typically the default router for the subnet). The network designer should also validate that the operating systems within their organization do not forward packets that include the routing header. If operating systems that do forward packets that include the routing header are on the network, then the network designer must configure the network to filter the routing header on access control devices. If MIPv6 is not needed, packets with the routing header can be easily dropped at access control devices without relying on the end host to not forward the packets. Although it is easy to start with a "no MIPv6" policy, the emerging

applications on handheld devices with Wi-Fi access will make that stance challenging to maintain [6].

The right thing to do is to determine what extension headers will be allowed through the access control device. Network designers should match their IPv6 policy to their IPv4 IP options policy. If any IPv4 IP options are denied on the access control device, the IPv6 access control device should implement the same policies. Additionally, administrators should understand the behavior of the end-host operating system when dealing with the extension headers and dictate security policy based on that behavior. For instance, as noted earlier, the administrator should validate that end-host operating systems do not forward packets that contain a routing header [6].

6. Security issues and Considerations

In the previous section we discussed the mechanisms how IPv4 and IPv6 communicate, these are through tunneling, translation and Dual-Stack. Now, we will discuss the security considerations when we use each this mechanism.

First is the issue of using the tunneling, 6to4 is a system that allows IPv6 packets to be transmitted over an IPv4 network without the need to configure communication tunnels. Routings are also in place that allows 6to4 hosts to communicate with hosts on the IPv6 environment. This is used when an end site or end user wants to connect to the IPv6 environment using their existing IPv4 connection.

The 6to4 is especially significant during the initial phase of IPv6 deployment to full, native IPv6 connectivity. However, it is intended only as transition mechanism and not permanent [1].

Even if the 6to4 system properly implemented, it also pose security threats. Following are some of the threats like, Denial-of-Service (DoS) attacks, Reflection attacks, Service Theft, in which a malicious node, sites, operator may make unauthorized use of service

Also, there are some potential problems accompanied when using tunneling, among these are:[1]

1. The 6to4 routers not being able to identify whether relays are legitimate
2. The 6to4 architecture used to participate in DoS or reflected DoS, making another attack harder to trace
3. The 6to4 relays being subject to “administrative abuse”

Second is the issue of Translation, using this mechanism also needs security considerations.

1. Improper Translation implementation may be subject to buffer overflow attack, but this kind of issue is implementation dependent.
2. Due to the nature of TCP/UDP relaying service, it is not recommended to use Translation for protocols that use authentication based on source IP address.
3. A transport relay system intercepts TCP connection between two nodes. This may not be a legitimate behavior for an IP node.
4. The IPsec cannot be used across a relay. Thus defeat the security purpose of Implementing IPv6.
5. Use of DNS proxies that modify the RRs will make it impossible for the resolver to verify DNSsec signatures.

6. Similar to an SMTP open relay, Translation for traffic to IPv4 can be abuse by malicious user, which is similar to circumventing ingress filtering, or to achieve some other improper use. Access control can be implemented to prevent such improper usage

Last is the Dual-Stack Mechanism, dual-stack operation can raise other security problems if consistent security policies are not created for both IPv6 and IPv4 traffic. For example, if a firewall is not configured to apply the same level of screening to IPv6 packets as for IPv4 packets, the firewall may let IPv6 pass through to dual-stack hosts within the enterprise network, potentially exposing them to attack [1].

7. Conclusion

IPv6 brings improvement to the old IPv4 protocol stack. However, along with the benefits it brings, it opens new considerations back from the old one. Transition of technologies always poses security threats that need to be considered for successful implementation and also the backward compatibility issues. In this paper we discussed the IPv4 and IPv6 security requirements for interoperability of both protocols. Therefore, there is a need to carefully study the requirements for the transition and address the security related issues on their implementation.

References

[1.] http://www.brucert.org.bn/files/IPv6-to-IPv4%20Transition%20&%20Security%20Issues.pdf, Retrieved, 2012/07/25.
[2.] H. Soliman, “Mobile IPv6: Mobility in a Wireless Internet”, Addison-Wesley Professional, ISBN: 0201788977, 2004.
[3.] E. Davies, “IPv6 Transition/Coexistence Security Considerations”, Request for Comments: 4942, Network Working Group, 2007.
[4.] H.S. Yoo, G. Cagalaban, S. H. Kim, “A Study on the Connectivity of IPv6 to IPv4 Domains and Its Security Issues”, International Journal of Advanced Science and Technology, Vol. 10, September, 2009.
[5.] Thorsten Brikey, “Security Measures to couple mixed IPv4/IPv6 Networks over a pure IPv6 Infrastructure by making Use of NAT-PT”, SANS Institute InfoSec Reading Room, 2003.
[6.] S. Convery, D. Miller, "IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)", http://seanconvery.com/v6-v4-threats.pdf.