International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Study and Comparison of Network Security in IPv4 and IPv6

Gagandeep Kaur, Dr. Karanjit Singh Kahlon

Department of CSE, Department of CSE, GNDU, GNDU, Amritsar, Amritsar, India

Abstract: ***Internet Protocol version 6 (IPv6) is the next generation internet protocol which is still in its transition phase from IPv4. The present paper not only discusses about the necessity of IPv6 which resulted from the exhaustion of IPv4 addresses but also present the study and comparison of various security issues in IPv4 and IPv6. It is clearly understood that today the IPv4 public addresses have been exhausted and there is clear need for transition to IPv6 which is necessary to remain connected with Internet. On the other hand, the migration process to IPv6 has strong impact on the network security. Although, IPv6 provides various innovative features which help to provide network security but because of infancy stage, it is also considered as a dangerous weapon that the attacker can use. In IPv4, various threats like viruses, worms, botnets and attacks like DoS, Fishing and Spoofing are independent of the Internet Protocol version used. In order to minimize the threats, more security measures are required. Firewall policies, network security rules must be hardened. As the IPv6 is new, the applications designed for IPv6 as well as the software are not yet field proven. They may contain bugs or errors that can become vulnerable to the network security. Also the quick transition from IPv4 to IPv6 is not possible and may span in years. With time and support, IPv6 when implemented will provide security on the equal level as today's IPv4 and even higher.***

Keywords: IPv4, IPv6, Network Security

1. Introduction

Billions of network devices are connected in a network and these networks are further joined to form the Internet. The number of devices is growing at such a large pace that the currently deployed internet protocol IPv4 when was designed never expected such a high growth. Personal computers, smart phones, switches, routers and many other devices require an IP address in order to connect with Internet. Such a large growth in the number of devices has made the 32 bit IPv4 unable to cater the increasing demand of IP addresses. IPv4 used many techniques to slow down the IP address drift[1].

In case of IPv4, various techniques were used like Dynamic Host Control Protocol (DHCP), Network Address Translation (NAT), Sub-netting in order to slow down the IPv4 IP address draught. Many devices working in the network can take IP address from a predefined IP pool in case of DHCP. NAT allows the users to share a few public IP addresses by many internal network users and sub-netting allows users sub-grouping the IP address range and thus solved the problem to some extent but not as a permanent solution. This situation thus created the necessity for IPv6 which is 128 bits as a solution to meet the increasing demand of IPv6. IPv6 can provide $34X10^{37}$ IP addresses which is considered as much more in comparison to IPv4 and can serve the network for many years to come.

Comparing IPv4 and IPv6 Header Format

The header size of IPv4 is 20 octet as shown in the Figure 1 whereas the header size if 40 octets in case of IPv6[5]. The header field of IPv6 is bigger than IPv4. The reason for this is IPv6 is 128 bit address. The notation of IPv6 address is as given below.

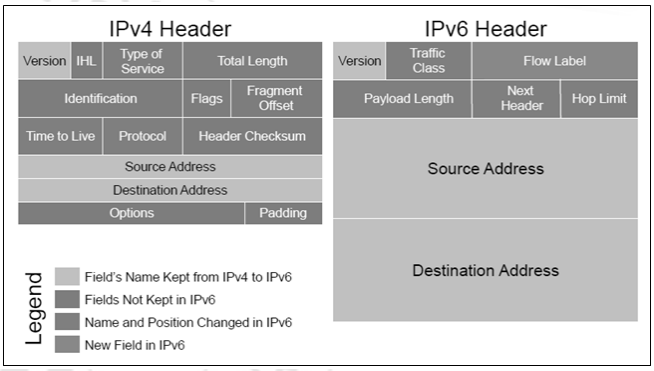

Figure 1: IPv4 and IPv6 Header Format

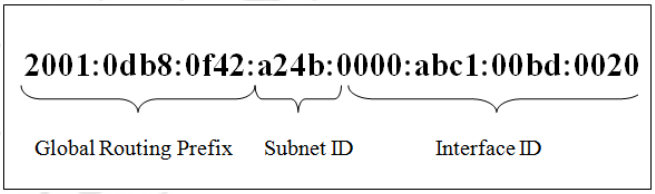

Figure 2: IPv6 Address Format

The addressing scheme of IPv6 comprises of 8 pairs of 2 byte blocks. The IP address has three portions known as Global Routing Prefix, Subnet ID and Interface ID. The Global Routing Prefix is assigned to a site which can be group of various subnets of links. The Subnet ID is used to identify a link in the site. The Interface ID is unique for every link. Also, while writing the IPv6 address format, colons are used as delimiters[5]. We can remove the leading zeros from the block. The above address can also be written as below.

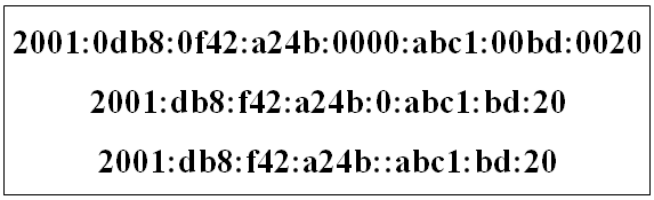

Figure 3: IPv6 Address format

Transition from IPv4 to IPv6

The Characteristics of IPv4 are compared with IPv6 in order to understand the security issues in connectivity methods used for connecting from IPv4 to IPv6 in the network. In order to do the transition to IPv6 from IPv4 various strategies are followed. Some have advantages over the other. These strategies are studies and discussed from the network security point of view.

Dual Stack

This method is used to introduce IPv6 in the network. Both IP protocol versions i.e. IPv4 and IPv6 are used in parallel[8]. The communication between the nodes receives only data from the other node using the same protocol version. The second layer is invisible to it. Considering the security issues of dual stack, it must be monitored and hardened and possible patched because such a network is prone to attacks based upon IPv4 as well as IPv6.

Tunneling

The second method that is used for transition from IPv4 is tunneling. In this method tunneling of one IP protocol is done in the other. Tunneling can be from IPv4 to IPv6 or vice versa. This allows the network nodes using IPv6 to connect via IPv4 tunnel and vice versa. Various tunneling techniques are used like Teredo (RFC 4380), ISATAP (RFC4214) or 6to4 (RFC 3056). Considering from the security issues point of view, the process of tunneling increases the network complexity. The network configuration while configuring the tunneling from IPv4 to IPv6 or vice versa makes the security devices like firewalls, filters etc. to become more complex and security vulnerable[9].

Translation

If the network comprises of IPv6 only hosts that need to communicate with IPv4, the translation between IPv6 and IPv4 is the only option. This method is becoming the most relevant technique like NAT64 is used by IPv6 nodes to connect to IPv4 nodes. From security point of view, translation helps the network to get rid of IPv4 based attacks and on the other hand it adds complexity which gives rise to security threats.

So, it can be concluded that from security point of view, none of the above strategies can be clearly preferred[7].

IPv6 Security Issues

IPv6 is considered as more secure in comparison to IPv4. It provides many innovative features and security features but still considered as vulnerable to network security and threats. There are various security issues still faced by IPv6 because of poorly configured servers, bugs in application based on IPv6 and weakly protected sites. The possible problems in IPv6 are because of the following reasons[11].

Header manipulation issues: The reason for this issue is no IPSec embedded functionality. This can result in attack because of header manipulation. When headers are processed by all the stacks, they can be overwhelmed to a particular node and this can become an attack. IPv6 Spoofing is also a security threat.

Flooding issues: IPv6 is also vulnerable to port scanning attacks. Complete ports are scanned and the free ports can be used for attacks. Flooding becomes a serious issue in network attack and vulnerable to network security.

Mobility issues: These issues also affect the security measures and there is a need to make the network administrator must be aware about IPv6 mobility issues.

Security Issues in IPv4 Vs IPv6

There are many security issues that are found in IPv4 as well as in IPv6. In the present paper three main security issues i.e. Network Address Translation (NAT), Internet Protocol Security (IPSec) and Layer 2 Security as discussed[13].

Network Address Translation (NAT): The declining number of IP address is a major issue in IPv4. NAT technology is used as a solution to this problem. Also, NAT provides security to the network because the internal users remain hidden from the outer world and they are not directly open to the Internet. Due to this reason, NAT is also preferred in IPv6. IPv6 uses Unique Local Addressing (ULA) which helps the users to protect their IP addresses and this is the reason that NAT is not used in IPv6.

Internet Protocol Security (IPSec): Advancement in Network Security is one of the motivation behind IPv4 to IPv6 transition. IPSec is the main cause behind this. It has become mandatory part of the IPv6. The data is encrypted and authenticated under IPv6 for data transmission over the network. Previously, in IPv4, IPSec can also be used but it was not mandatory and gives additional overhead in IPv4. Due to integration in IPv6 and IPSec it is considered as more secure to IPv4.

Layer 2 Security: In IPv6 Layer 2 security plays an important role and is more secure as compared to IPv4. The local link communication in IPv6 is made by ICMPv6. There are Router Solicitation (RS) message with Router Advertisement (RA) replies but it can also result in Man in The Middle (MITMA) attack. The hacker can send fake RA messages and act as router.

Another feature of layer 2 security is network neighbour discovery. The Neighbour Advertisement (NA) and Neighbour Solicitation (NS) occur in IPv6 host. The Address Resolution Protocol (ARP) is used in IPv4 whereas ICMPv6 is used for Address Resolution in IPv6. IPv6 does not support Duplicate Address Detection (DAD) because of which more than one device can use same IP address which may result in DDoS Attack.

2. Conclusion

As per the present scenario and study, it is quite clear that future of IP addressing is IPv6. The reason behind

transition from IPv4 to IPv6 is not the security issues. IPv4 is found to be fully secure and offers security from various network attacks. It is fully integrated in the present networking. The only reason for migration to IPv6 is the exhaustion of IP addresses in IPv4. With the study of security issues between IPv4 and IPv6 it is concluded that the issues largely remains the same. Various attacks of IPv4 can also be applied on IPv6. Only the attack behaviour and type of attack is changed. As per the study, the packet transport techniques, upper layer and application layer protocols are not affected at all[4].

In the newer version IPv6, IPSec is compulsory to make the network secure. The data communicated between network nodes is encrypted and no network policy can be applied on it. The new operating system supports IPv4 and IPv6 and user do not even realize any change in working. The IPv4 security threats also exist for IPv6 and even have increased. The attacks also have newer versions and only attack behaviour is changed. The Layer 2 security where provides security in IPv6 has also make the attacks like Man in the Middle possible for IPv6[14].

3. Future Scope

IPv6 is a very innovative and feature rich internet protocol. It is still in its infancy stage. The ip address numbering has already solved the issues of IP draught in IPv4 and have enough IP address to cater the ever increasing demands of IP addressing for future years. Although the IPv6 based applications are not fully bug free and network security is not very much convincing but ti is quite sure that with time IPv6 will be adopted in the corporate networking within a span of few years. The network security will be enhanced and new strategies will be implemented to make the IPv6 a much secure and feature rich internet protocol.

Acknowledgements and References

[1] Emre Durda, Ali Buldu, (2010), “IPV4/IPV6 security and threat comparisons”, *Technical Education Faculty, Marmara University, Istanbul, 34722, Turkey*, Procedia Social and Behavioral Sciences 2 (2010) 5285–5291.
[2] Nokia Siemens Networks, (2012), “Migrating to IPv6 Opportunity or threat for network security?” Copyright © 2012. All rights reserved.
[3] Emin Çalışkan, (2014), “IPv6 Transition and Security Threat Report”, CCDCOE, NATO Cooperative Cyber Defence, Centre of Excellence, Tallinn, Estonia.
[4] Government of the HKSAR, (2011), “IPv6 Security”, © The Government of the Hong Kong Special Administrative Region.
[5] Rohit Bothra, Dilip Sai Chandar, Network Consulting Engineer, Cisco (2012), “IPv6 Security Threats and Mitigations”, APRICOT.
[6] Bhavya Daya, (2008), “Network Security: History, Importance, and Future”, University of Florida Department of Electrical and Computer Engineering.
[7] R. L. Mitchell. The grill: John Curran. Computer-World, Apr. 2010.
[8] G. Huston, Geo Huston http://www.potaroo.net/tools/ipv4/index.html, DEC. 2013.
[9] Google Statistics, www.google.com/intl/en/ipv6/statistic.html,2012.
[10] BGP Analysis Reports Retrieved, Jan 2014.
[11] J. Rajahalme, A. Conta, B. Carpenter, S. Deering, IPv6 Flow Label Specification,, RFC3697 March 2004.
[12] P. Nikander, J. Kempf, E. Nordmark, IPv6 Neighbor Discovery (ND) Trust Models and Threats, RFC 3756, May 2004.
[13] S. Kent, K. Seo, Security Architecture for the Internet Protocol, RFC4301, December2005.
[14] Conta, S. Deering, M. Gupta, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 4443, March 2006.
[15] T. Narten, E. Nordmark, W. Simpson, H. Sliman, Neighbor Discovery for IP version 6 (IPv6), RFC 4861, September 2007.
[16] NMAP.Org, NMAP IPv6 Tool, Retrieved 2013.
[17] Cisco, Understanding and configuration DHCP snooping, December 2012.
[18] CISCO, IPv6 Breif, White Paper, Oct 2011.
[19] T. Chown, S. Venaas, Rogue IPv6 Router Advertisement Problem Statement, RFC6104, Feb. 2011.
[20] E. Vyncke, S. Hogg, IPv6 Internet Security for Network, Cisco Press, JUN 2009.
[21] C. Kaufman, P. Hoffman, P. Eronen, Internet key Exchange Protocol Version 2 (IKEv2), RFC 5996, SEPTEMBER 2010.
[22] T. Chown, S. Venaas, Rogue IPv6 Router Advertisement Problem Statement, RFC6104, Feb 2011.
[23] C. Kaufman, Y. Nir, P. Eronen, Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, Sep. 2010.
[24] H. Eltaj, F. Najjar, H. Alsenawi, M. Najjar, Intrusion Detection and Prevention Response based on Signature-Based and Anamoly-Based: Investigation Study, International Journal of Computer Science and Information Security, June 2013
[25] NMAP.org, Network Mapper, May 2012.
[26] Thc.org, thc-ipv6, Dec 2013.
[27] Supriyanto, Iznan Husainy Hasbullah, Raja Kumar Murugesan and Sureswaran Ramadass, "Survey of Internet Protocol Version 6 Link Local Communication Security Vulnerability and Mitigation Methods", Vol 30, no 1, pp 64-71, Jan-Feb 2013.
[28] Ala Hamarsheh, "Assuring Interoperability between Heterogeneous (IPv4/IPv6) Networks without using Protocol Translation", Vol 29, no 2, pp.114-32, Mar-Apr 2012