IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Migration Techniques And Security Issues Of Ipv6

Prabhjot Kaur[1], Charanpreet Kaur[2]

[1]Assistant Professor, Department of Computer Science and Engineering, Chandigarh University

[2]Assistant Professor, Department of Computer Science and Engineering, Chandigarh University

Abstract

At different rates in different parts of the world, the next-generation Internet protocol, IPv6, is inching its way toward adoption[13]. IPv6 (Internet Protocol version 6) is the latest revision of the Internet Protocol (IP) protocol that is designed to solve the problem of the current Internet Protocol version 4 (IPv4) depletion[14]. The purpose of this paper is to accelerate the adoption of IPv6 by highlighting the benefits of it compared to IPv4. It also includes migration mechanism from IPv6 to IPv4 and security issues involved.

Keywords: IPv6, IPv4, NAT.

Introduction

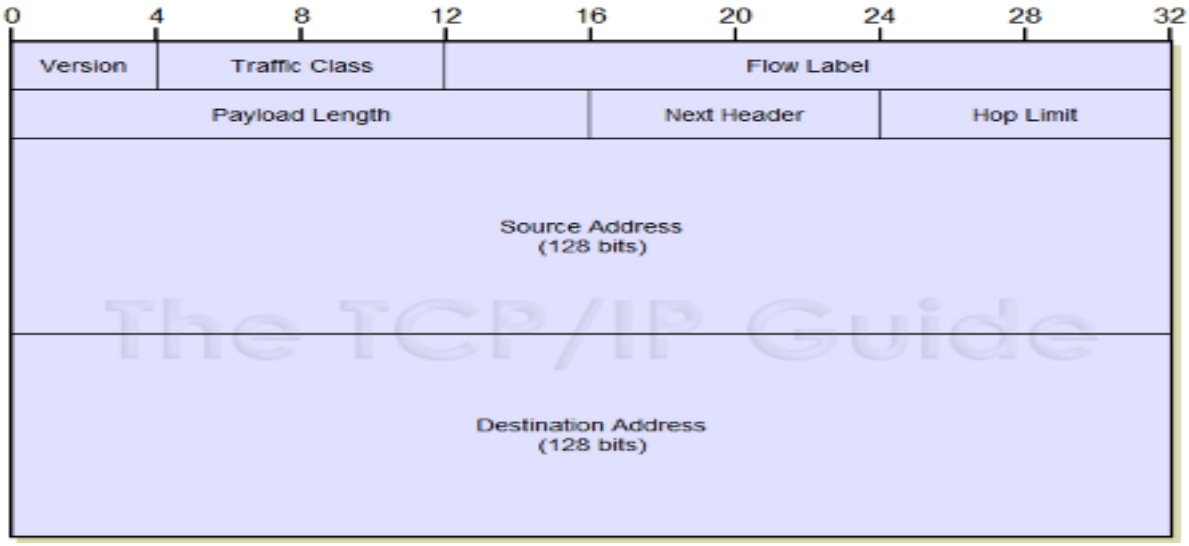
The Internet Protocol is a network-layer protocol in the OSI model[16] which contains addressing information and some control information that enable packets to be routed in a network. Internet Protocol has two primary responsibilities: providing connectionless, best-effort delivery of datagram's through a network; and providing fragmentation and reassembly of datagram's to support data links with different maximum-transmission unit (MTU) sizes. Each IP address has specific components and follows a basic format. Each computer (known as host) on a TCP/IP network is assigned a unique logical address (32-bit in IPv4) that is divided into two main parts: the network number and the host number.

The network number identifies a network and must be assigned by the Internet Service Provider (ISP). The host number identifies a host on a network and is assigned by the local network administrator. It is to be noted that IPv4 was designed with no security feature in mind, because it is assumed that security should be provided by the end nodes. This is because in IPv4, IPSec which is a security feature is optional, unlike in the new internet protocol IPv6 where IPSec is a mandatory feature[1].

The new standard protocol for the Internet, Internet Protocol version 6 (also known as IPv6), which is the next step beyond IPv4, the current standard protocol for the Internet. These protocols provide IP addresses, the "phone numbers" for the Internet that are responsible for identifying computers and devices so that they can communicate. IPv6 is designed to solve many of the problems of IPv4, including mobility, auto-configuration, and overall extensibility. IPv6 expands the address space on the Internet and supports a nearly unlimited number of devices that can be directly connected to the Internet.

IPv6

IPv6 is the replacement for IP version 4 (IPv4), the Internet layer protocol of the TCP/IP protocol stack in prevalent use around the world today. IPv6 solves many of the problems and shortcomings of IPv4, providing an Internet layer protocol that can scale to the future needs of devices that will connect to the Internet[14].



IPv6 Benefits

With IPv6, everything from appliances to automobiles can be interconnected. But an increased number of IT addresses isn't the only advantage of IPv6 over IPv4. In honor of World IPv6 Day, here are some more good reasons to make sure your hardware, software, and services support IPv6. These are as follow: -[3]

- **More Efficient Routing:** -IPv6 reduces the size of routing tables and makes routing more efficient and hierarchical. In addition, in IPv6 networks, fragmentation is handled by the source device, rather than the router, using a protocol for discovery of the path's maximum transmission unit (MTU).
- **More Efficient Packet Processing:** -IPv6's simplified packet header makes packet processing more efficient[19]. Compared with IPv4, IPv6 contains no IP-level checksum, so the checksum does not need to be recalculated at every router hop. Getting rid of the IP-level checksum was possible because most link-layer technologies already contain checksum and error-control capabilities[20].
- **Directed Data Flows:** -IPv6 supports multicast rather than broadcast. Multicast allows bandwidth-intensive packet flows (like multimedia streams) to be sent to multiple destinations simultaneously, saving network bandwidth. Disinterested hosts no longer must process broadcast packets. In addition, the IPv6 header has a new field, named Flow Label that can identify packets belonging to the same flow[19].
- **Simplified Network Configuration: -** Address auto-configuration (address assignment) is built in to IPv6. A router will send the prefix of the local link in its router advertisements. A host can generate its own IP address by appending its link-layer (MAC) address.
- **Larger addresses:** - From 32 bit address space in IPv4 to 128 bit address space of IPv6. It enables all nodes to be addressable and reachable, removing the need for network address translation and restoring the end-to-end model for end-to-end capabilities such as security[20].
- **Support for New Services**: - By eliminating Network Address Translation (NAT), true end-to-end connectivity at the IP layer is restored, enabling new and valuable services[18]. Peer-to-peer networks are easier to create and maintain, and services such as Quality of Service (QoS) become more robust.
- **Security: -** IPSec, which provides confidentiality, authentication and data integrity, is baked into in IPv6. Because of their potential to carry malware, IPv4 ICMP packets are often blocked by corporate firewalls, but ICMPv6, the implementation of the Internet Control Message Protocol for IPv6, may be permitted because IPSec can be applied to the ICMPv6 packets.

The Migration from IPv4 to IPv6

Migrating from IPv4 to IPv6 in an instant is impossible because of the huge size of the Internet and of the great number of IPv4 users. Moreover, many organizations are becoming more and more dependent on the Internet for their daily work, and they therefore cannot tolerate downtime for the replacement of the IP protocol. As a result, there will not be one special day on which IPv4 will be turned off and IPv6 turned on because the two protocols can coexist without any problems. The migration from IPv4 to IPv6 must be implemented node by node by using auto configuration procedure to eliminate the need to configure IPv6 hosts manually[18][4].

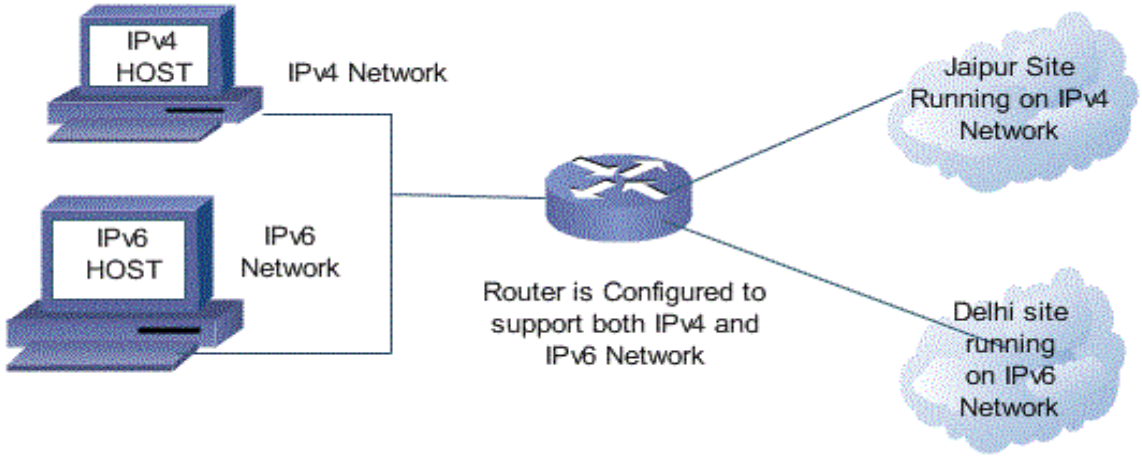
The key goals of the migration are as follow:-

- IPv6 and IPv4 hosts must interoperate.
- The use of IPv6 hosts and routers must be distributed over the Internet in a simple and progressive way, with a little interdependence.
- Network administrators and end users must think that the migration is easy to understand and implement.

There are several migration approaches provided to manage the migration and support both IPv4 and IPv6 protocols in parallel during the transition. We introduce a few important ones in this section[20].

1. Dual Stacking

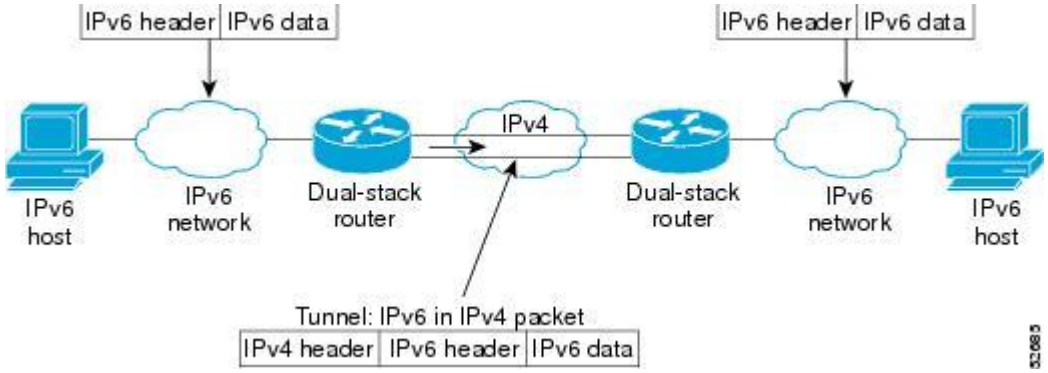
In dual stacking, a device runs both protocol stacks: IPv4 and IPv6. Of all the transition methods, this is the most common one. Dual stacking can be accomplished on the same interface or different interfaces of the device. Figure shows an example of dual stacking on a router, where Network has a mixture of devices configured for the two different protocols and the router configured in a dual stack mode. This transitional mechanism is relatively easy to implement. Both protocols co-exist and hence, there is no problem supporting older and newer applications that use IPv4 and IPv6 respectively. The disadvantage of this approach is that the devices have to support both versions and they need extra processing power (memory, CPU etc.) to handle both protocols. There is also inefficient use of bandwidth[5].



2.Tunnels

Tunneling uses encapsulation to carry IPv6 traffic in IPv4 packets and vice versa. This allows for a partial transition where portions of the network can migrate to IPv6 while the rest of the network remains in its original state.

Tunneling can be used in a variety of ways, such as: Router-to-Router, Host-to-Router, Host-to-Host and Router-to-Host. Tunneling techniques are also classified according to the mechanism by which the encapsulating node determines the address of the node at the end of the tunnel. In router-to-router or host-to-router methods, the IPv6 packet is tunneled to a router. In host-to-host or router-to-host methods, the IPv6 packet is tunneled all the way to its final destination[16][4].

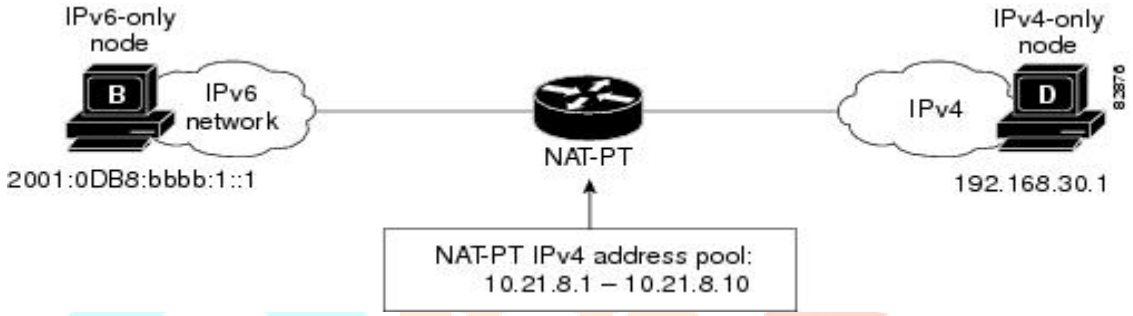


The advantage of tunnels is that you can reuse the existing infrastructure in situations where old devices do not have enough processing power to support both protocols or you are not ready or financially able to upgrade. The disadvantage of tunneling is that it involves tedious configuration. Tunnel endpoints need extra processing power to handle encapsulation and decapsulation. Tunnels can create routing inefficiencies if they are not configured to match the underlying routing topology. Tunnels also introduce security issues, as packets that were previously visible are now encapsulated. Troubleshooting within the tunnel is difficult due to the lack of visibility into the end-to-end traffic paths[18].

There are two types of tunnels: static and dynamic. Static tunnels are created manually. Dynamic tunnels use several techniques to automatically define the endpoints. Dynamic tunnels involve fewer configurations than static tunnels. However, they create IPv4 address bindings (when the tunnel endpoints are derived directly from IPv4 addresses). Providing redundancy with dynamic tunnels is also a challenge[5].

1. Translation

This is one of ways to facilitate interworking between IPv4 and IPv6 by putting address translator between two different versions of IP networks. Translation lets you convert packets from one protocol to another[]. The goal is to provide transparent routing for nodes in IPv6 networks to communicate with nodes in IPv4 networks and vice versa. The NAT (Network Address Translation) gateway uses a pool of globally unique IPv4 addresses and binds them to IPv6 addresses. No changes to the end nodes are necessary. The advantage of this approach is that it allows for communication between devices supporting any version. However the disadvantage is that the translator has to read every packet header and this requires extra processing power. Configuration of the translator is tedious. The translator also becomes a single point of failure.



Security Issues

Prior to migration or co-existence with IPv6, an understanding of its security implication is necessary to avoid worries or un-acceptance among users or decision makers. We need to prepare the network users against the possible threats or attacks that may affect the network and its resources. Prior to that, we need a better understanding in order to come up with a comprehensive and enforceable security policy for the network.

Header Manipulation Issues

The use of extension headers and IPSec can deter some common sources of attack based on header manipulation. However, the fact that extension headers must be processed by all stacks can be a source of trouble. A long chain of extension headers could be used to overwhelm certain nodes (e.g. firewalls) or masquerade an attack. Best practices recommend for filtering out traffic with unsupported services [16][9]. Spoofing continues to be a possibility in IPv6 networks. However, because of Neighbour Discovery (ND), spoofing is only possible by nodes on the same network segment. The same does not apply to 6 to4 transition networks. Although one approach to 6 to 4 transition is using some form of dual-stack functionality, another approach is using some type of tunneling. Because tunneling requires that a protocol is encapsulated in another, its use could be a source of security problems such as address spoofing [10].

Flooding Issues

In IPv6 networks, scanning for valid host addresses and services is far more challenging than in IPv4 networks. Because the address space is 64 bits, scanning an entire IPv6 segment might take up to 580 billion years. One may believe that this would avoid flooding, but they would be mistaken. Because, the wider addressing space does not mean that IPv6 is fully invulnerable to this type of attack. IPv6 is also more secure due to the lack of broadcast addresses. Multicast addresses, for example, continue to be a source of issues [11]. Multicast traffic is still vulnerable to Smurf-style assaults. Filtering out unwanted traffic is the recommended best practise once again [16][9].

Dual Stack

Most networks need to be dual-stacked. As IPv4 and IPv6 cannot communicate with each other, they will need to be deployed until the transition phase is complete, which could take many years. So, for the period during which you offer both IPv4 and IPv6, you have to do everything twice, including security. In most cases, settings will not be automatically copied between IPv4 and IPv6, so whenever you make a change for one protocol you have to do it for the other, which doubles the chances of making a mistake. Applications may also switch on IPv6 unintentionally, without it being clear to the operator. For example, while enabling web server software for IPv6, the management

package in the background might also run IPv6 and enable itself. Planning is needed to ensure that either the firewall filters are in place or that the software is configured to behave correctly[15].

Mobility

This is a totally new feature of IPv6 that was not available in IPv4. Mobility is a very complex function that raises a considerable amount of concern when considering security. Mobility uses two types of addresses, the real address and the mobile address. The first is a typical IPv6 address contained in an extension header. The second is a temporary address contained in the IP header. Because of the characteristics of this networks (something more complicated if we consider wireless mobility), the temporary component of a mobile node address could be exposed to spoofing attacks on the home agent. Mobility requires special security measures and network administrators must be fully aware of them[12].

Conclusion

The goal of approaching the public about the key position of IPv6 addresses and the want to have of migrating to IPv6 through the media is difficult to achieve because people's lack of understanding about IPv6 makes it difficult to persuade them to adopt. When compared to the IPv4 protocol stack, IPv6 is a significant advance. The new protocol suite adds a slew of additional features to the user experience as well as certain specialised security functions. The network's migration/coexistence of IPv4 and IPv6 has raised major security concerns, prompting us to prepare with appropriate security mechanisms. During the migration period, we highlighted potential security concerns[16].

References

[1] Ibikunle Frank. A., Transition Techniques of the Future Internet Protocol-IPv6, American Journal of Scientific Research, 2011.
[2] IPv6 Header Format “http://www.tech republic.com”.
[3] Benefits of IPv6 “http://www.network computing.com”.
[4] The Migration from IPv4 to IPv6, 56982_CH12I, “http://www.ip6.com”.
[5] Opnet Technologies Inc., “IPv6 Migration Planning”, White Paper, 2007, “http//www.opnet.com”.
[6] Dual Stack “http://computer networking notes.com”.
[7] Tunnel “http://www.cisco.com”.
[8] Translation “http://www.cisco.com”.
[9] Popoviciu, C; Levy-Avegnoli, E; Grossetete, P; deploying IPv6 networks, Cisco press, Indianapolis, IN, 2006.
[10] Szigeti, S; Risztic, P; “Will IPv6 bring better security?” proceedings 30th envomicro conf, 2004.
[11] Vives, A, Palet, J; “IPv6 distributed security problem statement” the 2005 symposium on applications and the internet workshops.
[12] “http://www.esecurityplanet.com”.
[13] Jain, N., Payal, A., “Performance Comparison Between Different Tunneling Techniques Using Different Routing Protocols”, Wireless Personal Communications, 2022, 123 (2), pp. 1395-1441.
[14] Ahmed, M.R.A., Shaikhedris, S.S.A., “Network Migration and Performance Analysis of IPv4 and IPv6”, Proceedings of : 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering, ICCCEEE 2020, DOI: 10.1109/ICCCEEE49695.2021.9429664.
[15] Cv, R.K., Goyal, H., “ IPv4 to IPv6 Migration and Performance Analysis using GNS3 and Wireshark”, International Conference on Vision Towards Emerging Trends in Communication and Networking, 2019, DOI: 10.1109/ViTECoN.2019.8899746.
[16] Briscoe, N. (2000). Understanding the OSI 7-layer model. PC Network Advisor, 120(2), 13-15.
[17] Siddika, F., Hossen, M.A., Saha, S., “Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow”, Proceedings of 2017 International Conference on Networking, Systems and Security, 2017, DOI: 10.1109/NSysS.2017.7885821.
[18] Terli, V.K.K., Chaganti, S.P., Alla, N.B., Sarab, S., El Taeib, T., “Software implementation of IPv4 to IPv6 migration”, IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016, DOI: 10.1109/LISAT.2016.7494160.

[19] Wu, Y., Zhou, X., "Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition", ICCSE 2011 - 6th International Conference on Computer Science and Education, 2011, pp. 1091-1093, DOI: 10.1109/ICCSE.2011.6028824.
[20] Nowicki, K., Stankiewicz, M., Mrugalska, A., Woźniak, J., Mrugalski, T., "Extension management of a knowledge base migration process to IPv6", Proceedings - 11th IEEE/IPSJ International Symposium on Applications and the Internet, 2011, pp. 497-501, DOI: 10.1109/SAINT.2011.92.