International Journal of Advanced Science and Technology
Vol. 10, September, 2009

A Study on the Connectivity of IPv6 to IPv4 Domains and Its Security Issues

Hwan-Souk Yoo[1], Giovanni A. Cagalaban[2], Sang-Ha Kim[1]

Chungnam National University, Daejeon, Korea[1]
Hannam University, Daejeon, Korea[2]
grep@cclab.cnu.ac.kr[1], *shkim@cnu.ac.kr*[3]
gcagalaban@yahoo.com[2]

Abstract

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. Transition technologies were developed to support the transition from the IPv4-based Internet to IPv6-based Internet. This paper discusses the 6to4 mechanism, a powerful IPv6 transition tool 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 to IPv4 domains particularly the 6to4 mechanisms.

1. Introduction

The current Internet Protocol, version 4, known as IPv4, has been developed to support the Internet's rapid growth during the 80s. IPv4 has been shown to be robust, easily implemented and interoperable. It uses a 32-bit address space, in which can accommodate about 4 billion unique addresses. Today, however, that amount is insufficient, even more if we consider emerging new technologies such as 3G/4G wireless devices and other wireless appliances [1]. The Internet has grown much bigger than was anticipated before. Due to this, there are several problems such as impending exhaustion of the IPv4 address space, configuration and complexities and poor security at the IP level that must be considered.

Aware of the limitations of the current Internet infrastructure, IETF (Internet Engineering Task Force (IETF) began developing a new IP protocol in the early 90s to replace IPv4. The next generation Internet Protocol [2], first called as IPng and then as IPv6, will use a 128-bit address space. It would support unique addresses well beyond the trillions. It will not only eliminate the shortcomings of IPv4, but also deliver new features and services. The development of IPv6 has been on how to do the transition away from IPv4, and towards IPv6. The work on transition strategies, tools, and mechanisms has been part of the basic IPv6 design effort from the beginning of its development.

The design efforts resulted in a basic Transition Mechanisms specification for IPv6 hosts and routers [3] that specifies the use of a Dual IP layer providing complete

support for both IPv4 and IPv6 in hosts and routers, and IPv6-over-IPv4 tunneling, encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures. These design concepts are greatly depended on for transition from the traditional IPv4-based Internet to an IPv6-based Internet. IPv4 and IPv6 are anticipated to coexist for many years during this transition.

One of the concerns to transition strategy planners is how to provide connectivity between IPv6-enabled end-user sites when they do not yet have a reasonable choice of Internet Service Provider (ISP) that provides native IPv6 transport services. Another concern is that, IPv4 was created with no security in mind. Because of its end-to-end model, IPv4 relies on the end-hosts to provide the appropriate security during communication.

This study aims to discuss the connectivity between IPv6 to IPv4 routing domains as well as the emphasis on their security-related functionality. This paper specifically analyzes the 6to4 security issues in more detail and provides some enhancements to security mechanisms.

2. IPv4 Security Issues

2.1. Hierarchical Mobile IPv6

Before studying IPv6, we need to understand some of the best known limitations of its predecessor, IPv4. IPv4 was designed with no security in mind. Because of its end-to-end model, IPv4 relies on the end-hosts to provide the appropriate security during communication [4]. Today, the Internet continues to be completely transparent and no security framework provides for resilient against threats such as:

• Denial of Service Attacks (DOS): it is a kind of attempt to make a computer resource unavailable to its intended users by being flooded with a large amount of illegitimate requests. An example of DOS attack that results from an architectural vulnerability of IPv4 is the broadcast flooding attack or Smurf attack [5].

• Malicious code/program distribution: malicious code/program such as viruses and worms can replicate themselves from one infected or compromised hosts to another. IPv4's small address space can facilitate malicious code distribution [5].

• Man-in-the-middle attacks (MITM): IPv4's lack of suitable authentication mechanisms may allow an attacker is able to read, insert and modify at will messages between two hosts without either hosts knowing that their communication has been compromised. ICM redirects can also be used to carry out this type of attacks [5][6].

• Fragmentation attacks: this type of attack uses many small fragmented ICMP packets which when reassembled at the destination exceed the maximum allowable size for an IP datagram which can cause the target system to crash, hang or even reboot [5].

• Port scanning and reconnaissance attacks: this attack is used to scan for multiple listening ports on a single, multiple or an entire network hosts. Open ports can be used to exploit the specific hosts further. Because of the small address space, port scanning is easy in IPv4 architecture and can take a little more than 4 minutes [7].

• ARP Poison: Address Resolution Protocol (ARP) poison attack is to send fake, or spoofed, ARP messages to a network. The aim is to associate the attacker's MAC

address with the IP address of another node. Any traffic meant for that IP address would be mistakenly sent to the attacker instead [5].

However, many techniques or method had been developed to overcome the abovementioned security concerns. For example, the use of IPSec to assist the use of encrypted communication between hosts, but this is optional and continues to be the major responsibility of the end hosts.

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.

One way to provide IPv6 connectivity between end-user sites is to use IPv6-over-IPv4 tunneling between them, similar to the technique currently used in the 6bone [5] IPv6 testbed network. This requires complexity for both end-user sites, and the networks providing the tunneling service, in creating, managing, and operating manually configured tunnels. See Figure 1 for a manually configured tunnel. End-User addresses are carried in the Global Domain Name System (DNS).

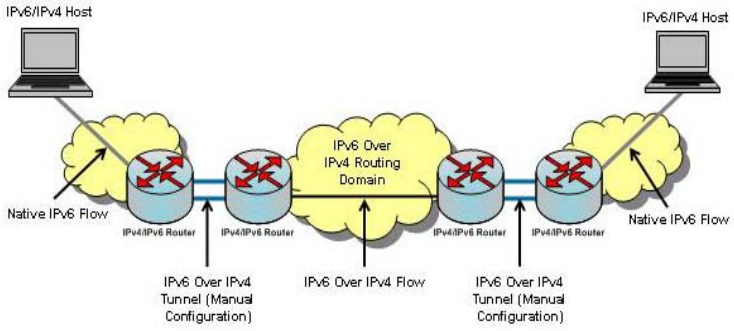

Figure 1. Manually Configured Tunnel

The 6to4 transition mechanism, "Connection of IPv6 Domains via IPv4 Clouds without Explicit Tunnels" [6], provides a solution to the complexity problem of using manually configured tunnels by specifying a unique routing prefix for each end-user site that carries an IPv4 tunnel endpoint address. 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. 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.

When end-user site networks enable IPv6 in their local host and router systems, but have no native IPv6 Internet service, connectivity to other IPv6 routing domains across

a worldwide Internet must be accomplished another way, or the value of a connected Internet is lost. Prior to the 6to4 transition mechanism, a site's network staff would have to rely on the manual configuration of IPv6-over-IPv4 tunnels to accomplish this connectivity.

This connectivity could be accomplished by arranging tunnels directly with each IPv6 site to which connectivity is needed, but more typically is done by arranging a tunnel into a larger IPv6 routing infrastructure that could guarantee connectivity to all IPv6 end-user site networks. See Figure 2 for a 6to4 tunnel configuration.

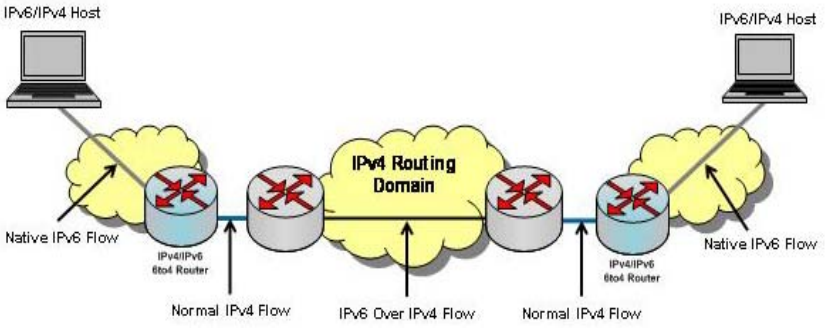

Figure 2. 6 to 4 Tunnel Configuration

The 6to4 transition mechanism provides a solution to the complexity problem of building manually configured tunnels to an ISP by advertising a site's IPv4 tunnel endpoint (to be used for a dynamic tunnel) in a special external routing prefix for that site. Thus one site trying to reach another will discover the 6to4 tunnel endpoint from a DNS name to address lookup and use a dynamically built tunnel from site to site for the communication. The tunnels are transient in that there is no state maintained for them, lasting only as long as a specific transaction uses the path. A 6to4 tunnel also bypasses the need to establish a tunnel to a wide-area IPv6 routing infrastructure, such as the 6bone.

Figure 3. Prefix Format

Figure 3 shows the specification of a 48-bit external routing prefix in the IPv6 Aggregatable Global Unicast Address Format [10] that provides just enough space to hold the 32 bits required for the 32-bit IPv4 tunnel endpoint address (V4ADDR in Figure 3) makes this setup possible. Thus, this prefix has exactly the same format as normal prefixes assigned according to the AGGR. Within the subscriber site it can be

used exactly like any other valid IPv6 prefix, for instance, for automated address assignment and discovery according to the normal IPv6 mechanisms for this.

The most interesting, and most complex, 6to4 scenario is that of sites with only 6to4 connectivity communicating with sites with only native IPv6 connectivity. This is accomplished by the use of a 6to4 relay that supports both 6to4 and native IPv6 connectivity as shown in Figure 4. The 6to4 relay is nothing more than an IPv4/IPv6 dual-stack router.

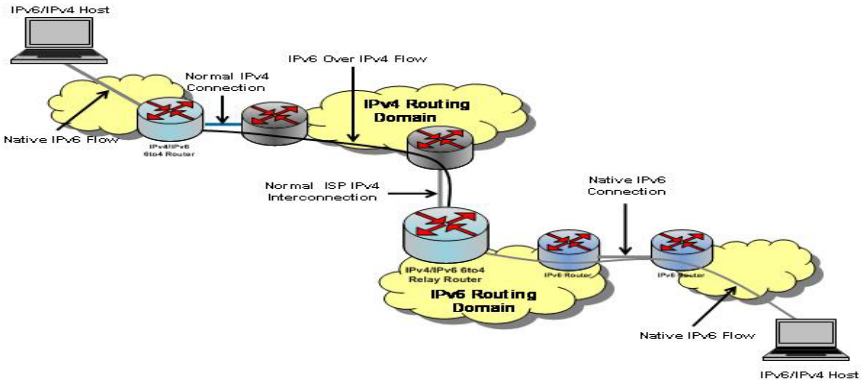

Figure 4. 6 to 4 Relay

The 6to4 relay advertises a route to 2002::/10 for itself into the native IPv6 infrastructure it is attached to. The native IPv6 network operators must filter out and discard any 6to4 prefix advertisements longer than /16. In addition, the 6to4 relay may advertise into its 6to4 connection whatever native IPv6 routes its policies allow, which the 6to4 router at the 6to4-only site picks up with either a BGP4+ peering session, or with a default route, to the 6to4 relay.

As such, it is expected that native IPv6 service providers will choose to operate 6to4 relays as a simple extension of their service. There are no special rules or exceptions to 6to4 as described here for this to happen because the 6to4 relay is simply operated as part of an end-user site that belongs to the IPv6 ISP.

4. IPsec

IPv4 offers support for IPSec but it is optional. By contrast, the RFC4301 mandates for IPv6 to use IPSec in all nodes [6] [11]. IPSec consists of a set of cryptographic protocols that provide for securing data communication and key exchange. IPSec uses two wire-level protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). The first protocol provides for authentication and data integrity. The second protocol provides for authentication, data integrity, and confidentiality [11].

In IPv6 networks both the AH header and the ESP header are defined as extension headers. Additionally, IPSec provides for a third suite of protocols for protocol negotiation and key exchange management known as the Internet Key Exchange (IKE). This protocol suite provides the initial functionality needed to establish and negotiating

security parameters between endpoints. Also, it keeps track of this information to guarantee that communication continues to be secure up to the end.

4.1. Authentication Header

Authentication header prevents IP packets from being tampered or altered. In a typical IPv4 packet, the AH is part of the payload. When the AH protocol was implemented, there was some concern about how to integrate it to the new IPv6 packet format. The problem centered on the fact that IPv6 extension headers can change in transit as information they contain is updated through the network. To solve this problem, IPv6 AH was designed with flexibility in mind—the protocol authenticates and does integrity check only on those fields in the IPv6 packet header that do not change in transit. Also, in IPv6 packets, the AH is intelligently located at the end of the header chain – but ahead of any ESP extension header or any higher level protocol such as TCP/UDP [1].

The AH header protocol also provides optional protection against replay attacks. The protocol uses its sequence number field as part of a sliding window mechanism that prevents arbitrary packet delays and malicious replay [1] [12].

4.2. Encapsulating Security Payload

In addition to providing the same functionality the AH protocol provides – authentication, data integrity, and replay protection – ESP also provides confidentiality. In the ESP extension header, the security parameter index (SPI) field identifies what group of security parameters the sender is using to secure communication. ESP supports any number of encryption mechanisms. However, the protocol specifies DES-CBC as its default. Also, ESP does not provide the same level of authentication available with AH. While AH authenticates the whole IP header (in fact, only those fields that do not change in transit), ESP authenticates only the information that follows it [1].

ESP provides data integrity by implementing an integrity check value (ICV) that is part of the ESP header trailer – the authentication field. The ICV is computed once any encryption is complete and it includes the whole ESP header/trailer – except for the authentication field, of course. The ICV uses hash message authentication code (HMAC) with SHA-1 and MD5 as the recommended cryptographic hash functions [12].

In IPv6 networks, both the AH header and the ESP header are defined as extension headers. Additionally, IPSec provides for a third suite of protocols for protocol negotiation and key exchange management known as the Internet Key Exchange (IKE). This protocol suite provides the initial functionality needed to establish and negotiating security parameters between endpoints. In addition it keeps track of this information to ensure secure communication at all times.

5. 6 to 4 Security Issue

The 6to4 specification outlines a few security considerations and rules but is ambiguous as to their exact requirement level. Furthermore, the description of the considerations was rather short, and some of them have proven difficult to understand

or impossible to implement. The characteristics of the 6to4 mechanism introduce four main potential problems, as stated below:

1. The 6to4 routers are not able to identify whether relays are legitimate.
2. The 6to4 routers or relay security checks are wrong or impartially implemented.
3. The 6to4 architecture is used to participate in DoS or reflected DoS, making another attack harder to trace.
4. The 6to4 relays are being subject to administrative abuse.

Even if the 6to4 system is properly implemented, it still poses security threats. Following are some of the threats that can be performed:

- Denial-of-Service attacks
- Reflection Denial-of-Service attacks
- Service Theft, in which a malicious node/site/operator may make unauthorized use of service

Additional security issues with 6to4 relays are due to the fact that 6to4 relays by nature have a native IPv6 connection in addition to IPv4 and relay rather freely between the two. Native IPv6 nodes anywhere can use the relay as a means to obscure their identity when attacking. Attackers from IPv6 can attack IPv4 hosts with tunnelled packets sending spoofed 6to4 packets via a relay to the IPv4 hosts. The relay can obscure identity, if it relays any packets while not checking if the 6to4 address actually matches the IPv4 host the packet comes from.

6. Conclusions

IPv6 represents a considerable improvement if compared to the old IPv4 protocol stack. The new suite of protocols provides innumerable features that improve both the overall functionality as well as some specific security functions. Transition technologies always poses security threats, for instance most security related products (firewall/IDS/IPS) have not been programmed to inspect IPv6 packets in depth thus can allow malicious packets to pass through by taking advantage on the encapsulation of IPSEC in IPv6.

The 6to4 mechanism allows isolated IPv6 routing domains to communicate with other IPv6 routing domains, even in the total absence of native IPv6 service providers. It is a powerful IPv6 transition tool 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.

Despite its attractiveness, this transition mechanism poses security issues where malicious users can fully exploit. Therefore, there is a need to carefully study the requirements for the transition and address the security related issues on their implementation.

References

[1] Davies, J., Understanding IPv6, 2003.
[2] Deering, S., Hinden, R., “Internet Protocol Version 6 (IPv6) Specification,” RFC 2460, http://www.ietf.org/rfc/rfc2460.txt.
[3] Transition Mechanisms for IPv6 Hosts and Routers. http://www.ietf.org/rfc/rfc1933.txt
[4] Bradner, S., "The End-to-End Security," IEEE Security & Privacy, pp., 76-79, 2006.
[5] Campbell, P.; Calvert, B.; Boswell, S., Security+ Guide to Network Security Fundamental, 2003.
[6] Popoviciu C., Levy-Avegnoli, E., Grossetete, P., Deploying IPv6 Networks, 2006.
[7] Ford, M., “New Internet Security and Privacy Models Enabled by IPv6,” The 2005 Symposium on Applications and the Internet Workshops, 2005.
[8] The 6bone IPv6 Testbed Network, http://www.6bone.net
[9] Connection of IPv6 Domains via IPv4 Clouds without Explicit Tunnels" ("6to4"), http://www.6bone.net/misc/6to4.txt
[10] "IPv6 Aggregatable Global Unicast Address Format," RFC 2374, http://www.ietf.org/rfc/rfc2374.txt
[11] Kent, S., Seo, K., “Security Architecture for the Internet Protocol,” RFC 4301, Dec. 2005, http://tools.ietf.org/html/4301.
[12] Friedl, S., “An illustrated Guide to IPSec,”Unixwiz.net, Aug. 2005, http://www.unixwiz.net/techtips/iguide-ipsec.html.

Authors

Hwan-Souk Yoo received the B.S. and M.S. degree in Computer Science from Chungnam National University, Daejeon, Korea, in 2001 and 2003. He has joined Electronics and Telecommunications Research Institute(ETRI) as a visited assistance researcher between 2001 and 2002. He went on for a Ph.D. program in Computer

Science from Chungnam National University, in 2003. He was with SDR Middleware Research Team(ETRI) as a researcher and R&D for SDR Technology, between 2007 and 2009. His current research interests include wireless communication network, software defined radio, SCA, network simulator, IPTV Qos, and inter-domain routing. His email address is grep@cclab.cnu.ac.kr.

Giovanni A. Cagalaban received a B.S degree in Computer Science from the University of the Philippines in the Visayas, Miag-ao, Iloilo, Philippines, 2000 and M.S. degree in Computer Science from Western Visayas College of Science and Technology, Iloilo City, Philippines, 2007. Currently, he is on the Integrated Course in Multimedia Engineering from Hannam University. His research interests include multimedia system, SCADA security and sensor network. gcagalaban@yahoo.com

Sang-Ha Kim received the B.S. degree in chemistry from Seoul National University, Seoul, Korea, in 1980, and he received the M.S. and Ph.D. degrees in quantum scattering and computer science from the University of Houston, Houston, TX, in 1984 and 1989, respectively. He was with the Supercomputing Center, SERI, Korean Institute of Science and Technology (KIST) as a senior researcher between 1990 and 1991. He has joined Chungnam National University, Daejeon, Korea, since 1992, where he is a Professor. His current research interests include wireless networks, *ad hoc* networks, sensor networks, QoS, optical networks, and network analysis. Prof. Kim is a member of ACM, IEEE Communications Society, IEEE Computer Society, KICS, KIPS, etc. His email address is shkim@cnu.ac.kr