Volume 4, Issue 11, November 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A study of IPv4 and IPv6 features

Rajinder Singh
Department of Computer Science and Applications
Panjab University S.S.G. R.C. Hoshiarpur,
Punjab, India

Abstract—Internet Protocol (IP) is widely used on the internet. It is one of the major protocols in TCP/IP protocol suite. It is used to identify each host on the network through logical addresses. Nowadays there are two versions of internet protocol, Ipv4 (Internet protocol version 4) and Ipv6 (Internet protocol version 6). IPv6 is the latest (sixth) revision to the Internet Protocol and it is the successor to IPv4. In this paper a comparative study between the various features of both has been made.

Keywords: Internet Protocol; Ipv4; Ipv6ng; any cast; multicast IPSec;

I. INTRODUCTION

A computer network is a group of two or more than two computer systems which are linked through communication channels (wired or wireless) to facilitate communication, resource sharing and exchanging of data. In computer network majority of the communication takes place with the help of Internet Protocol (IP). Internet protocol is used to identify each host on the network through logical address. Every node on the network has a unique identifying number called an IP Address. It also specifies the technical format of the packets which are routed from source to destination across the network. The Internet Protocol (IP) is the primary protocol in the Internet protocol suite used for transferring packets across the network. The main function of Internet Protocol is addressing the hosts and routing packets across one or more IP networks. Currently there are two versions of internet protocol. IPv4 (Internet protocol version 4) and IPv6 (Internet protocol version 6). IPv6 is successor to IPv4 [1].

II. IPV4

IPv4 protocol works at Network layer of OSI model and at Internet layer of TCP/IP model. This protocol is responsible for identification of hosts by their logical addresses [2]. Internet Protocol Version 4 (IPv4) is the fourth revision of the internet protocol (IP) and it is widely used in data communication over different kinds of networks. It is a connectionless protocol and is used on packet switch internetworks. This protocol transports data in packets called datagram [3]. IPv4 is defined and described in IETF publication RFC 791 (September 1981). It is based on best effort delivery model, means it provides no error checking or tracking that the packets will be delivered to destination host. These aspects are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP). IPv4 uses 32-bit address scheme, so total number of addresses on the internet are limited to 4294967296.

Main limitations of IP are:

i) Due to the rapid growth of internet in last few years and increased number of internet devices has caused the exhaustion of the IPv4 addresses.

ii) Earlier during the development of IPv4 a very little attention was given to the security [4].

III. IPv6

IPv6 (Internet Protocol Version 6) is successor to Internet Protocol Version 4 (IPv4). It is also called IPng (Internet Protocol next generation).

Main features of Ipv6 are:

i) Larger Address Space:

IPv6 addresses are 128-bits long as compared to IPv4 address (32 bit address). The very large IPv6 address space allows a better systematic, hierarchical allocation of addresses to the hosts [5].

ii) New Packet Format:

IPv6 specifies a new packet format which is much simpler than IPv4 Header. IPv6's header is very simple as compared to IPv4 Header. It is achieved by moving all unnecessary and optional fields to the end of IPv6 header. This simplified header makes Router to take routing decision very quickly [6]. Due to the difference between IPv4 and IPv6 these two protocols are not interoperable.

iii) State full and Stateless IPv6 address configuration:

IPv6 supports both state full or stateless auto configuration. In case of stateless configuration addresses are derived from the receipt of router advertisement packet. These packets contain stateless address prefixes. In case of state full configuration the hosts use Dynamic Host Configuration Protocol version 6 (DHCPv6) to obtain the addresses and other necessary configuration parameters.

iv) Anycast:

In case of IPv4 there are three types of communication are available, unicast, multicast and broadcast. In case of unicast there is one to one communication between the nodes, in case of multicast there is one to many communication and in broadcast there is one to all communication. In case of IPv6 Broadcast communication is not available [5]. In case of IPv6 there is new kind of communication is available called anycast. In this case multiple interfaces are assigned same Anycast IP address on the internet [6].

v) Internet Protocol Security (IPSec):

Internet Protocol Security (IPSec) was optional in IPv4 but it is mandatory in IPv6 making it more secure than IPv4 [6].

IV. SECURITY IN IPV4

Due to early stage of data communication IPv4 was created for delivering data and attention was given to security. IPv4 does not have a built in security protocol. Main security threats that can be made on IPv4 are:

i) Denial of Service attack (DOS)

In denial-of-service attack an attacker makes an attempt to make a computer or network's resources unavailable for legitimate users. Main resources which are affected by DOS attacks are computer system resources for example CPU and bandwidth of network.

ii) Man In the Middle Attack (MITM)

In this type of attack an attacker is able to read, modify and insert malicious data between the two communicating hosts without either host knowing this.

iii) Fragmentation Attack

Fragmentation means breaking an IP datagram into smaller packets and then transmitting these smaller packets over different networks and then reassembling them at the other end. A fragmentation attack is an attempt to deny access to a computer or network by transmitting small fragmented ICMP datagrams.

iv) ARP poisoning Attack

In this type of attack attacker send fake or spoofed ARP messages to a network. Attacker associates its MAC address with the IP address of another node on the network. So now any traffic sent for that IP address would be sent to the attacker instead [7].

Many of the attacks can be avoided by using IPSec protocol, but use of IPSec in IPv4 is optional. IPSec provides security by encrypting data and authenticating all IP packets [8].

V. SECURITY IN IPV6

The use of IPSec in IPv6 is not optional, but mandatory as compared to IPv4. IPSec protocol consists of a set of cryptographic protocols for providing security. IPSec provides communication security by authentication and encrypting IP packets.

1) Mandatory use of Internet Security Protocol (IPSec): IPSec suite is publicly available and it provides security across the network through following protocols.

a) Authentication Header (AH)

AH provides data integrity and authentication for IP datagrams. Authentication means that IP packet received from the network is originated from a valid IP address.

Integrity of data means that the content of that data has not been changed from the source to the destination across the network. This protocol also provides protection against replay attacks.

b) Encapsulating Security Payloads (ESP) provide confidentiality, authentication, and data integrity.

c) Security Associations (SA) provides the bundle of algorithms and data that provide the necessary keys to support secure communication [9].

2) Large Addressing Space:

IPv6 has 128 bit source and destination addresses whereas in case of IPv4 source and destination addresses are of 32 bit.

Therefore in case of IPv4 port scanning is very simple task. But in case of IPv6 due to large addressing space port scanning is very difficult.

3) Neighbor Discovery:

Use of ND (Neighbor Discovery) protocol makes IPv6 more secure than its predecessor [10].

VI. MAIN DIFFERENCES BETWEEN IPV4 AND IPV6

Addresses:

The IPv4 addresses are only 32 bits long, but IPv6 addresses are 128 bits long.

Address Configuration:

IPv6 supports both stateful and a stateless address configuration mode. In case of IPv6 Stateful address configuration is done similar as by DHCP in IPv4. But IPv6 also supports Stateless Address Auto Configuration (SLAAC).

In this mode, nodes can automatically configure their network configuration without any user interaction.

ICMP:

ICMP protocol is an important part of IPv6. Besides the basic ICMP messages which are used in IPv4, IPv6 also provides some new ICMP messages. For example Neighbor Discovery (ICMP Types 135 & 136) and Router Discovery (ICMP Types 133 & 134) messages are used to support neighbor discovery instead of ARP functionality of IPv4.

IPv6 Packet Structure:

An IPv4 packet consists of two parts i) header section and ii) data section. In IPv4 there are total 14 fields. The 13 fields are required by IPv4 but the 14th one is optional [4]. An IPv6 header is fixed in size and it consists of 320 bits [18].

Multicast:

Multicast is a feature used by IPv4 but IPv6 uses anycast feature [11].

Efficient Routing:

Using IPv6 protocol reduces the size of routing tables and makes routing more efficient as compared to IPv4[12].

Quality of Service:

Quality of the service of a network depends upon various parameters such as bandwidth, throughput, transmission delay and jitter, etc.[13].

In case of IPv4 Quality of Service is limited and it is achieved through Type of Service field. But in case of IPv6 Quality of service can be achieved through Flow Label field and Traffic Class Field [14].

NAT (Network Address Translation):

In case of IPv6 Network address translation is not commonly used because IPv6 provides true host-to-host connectivity [15]. But NAT is necessary in IPv4 when the number of IP addresses assigned by Internet Service Provider is less than the total number of computers wishing for the internet access [16].

Simple Header Format:

IPv6 header design is very simple as compared to IPv4. Ipv6 header is fixed in size (40 bytes). Due to its fixed size its processing at routers is very efficient as compared to IPv4 [17].

VII. CONCLUSIONS

Due to sudden growth of the Internet users, increased number of internet devices and increase in internet facilities caused exhaustion of IP addresses problem in IPv4. But this problem can be resolved by using IPv6. IPv6 is the successor to IPv4. In terms of security also IPv4 is not as much secure as compared to IPv6. Mandatory use of IP Security (IPSec) in the IPv6 protocol makes IPV6 more secure than the IPv4.

REFERENCES

[1] http://en.wikipedia.org/wiki/Internet_Protocol
[2] http://www.tutorialspoint.com/ipv4/ipv4_tcpip_model.htm
[3] http://www.techopedia.com/definition/5367/internet-protocol-version-4-ipv4
[4] http://en.wikipedia.org/wiki/IPv4
[5] http://www.omnisecu.com/tcpip/ipv6/ipv6-features.php
[6] http://www.tutorialspoint.com/ipv6/ipv6_features.htm
[7] http://www.brucert.org.bn/files/IPv6-to-IPv4%20Transition%20&%20Security%20Issues.pdf
[8] http://ipv6security.wikia.com/wiki/IPv4_vs._IPv6
[9] http://en.wikipedia.org/wiki/IPsec
[10] http://resources.infosecinstitute.com/ipv6-security-overview-a-small-view-of-the-future
[11] http://www.gogo6.com/group/IPv6News/page/major-differences- between-ipv6-and
[12] http://www.networkcomputing.com/networking/six-benefits-of-ipv6/d/d-id/1232791?
[13] http://en.wikipedia.org/wiki/Quality_of_service
[14] http://what-when-how.com/ipv6-for-enterprise-networks/quality-of-service-qos-ipv6/
[15] http://en.wikipedia.org/wiki/Network_address_translation
[16] http://www.openbsdindia.org/faq/pf/nat.html
[17] http://www.h3c.com/portal/products___solutions/technology/ipv4___ipv6_services/technology_introduction/200702/201238_57_0.htm
[18] http://en.wikipedia.org/wiki/IPv6_packet

