International Journal of Engineering Research & Management Technology

May- 2015 Volume 2, Issue-3
ISSN: 2348-4039

Email: editor@ijermt.org www.ijermt.org

IJERMT

"Sharpening Skills.....
Serving Nation"

Special Issue: 2nd International Conference on Advanced Developments in Engineering and Technology
Held at Lord Krishna College of Engineering Ghaziabad, India

IPV4 to IPV6 Translation and Securities

Rahul Nagar
M.Tech Scholar
Al- Falah School of Engineering & Technology
Faridabad, Haryana

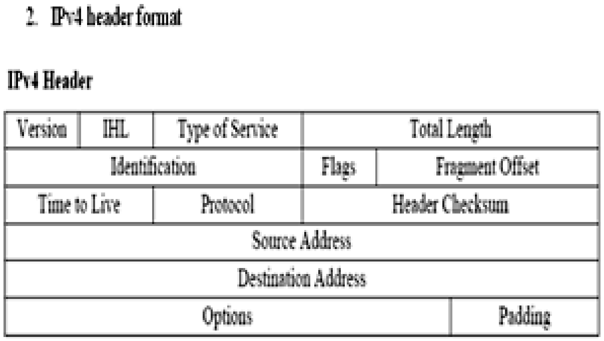
Ashif Ali
Assistant Professor
Al- Falah School of Engineering & Technology
Faridabad, Haryana

ABSTRACT—
The IPv6 protocol has solved some, but not all, of the security problems found in IPv4 networks. One example is the mandatory inclusion of IP Security (IP sec) in the IPv6 protocol, which makes it fundamentally more secure than the older IPv4 standard. However, given its flexibility, the IPv6 protocol introduces new problems. A mobile IP protocol is built into the IPv6 protocol, and security solutions for this protocol are still under development.

Keywords— IPV4, IPV6, types of translation, translation, conversion, security method and threats.

I. IPV4

The prevailing Internet Protocol standard is IPv4 (Internet Protocol version 4), which dates back to the 1970s. There are well known limitations of IPv4, including the limited IP address space and lack of security. IPv4 specifies a 32 bit IP address field, and available address spaces are rapidly running out. The only security feature provided in IPv4 is a security option field that provides a way for hosts to send security and handling restrictions parameters. As shown in figure 1.[1][2]



2. IPv4 header format

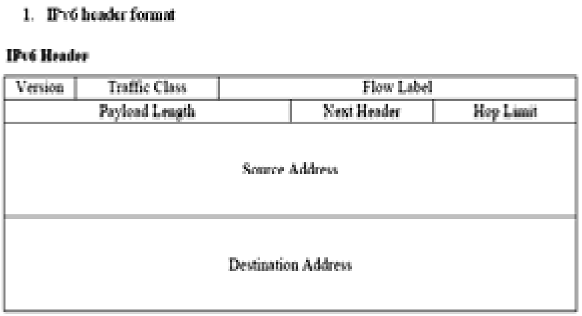
IPv4 Header

<table>
<tr><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="3">Header Checksum</td></tr>
<tr><td colspan="6">Source Address</td></tr>
<tr><td colspan="6">Destination Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

Figure 1: IPV4 HEADER

II. IPV6

A new header format A much larger address space (128bitin IPv6, compared to the 32-bit address space in IPv4) .An efficient and hierarchical addressing and routing infrastructure. Both stateless and stateful address configuration. as shown in figure 2.[1][2]



1. IPv6 header format

IPv6 Header

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Figure 2: IPV6 HEADER

III. TYPES OF TRANSLATION

Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. It is unlike implementation of other new technologies where the newer one is backward compatible so the older system can still work with the newer version without any additional changes.

To overcome this short-coming, we have a few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6.

A. Dual Stack Routers

A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.[4]As shown in figure 3.

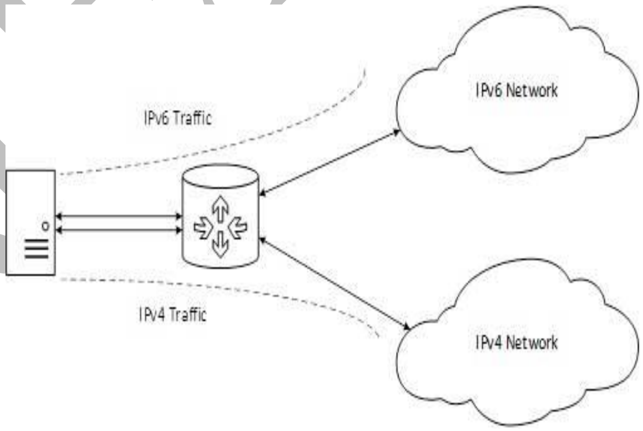


Figure 3: Dual Stack Router

A. Tunneling

In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through a non-supported IP version. As shown in figure 4.[5]

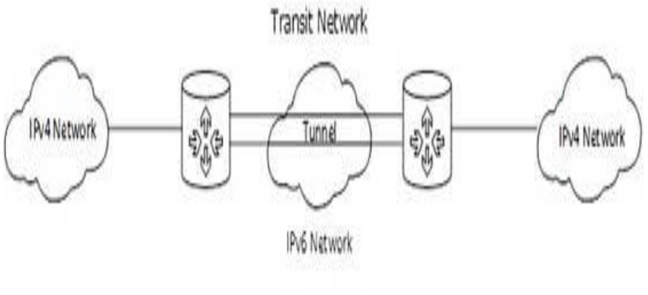


Figure 4: TUNNELING

A. NAT Protocol Translation

This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa. A host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa. As shown in figure 5.[5].

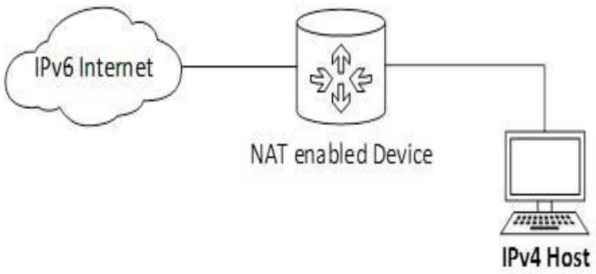


FIGURE 5: NAT

IV. TRANSLATION

The concept of address translation is also not a new concept to most network engineers; this is because Network Address Translation (NAT) is implemented between different IPv4 networks in almost every residential household. The concept behind this type of NAT and the newer technologies that support address translation between IPv4 and IPv6 networks is similar. IPv6 translation technologies differ from IPv6 tunneling technologies; this is because the translation technologies enable IPv4-only devices to speak to IPv6-only devices, which is not possible with any of the tunneling methods.

However, IPv4/IPv6 translation and IPv4-only translation entail a certain amount of complexity. What happens when an IPv6-only device is attempting to communicate with a device on the public IPv4 Internet and only an IPv4 DNS record (A) exists? In these situations, a secondary technology is required to step in and provide additional services for the connection to work.

The first method to be introduced to provide IPv6 translation services was Network Address Translation - Protocol Translation (NAT-PT). NAT-PT defined a mechanism to not only translate between IPv4 to IPv6 addresses but also a built-in ability to provide protocol translation services for Internet Control Message Protocol (ICMP), File Transfer Protocol (FTP), and Domain Name System (DNS). The component that was responsible for these translation services is called the application layer gateway (ALG).[6]

The ALG piece of the NAT-PT method raised a number of issues. With additional testing and real-life experience, a new method was introduced that separated the address translation functionality and the application layer translation functionalities: NAT64 and DNS64.

DNS64 can synthesize IPv6 address resource records (AAAA) from IPv4 resource records (A); it does this by encoding the returned IPv4 address into a IPv6 address format.

Some more tunneling methods explained below in table 1:-

Tunneling Method	Suggested Usage
Manual	Used to provide a point-to-point IPv6 link over an existing IPv4 network; only supports IPv6 traffic.
GRE	Used to provide a point-to-point IPv6 link over an existing IPV4 network; supports multiple protocols, including IPv6.
6to4	Used to provide a point-to-multipoint IPv6 link over an existing IPv4 network; sites must use IPv6 addresses from the 2002::/16 range.
6rd (or 6RD)	Used to provide a point-to-multipoint IPv6 link over an existing IPv4 network; sites can use IPv6 addresses from any range.
ISATAP	Used to provide point-to-multipoint IPv6 links over an existing IPv4 network. Designed to be used between devices inside the same site.

Table 1: Translation Method

V. IPv4 TO IPv6 CONVERSION

The IPv4 to IPv6 Conversion tool helps you see how your IPv4 address would be represented in the new IPv6 protocol. This can aid network administrators who are migrating IPv4 to IPv6 networks and wish to preserve IPv4 addressing for compatibility and/or tracking purposes. For example if your IPv4 IP is 209.173.53.167 the valid IPv6 version will be 0:0:0:0:0: ffff:d1ad:35a7.[6].

VI. SECURITY ATTACKS AND THREATS OF IPV4 AND IPV6 TOGETHER

1. The sniffing attacks

A typical example of an attack that affects both IPv4 and IPv6 network is a sniffing attack. The sniffing attack involves capturing of the data being transmitted through the network. In case that confidential data are transmitted in a plaintext protocol, they can easily be compromised by an attacker running sniffing attack. A sniffing attack type can be avoided by a proper use of the IPsec security architecture, which is used in IPv4 as an option and in IPv6 as an obligation. [7]

2. Application layer attacks

Application layer attacks are the most common attacks today. Here e.g. belong buffer overflow attacks, web application attacks (e.g. CGI attacks), different types of viruses and worms. Unfortunately, transition to the IPv6 protocol will neither prevent computer systems and networks from these attacks nor alleviate their consequences since both IPv4 and IPv6 are protocols of the network layer and these types of attacks are performed at the application layer of the ISO/OSI network model. [7]

3. Flooding attacks

One of the most frequent attack types present in IPv4 networks is a flooding attack. It connotes flooding a network device (e.g. a router) or a host with large amounts of network traffic. A targeted device is unable to process such large amount of network traffic and becomes unavailable or out of service. A flooding attack can be local or a distributed denial of service attack (DoS), when the targeted network device is being flooded by network traffic from many hosts simultaneously. This type of attack can also affect the IPv6 networks, because the basic principles of the flooding attack remain the same. New types of extension headers in IPv6, new types of ICMPv6 messages and dependence on multicast addresses in IPv6 (e.g. all routers must have site-specific multicast addresses) may provide new ways of misuse in flooding attacks.[7]

4. Fragmentation related security threats

According to IPv6 protocol specification, packet fragmentation by intermediary nodes is not allowed. Since in IPv6 networks the usage of the path MTU discovery method (based on ICMPv6 messages) is an obligation, packet fragmentation is possible only at the source node. The minimal recommended MTU size for IPv6 networks is 1280 octets. For security reasons it is highly recommended to discard all fragments with less than 1280 octets unless the packet is the last in the flow. Using fragmentation an intruder can achieve that port numbers are not found in the first fragment and in that way bypass security monitoring devices (which do not reassemble fragments) expecting to find transport layer protocol data in the first fragment. By sending a large number of small fragments an attacker can cause an overload of reconstruction buffers on the target system potentially implying a system to crash (a type of a denial of service attack). To avoid such problems it is a recommended security practice to limit the total number of fragments and their allowed arrival rate.[7].

VII. CONCLUSION

The selection of an IPv6 transition mechanism depends greatly on the current status of an organization's network and how fast they want to transition their devices from IPv4 to IPv6. Logic seems to say that those organizations with bleeding-edge technology tastes and small staffs will probably be (or are already) the first people in line to transition over to IPv6. Those larger companies that have tens of thousands of network devices will most likely transition a piece at a time following the experience level of each department.

The transition to IPv6 is coming, and all those network engineers reading this article should become experts in IPv6 as quickly as possible. The process of converting networks from IPv4 to IPv6 will shortly become a large-scale request, and those with the correct skills will be in demand, a fact even more important in the current economy.

REFERENCES

1. IETF RFC 791 (September 1981).
2. Deering, S., &Hinden, R. (December1998). Internet Protocol Version 6 (IPv6) Specification, IETF RFC 2460
3. Narten, T., Nordmark, E., Simpson, W., &Soliman, H. (September 2007). NeighborDiscovery for IP version 6 (IPv6),IETF RFC 4861
4. Thomson, S., Narten, T., &Jinmei, T. (September 2007). IPv6 Stateless Address Autoconfiguration, IETF RFC 4862Conta, A., Deering, S., & Gupta, M. (March 2006). Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version6 (IPv6)Specification),IETF RFC 4443
5. Hinden, R., &Deering, S. (February 2006) IP Version 6 Addressing Architecture, IETF RFC 4291
6. Kent, S., &Seo, K. (December 2005). Security Architecture for the Internet Protocol , IETF RFC 4301
7. Ziring N. (May 2006). Router Security Configuration Guide Supplement - Security for IPv6 Routers. [Online]. Available: www.nsa.gov/ia/_files/routers/I33-002R-06.pdf
8. Hermann, P.-Seton (2002). Security Features in IPv6. [Online].Available:www.sans.org/reading_room/whitepapers/.../security_features_in_ipv6_380
9. Sotillo, S. (2006). IPv6 Security Issues. [Online]. Available: www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf
10. Sailan, M.K., Hassan, R., & Patel, A. (2009). A Comparative Review of IPv4 and IPv6 for Research Test Bed. 2009 International Conference on Electrical Engineering and Informatics, Selangor, Malaysia.
11. Caicedo, C.E., Joshi, J.B.D., &Tuladhar, S.R.(2009). IPv6 Security Challenge. Computer,42, 36-42.
12. Davies, J. (2003). Understanding IPv6, Microsoft Press.
13. Kanda, M. (2004). IPsec: a basis for IPv6 security. [Online]. Available:http://www.ipv6style.jp/en/tech/20040707/index.shtml.
14. Radwan, A.M. (2005). Using IPSec in IPv6 Security. [Online].Available:http://www.uop.edu.jo/csit2006/vol2%20pdf/pg471.pdf
15. Saito, Y. (December 2003). IPv6 and New Security Paradigm. NTT Communications, Doc. No. 79
16. Cisco Systems Report (2004). IPv6 SECURITY Session Sec-2003.
17. Oh, H., Chae, K., Bang, H., & Na, J. (February 2006). Comparisons analysis of Security Vulnerabilities for Security Enforcement in IPv4/IPv6.