Comparative Analysis between Internet Protocol Version 4 & 6 (IPv4 and IPv6)

Aluko T.S, Olusanya O.J, Oloyede O.E , Ebisin A.F

Abstract— IP protocol was first proposed in 1974 in a research paper by Vinton G . Cerf and Robert E. kahn . Internet Protocol Version 4 (IPv4) which was developed almost three decades ago is the mostly prevalent protocol version in use today. However, due to the rapid and ubiquitous growth of internet and increase in number of connected devices we are facing a scenario where IPv4 address are essentially exhausted . The IPv4 extensions such as Network address translation (NAT), Classless Inter-Domain Routing (CIDR) etc are merely limited short-term solution. Moreover the scalability and security features that are required by the modern Internet cannot be fully provided by IPv4. The long term solution of these problems is a step-by-step, phased but complete migration to IPv6. While IPv4 address space can hold billions of address, IPv6, which is the next version of the protocol, has provided trillions of addresses which are potentially inexhaustible.

The primary focus of this write up is to compare and analyze IPv4 and IPv6 networks, study their characteristics and header formats. The write up also attempts to outline the key deployment issues and security –related challenges which are being faced and dealt with during the migration process

Keywords: Ipv4, Ipv6, Internet Protocol, Network address translation (NAT),Classless Inter-Domain Routing (CIDR), Security, Header.

1.0 Introduction

Internet is a global system of interconnected computer networks that use the standard internet protocol suite {TCP/IP} to link several billion devices worldwide. The Internet is not just at the center of today's mass market consumer service enterprise, it is now at the heart of many aspects of our lives. It's not just the current fads of the social networking tools, but so much more. How we work; how we buy and sell even what we buy and sell; how we are entertained; how democracies function, even how our societies are structured; and so much more—all of these activities are mediated by the Internet.

Internet protocol is defined as the format or means used in the linking of billions of devices worldwide over the internet for the enablement of sharing and transmitting of data's and information.

It has been responsible for the addressing hosts and for routing datagram's {packets} from the source host (the sender} to the destination host {the receiver} across one or more IP networks.

This paper work will majorly discuss on the first major version of IP, internet protocol version 4 {IPv4} to its successor internet protocol version 6{IPv6} since they are the two advancement of internet protocol in the technology.

IPv4 is the fourth version in the development of the internet protocol {IP} internet and routes most traffic on the internet.IPv4 is a connectionless protocol for use on packet-switched networks. It operates on the best effort delivery model; in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery.

IPv6 is the successor of the IPv4 .it was originally abbreviated as SIPP {Simple Internet Protocol Plus}, the sixth version of the Internet protocol which is now known as IPv6 is the latest version of the internet protocol {IP}. It's the communication that provides an identification and location system for computers on the networks and routes traffic across the Internet. IPv6 was developed by the internet Engineering Task Force {IETF} to deal with the long-anticipated problem of IPv4 address exhaustion.

Comparatively IPv4 and IPv6 technical functioning of the Internet remains the same with both versions and it is likely that both versions will continue to operate simultaneously on networks well into the future. To date, most networks that use IPv6 support both IPv4 and IPv6 addresses in their networks.

The major difference between IPv4 and IPv6 is the number of IP addresses and their space. There is 4,294,967,296IPv4 addresses. In contrast, there are 340,282,366,920,938,463,463,374,607,431,768,211,456 IPv6 addresses. Obviously proving that with the advancement in technology towards the future IPv6 is a best option to be fully used.

2.0 Functions of Internet Protocols

1. **Addressing:** In order to perform the job of delivering datagram's, IP must know where to deliver them to! For this reason, IP includes a mechanism for host addressing. Furthermore, since IP operates over internetworks, its system is designed to allow unique addressing of devices across arbitrarily large networks. It also contains a structure to facilitate the routing of datagram to distant networks if that is required.
2. **Data Encapsulation and Formatting/Packaging:** As the TCP/IP network layer protocol, IP accepts data from the transport layer protocols UDP and TCP. It then encapsulates this data into an IP datagram using a special format prior to transmission.
3. **Fragmentation and Reassembly:** IP datagrams are passed down to the data link layer for transmission on the local network. However, the maximum frame size of each physical/data-link network using IP may be different.
4. **Routing / Indirect Delivery:** When an IP datagram must be sent to a destination on the same local network, this can be done easily using the network's underlying LAN/WLAN/WAN protocol using what is sometimes called *direct delivery*. IP accomplishes this in concert with support from the other protocols including ICMP and the TCP/IP gateway/routing protocols such as RIP and BGP.

2. 1 Characteristics of Internet Protocol

Of course there are a myriad of ways in which IP could have been implemented in order to accomplish this task. To understand how the designers of TCP/IP made IP work; let's take a look at the key characteristics used to describe IP and the general manner in which it operates. The Internet Protocol is said to be:

1. **Universally-Addressed**

In order to send data from point A to point B, it is necessary to ensure that devices know how to identify which device is "point B". IP defines the addressing mechanism for the network and uses these addresses for delivery purposes.

2. **Underlying-Protocol Independent**

IP is designed to allow the transmission of data across any type of underlying network that is designed to work with a TCP/IP stack. It includes provisions to allow it to adapt to the requirements of various lower-level protocols such as Ethernet or IEEE 802.11. IP can also run on the special data link protocols SLIP and PPP that were created for it. An important example is IP's ability to fragment large blocks of data into smaller ones to match the size limits of physical networks, and then have the recipient reassemble the pieces again as needed.

3. **Delivered Connectionless**

IP is a connectionless protocol. This means that when

4. **Delivered Unreliably**

IP is said to be an "unreliable protocol". That doesn't mean that one day your IP software will decide to go fishing rather than run your network. □ It does mean that when datagrams are sent from device *A* to device *B*, device *A* just sends each one and then moves on to the next. IP doesn't keep track of the ones it sent. It does not provide reliability or service quality capabilities such as error protection for the data it sends (though it does on the IP header), flow control or retransmission of lost datagrams.

5. **Delivered Without Acknowledgments**

In a similar manner to its unreliable nature, IP doesn't use acknowledgements. When device *B* gets a datagram from device *A*, it doesn't send back a "thank you note" to tell *A* that the datagram was received. It leaves device *A* "in the dark" so to speak

.

3.0 VERSIONS OF TCP/IP

The IP defined in RFC 791 was the first widely-used version of the Internet Protocol. Interestingly, however, it is not version 1 of IP but version 4! This would of course imply that there were earlier versions of the protocol at one point. Interestingly, however, there really weren't. As we mentioned above, IP was created when its functions were split out from an early version of TCP that combined both TCP and IP functions. TCP evolved through three earlier versions, and was split into TCP and IP for version 4. That version number was applied to both TCP and IP for consistency

Internet Protocol Version 4 (IPv4) Datagram Format*: This diagram shows graphically the all-important IPv4 datagram format. The first 20 bytes are the fixed IP header, followed by an optional Options section, and a variable-length Data area. Note that the Type Of Service field is shown as originally defined in the IPv4 standard.*

3.1 BENEFITS OF IPV4

In the last few years the number of web users increased and this has cause the onset of challenges for service providers, stack holders and management goods., internet infrastructure is expanding everyday due to advancement in technology, which means we now have the opportunity to enjoy web services even in the remote areas. The IPV4 internet protocol addressing was designed to be more palatable but it soon expected to become extinct due to the increasing number of internet users and devices.

1. Reliable Security

When you want to communicate to other users via a public medium it is important to encrypt the information to uphold privacy and security. With advancement in technology, we now have a reliable security measures for IPV4 address packet. Internet protocol security allows data encryption to maintain privacy and security.

2. Large Routine Task

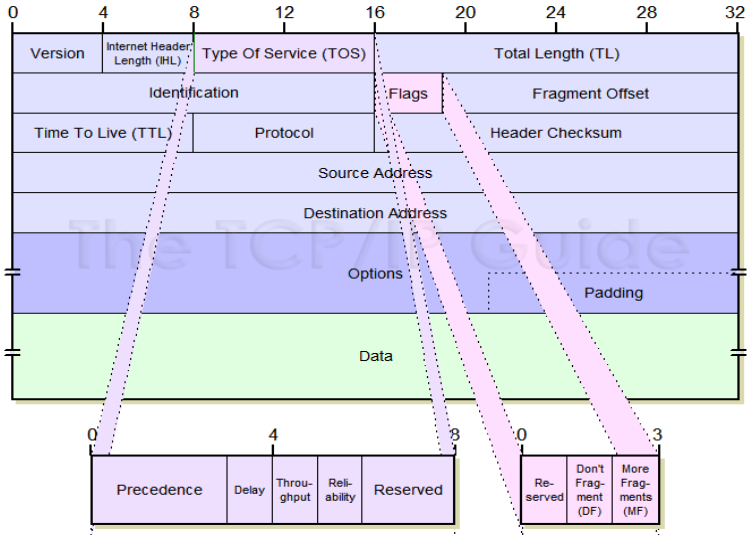
IPV4 network allocation is vital and currently has become more than 85,000 functional routers and forms the internet backbone. This infrastructure is depending on hierarchical and flat routing as well. Additionally, it becomes easy to connect multiple devices across a wide network without NAT. In other words application that doesn't require NAT easily work through firework.

3. Video Library and Conferences

Due to the increasing in number of internet users, browsing and data transfer online as become slowly. this model of communication therefore provides quality services as well as efficient data transfer. In most cases these services use TCP and UDP. Despite of having limited functionality, IPV4 addresses are refined and allowed data encryption.

4. Flexible

With IPV4, routine as become more scalable and efficient because addressing is aggregated efficiently. This works well for organizations that use multi-task, data communication across the network becomes more specific.



3.2 LIMITATIONS OF IPv4

The main limitations of internet protocol version 4{IPv4} are

1. Scarcity of IPv4 address
2. Security related issues
3. Quality of services and Address configuration related issues

IPv4 was published in 1981 and the initial design did not anticipate the expansion of internet, hence it created a lot of issues which proved that it needed to be changed. This brings us to the development and adoption of IPV6 as an alternate solution.

3.3 IP's Success Despite Its Limitations

The last three characteristics in the preceding list might be enough to make you cringe; thinking that giving your data to IP would be somewhat like trusting a new car to your sixteen-year-old son. If we are going to build our entire network around this protocol, why design it so that it works without connections, doesn't guarantee that the data will get there, and has no means of acknowledging receipt of data?

The reason is simple: establishing connections, guaranteeing delivery, error-checking and similar "insurance" functions have a cost: ***performance***. It takes time, computer resources and network bandwidth to perform these tasks, and they aren't always necessary for every application. Now, consider that IP carries pretty much ***all*** user traffic on a TCP/IP network. To build this complexity into IP would burden all traffic with this overhead whether it was needed or not.

The solution taken by the designers of TCP/IP was to exploit the power of layering. If service quality features such as connections, error-checking or guaranteed delivery are required by an application, they are provided at the transport layer (or possibly, the application layer). On the other hand, applications that don't need these features can avoid using them. This is in fact the major distinction between the two TCP/IP transport layer protocols: TCP and UDP. TCP is full-featured but a bit slower than UDP; UDP is Spartan in its capabilities, but faster than TCP. This system is really the "best of both worlds". And unlike your teenager with the shiny new license, it has been proven to work well in the real world.

3.4 Internet Protocol Version 6 (Ipv6)

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic.

IPv6 stands for Internet Protocol version 6 also known as Ipng (IP next generation) is the second version of the Internet Protocol to be used generally across the virtual world. The first version was IPv4. IPng was designed to take an evolutionary step from IPv4. It was not a design

goal to take a radical step away from IPv4. Functions which work in IPv4 were kept in IPng. Functions which didn't work were removed.

The Internet operates by transferring data between hosts in packets that are routed across networks as specified by routing protocols. These packets require an addressing scheme, such as IPv4 or IPv6, to specify their source and destination addresses. Each host, computer or other device on the Internet requires an IP address in order to communicate.

The growth of the Internet has created a need for more addresses that are possible with IPv4. Like IPv4, IPv6 is an internet-layer protocol for packets witched internetworking and provides end-to-end datagram transmission across multiple IP networks. While IPv4 allows 32 bits for an IP address, and therefore has 232 (4 294 967 296) possible addresses, IPv6 uses 128-bit addresses, for an address space of 2128 (approximately 3.4×1038) addresses. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

3.5 Features of IPv6

Features of IPv6 are listed below:

1. **New Packet Format and Header**

IPv6 specifies a new packet format. The new IPv6 packet format helps to minimize packet header processing by routers. This is achieved by moving both nonessential and optional fields to extension headers that are placed after the IPv6 header. Since IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable.

2. **Large Address Space**

IPv4has 32 bit {4-byte} address space, but IPv6 has 128-bit {1-byte} address space. The very large address space supports a total of 2^{128}{$3.4*10^{38}$} addresses. This large address space allows a better, systematic, hierarchical allocation of addresses and efficient route aggregation. With the large number of available addresses we can eliminate address-conservation techniques like NAT {network Address Translation}.

3. **State full and Stateless IPv6 Address configuration**

In IPv6 State full and stateless configuration is possible. Hosts on a link can automatically configure with IPv6 addresses called link-local addresses and with addresses derived from prefixes advertised by local routers. When first connected to a network a host sends a local-link router solicitation multicast requests for its configuration parameters. The router which is available in the link responds to the request from the host with a router advertisement packet that contains network-layer configuration parameters. Host can configure link-local addresses automatically and communicates with each other without manual configuration even there is no routers available. The hosts may also have state full configuration protocol version 6 {DHCPv6} or static configurations, IPv4.

4. **Multicast**

The three types of communication available in IPv4 are **unicast, multicast and broadcast. Unicast** is one-to-one communication; **multicast** is one –to- many communications and **broadcast** is one-to-all communication. The transmission of a packet to all hosts was performed by using special broadcast addresses in IPv4. Broadcast communication is not available in IPv6 and therefore does not define broadcast addresses. IPv6, the effect of broadcast can be achieved by sending a packet to the link-local all nodes multicast group at address ff02::1

5. **Integrated Internet Protocol Security {IPSec}**

IPSec is a set of Internet standards that uses cryptographic security services to provide Confidentiality, Authentication, Data integrity. The support for **Internet Protocol security {IPSec}** was optional to IPv4. Internet Protocol Security {IPSec} is an integral part of the base protocol suite in IPv6. **Internet Protocol security {IPSec}** support is mandatory in IPv6.

6. Neighbor Discovery Protocol

The Neighbor Discovery Protocol {NDP} is a protocol available in IPv6. The Neighbor Discovery Protocol {NDP} is based on Internet Control Message Protocol Version 6 {ICMPv6} messages that manage the interaction modes on the same link. There is no Address Resolution Protocol {ARP} for IPv6 and the role of ARP is replaced by Neighbor Discovery Protocol {NDP}.

7. Extensibility

The feature of IPv6 can be extended by adding extension headers after IPv6 header. The size IPv6 extension header is constrained only by the size of the IPv6 datagram packet, unlike 40 bytes of option of IPv4.

8. Jumbo grams

Jumbo gram is an optional feature of IPv6. Jumbo grams allows packets with payloads 2^32 -1 {4,294,967,295} bytes by making use of a 32-bit length field.

3.6 IPv6 Header Structure

Figure below shows the difference between IPv6 and IPv4 headers.

I. The length of header has been changed from 20 to 40 bytes

II. IPv4 has 4 bytes for address (i.e. 32 bits) while as IPv6 has16 bytes (128 bits).

III. The fields in the header has been reduced from 12(IPv4) to 8(IPv6).

IV. There is no options field in IPv6 header, however it uses “extension headers” that support greater functionalities

3.7 IPv4 and IPv6 Header comparison

The header fields are described below:

1) Version: Version field describes the current version of the IP protocol. Its value is 6.

2) Traffic class: Previously in IPv4, defined as the type-of-service (ToS), the traffic class field defines the class-of-service priority of the packet. Its length is 8 bits. Priority ranges from 0 (lowest) to 7 (highest)

3) Flow Label: Flow Label is used by the source to label all packets belonging to a particular flow. The flow is a unique combination of the source address and the value of a non zero flow label. Multiple flows may exist between destination and source nodes. The routers treat packets belonging to a particular flow in a similar way .Its length is 20 bits.

4) Payload Length: **T**he payload length field specifies the length of the IPv6 payload. Its Length is 16 bits.

5) Next Header: Next Header field shows the next extension header to examine. Its Length is 8 bits.

6) Hop Limit: Also known as TTL in IPv4, the value in this field gets decremented each time packet passes through a router. When the value approaches zero without making up to its intended destination, the packet gets discarded. The maximum allowed value in IPv6 is 255 hops. The length of this field is 8 bits.

7) Source and Destination Address: This field specifies the 128 bit source and destination IP addresses.

3.8 IPv6 Extension Headers

The Extension header fields are listed below:

1) Hop by Hop Option: This option is used when the source passes the information to all the routers visited by a datagram. Only 3 options are currently defined so far: Pad-1, Pad-n, Jumbo payload.Pad-1 option having length 1 byte is designed for alignment purposes. Pad-n option is similar to pad-1 except it’s used when 2 or more bytes are used for alignment purposes. Jumbo payload refers to a payload length more than 65,535 bytes.

2) Source Routing: It involves the concept of strict source route and loose source route as in IPv4.Strict source route is used by the source for predetermined route for the datagram as it travels through the internet. The sender can make a choice about route with a specific type of service such as minimum delay or max throughput. It may also choose a route that is safer and more reliable for the sender’s purpose. If a datagram chooses a strict source route, all the defined routers in the option are to be visited by the datagram. Loose source route is similar to the strict source route but a bit flexible. Along with each router in the list that must be visited, the

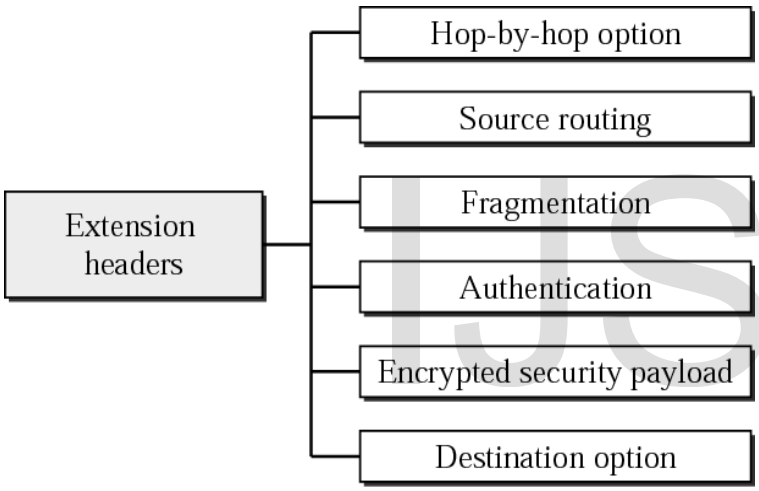
datagram can visit other routers as well which are not in the list.

3) Fragmentation: Its same concept as in IPv4 however with a little difference. In IPv4, the source or a router fragments the datagram if the size of the datagram is larger than the supported MTU of the network over which the datagram has to travel. In IPv6, the original source can only fragment. A source then finds the smallest value of MTU supported by any network on the path by using a technique for path MTU discovery. Using this gained knowledge, the source then re-fragments the datagram.

4) Authentication: This header carries out the validation of the message sender and ensures that the integrity of data is maintained.

5) Encrypted Security Protocol: This header provides confidentiality and guards against eavesdropping

6) Destination Option: It's used when the source passes the information to the intended destination only. The routers in-between are not permitted to access to this information



IPv6 Extension Headers

3.9 IPv6 Datagram Packet Structure

IPv6 has a much simpler packet header compared with IPv4, by including only the information needed for forwarding the IP datagram. IPv4 has a fixed length header of size 40 bytes. Fixed length IPv6 header allows the routers to process the IPv6 datagram packets more efficiently. The following figure shows the structure of IPv6 datagram packet.

We may divide IPv6 datagram packet header as three parts

1. IPv6 datagram packet header
2. Extension header
3. Upper layer protocol header

IPv6 datagram packet has also extension headers of varying lengths. If extension headers are present in IPv6 datagram packet, a Next Header field in the IPv6 header points the first extension header. Each extension header contains another Next Header field, pointing the next extension header. The last IPv6 datagram packet extension header points the upper layer protocol header {Transmission Control Protocol {TCP}, User Datagram Protocol {UDP}, or Internet Control Message Protocol {ICMPv6}}. There is no "option" in IPv6 datagram packet header, which was present in IPv4 header.

Version: The size of the version field in 4 bits. The version field shows the version of IP and is set to 6

Traffic Class: The size of traffic clad field is 8 bits. Traffic Class field is similar to the IPv4 Type Of Service {TOS} field. The traffic Class field indicates the IPv6 packet's class or priority.

Flow Label: The size of flow label field is 20 bits. The Flow Label provides additional support for real-time datagram delivery and quality of services features. The purpose of Flow label Field is to indicate that this packet belongs to a specific sequence of packets between a source and destination and can be used to prioritized delivery of packets for services like voice.

Payload length: the size of the payload Length Field is 16 bits. The Payload length field shows the length of the IPv6 payload, including the extension headers and the upper layer protocol data.

Next Header: The size of the Next Header field is 8 bits. The Next Header fields shows either the type of the first extension {if any extension header is available} or the protocol in the upper layer such as TCP, UDP, or ICMPv6.

Hop Limit: the size of the Hop Limit field is 8 bits. The Hop Limit field shows the maximum number of routers the IPv6 packet can travel. This Hop Limit field is similar to IPv4 Time to Live {TTL} field.

This field is typically used by distance vector routing protocols, like Routing Information Protocol {RIP} to prevent layer 3 loops {routing loops}.

Source Address: The size of the source address field is 128 bits. The Source Address field shows the IPv6 address of source field shows the IPv6 address of the source of the packet.

Destination Address: the size of the Destination Address is 128 bits. The destination Address field shows the IPv6 address of the destination of the packet.

3.10 ADVANTAGES OF IPV6

With such a huge address space, ISPs will have sufficient IP addresses to allocate enough addresses to every customer so that every IP device has a truly unique address whether it's

behind a firewall or not. NAT (network address translation) has become a very common technique to deal with the shortage of IP addresses. Unfortunately, NAT doesn't work very well for many Internet applications, ranging from old dependable, such as NFS and DNS, to newer applications such as group conferencing. NAT has also been an impediment for business-to-business direct network connections, requiring baroque and elaborate address translators to make everything work reliably, scaling poorly, and offering a highly vulnerable single point of failure.

1. ADDRESS SPACE EXPANSION

One of the goals of IPv6's address space expansion is to make NAT unnecessary, improving total connectivity, reliability, and flexibility. IPv6 will re-establish transparency and end-to-end traffic across the Internet. The new IPv6 addresses are large and cumbersome to deal with, so IPv6 reduces the number of people who have to read and write them.

2. TIME EFFICIENCY

A second major goal of IPv6 is to reduce the total time which people have to spend configuring and managing systems. An IPv6 system can participate in "stateless" auto configuration, where it creates a guaranteed-unique IP address by combining its LAN MAC address with a prefix provided by the network router – DHCP is not needed. Of course, DHCP is still useful for other parameters, such as DNS servers, and is supported as DHCPv6 where needed. IPv6 also offers a middle ground between the two extremes with protocols such as SLP ("Service Location Protocol"), which may make the lives of network managers easier.

3. MORE EFFICIENT ROUTING

IPV6 reduces the size of routing tables and makes routing more efficient and hierarchical.IPV6 allows ISPs to aggregate the prefix of their customers' networks into a single prefix and announce this one prefix to the IPV6 internet. In addition, in IPV6 networks, fragmentation is handled by the source device, rather than the router, using a protocol for recovery of the path's maximum transmission unit (MTU)

4. HIGH BANDWIDTH MULTIMEDIA

High-bandwidth multimedia and fault tolerance applications are the focus of the fourth major goal of IPv6. Multimedia applications can take advantage of multicast: the transmission of a single datagram to
multiple receivers. Although IPv4 has some multicast capabilities, these are optional and not every router and host supports them. WithIPv6, multicast is a requirement. IPv6 also defines a new kind of service, called "any cast." Like multicast, any cast has groups of nodes which send and receive packets. But when a packet is sent to an any cast group in IPv6, it is only delivered to one of the members of the group. This new capability is especially appropriate in a fault-tolerant environment: web servers and DNS servers could all benefit from IPv6's any cast technology. Another aspect of VPNs built into IPv6 is QoS (Quality of Service). IPv6 supports the same QoS features as IPv4, including the Diffuser indication, as well as a new 20-bit traffic flow field. Although the use of this part of IPv6 is not defined, it is provided as a solid base to build QoS protocols.

5. SECURITY

The fifth major goal of IPv6 is VPNs, virtual private networks. The new IPSec security protocols, ESP (encapsulating security protocol) and AH (authentication header) are add-ons to IPv4. IPv6 builds-in and requires these protocols, which will mean that secure networks will be easier to build and deploy in an IPv6 world

4.0 WHEN TO CHOOSE IPV6

As long IPv4 networks do what you need them to do, let them run. But when an IPv4 network hits the limits for some reason, choose IPv6.

IPv6 is mature enough to be used in corporate and commercial networks, as many case studies and desployments worldwide show. High investments in new IPv4 setups, fixes, or complex configurations for IPv4 (especially NATs) should be avoided if possible because they are investments in a technology that will slowly be phased out.

When you reach the point where this becomes necessary, evaluate IPv6. Whatever you invest in IPv6 is an investment in future technology

Here's the list of indicators that it may be time for you to consider or integrate IPv6:

a. Your IPv4 network or NAT implementation needs to be fixed or extended.

b. You are running out of address space.

c. You want to prepare your network for applications that are based on advanced features of IPv6.

d. You need end-to-end security for a large number of users and you do not have the address space, or you struggle with a NAT implementation.

e. Your hardware or applications reach the end of their lifecycle and must be replaced. Make sure you buy products that support IPv6, even if you don't enable it right away.

4.1 THE MIGRATION FROM IPV4 TO IPV6

The years from 1997 to 2000 will be characterized by the adoption of IPv6 by ISPs and users. During 1997, users could still have problems related to the newness of products, but starting from 1998, IPv6 will be part of mass-produced protocols distributed on routers, on workstations, and on PCs. At that point, organizations will begin to migrate, less or more gradually, to IPv6 .The key goals of the migration are as follow:

a. IPv6 and IPv4 hosts must interoperate.

b. The use of IPv6 hosts and routers must be distributed over the Internet in a simple and progressive way, with a little interdependence.

c. Network administrators and end users must think that the migration is easy to understand and implement.

A set of mechanisms called SIT (Simple Internet Transition) has been implemented; it includes protocols and management rules to simplify the migration.

The main characteristics of SIT are the following:

1. Possibility of a progressive and non traumatic transition: IPv4 hosts and routers can be updated to IPv6, one at a time, without requiring other hosts or routers to be updated simultaneously.
2. Minimum requirements for updating: The only requirement for updating hosts to IPv6 is the availability of a DNS server to manage IPv6 addresses. No requirements are needed for routers.
3. Addressing simplicity: When a router or a host is updated to IPv6, it can also continue to use IPv4 addresses.
4. Low initial cost: No preparatory work is necessary to begin the migration to IPv6. Mechanisms used by SIT include the following:

a. A structure of IPv6 addresses that allows the derivation of IPv6 addresses from IPv4 addresses.

b. The availability of the dual stack on hosts and on routers during the transition—that is, the presence of both IPv4 and IPv6 stacks at the same time.

c. A technique to encapsulate IPv6 packets inside IPv4 packets (tunneling) to allow IPv6 packets to traverse clouds not yet updated to IPv6.

d. An optional technique that consists of translating IPv6 headers into IPv4 headers and vice versa to allow, in an advanced phase of the migration, IPv4-only nodes to communicate with IPv6-only nodes.

As with any migration, there are risks involved. The risks may be described as follows:

i. If there is a problem, many users may be affected.

A phased approach to migrate a few users at a time may bea good idea. With adequate testing, many flaws should be uncovered before implementation. Still, as each group of clients is added, there may be configuration issues.

ii. What happens if the path or route fails?

As in IPv4, routing should recover from failures. But, the IPv6 routing protocols have not been tested as thoroughly as the IPv4 routing protocols. It is unclear how quickly convergence will occur, if routing loops will be created or if the routing tables will fail to be properly managed.

iii. It may take longer for the transactions to complete.

Extra overhead is imposed on the routers and backbone links because of multiple IPv4 and IPv6 routes. The routers doing the conversion may become bottlenecks.

A technique and set of protocols for ensuring smooth forward, stepwise and independent changeover to IPv6 services is required. The Ngtrans Group created by IETF is assigned the job to facilitate the smooth transition from IPv4 to IPv6 services. The various transition strategies can be broadly divided into two categories, including dual stack and tunneling mechanisms.

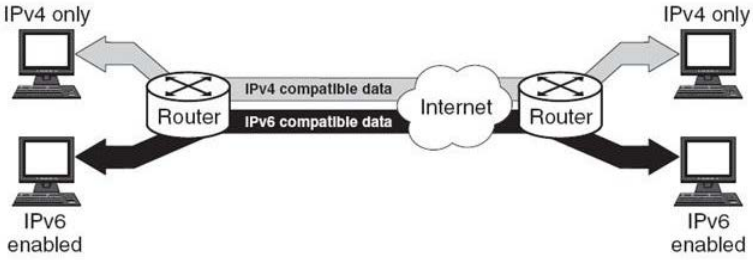
A. Dual Stack

Dual-stack (or native dual-stack) refers to simultaneous implementation of IPv4 and IPv6. In this case, all the routers are able to process both protocols. Dual-stack is mentioned in RFC 4213[11].Although, dual stack is the most preferred implementation because it avoids various complexities and roadblocks associated with tunneling (such as increased security, increased latency and overall management overhead),it's not always possible due to the presence of outdated network infrastructure which may not support IPv6.

Dual Stack Router Implementation

4.2 Differences and Comparison Between IPv4 and IPv6 addresses

The following table lists the important differences between IPv4 and IPv6.



S/N	IPv4	IPv6
1.	IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
2.	IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimal.
3.	IPSec support is only optional.	Inbuilt IPSec support.
4.	Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by the sender.
5.	No packet flow identification.	Packet flow identification is available within the IPv6 header using the Flow Label field.
6.	Checksum fields are available in IPv4 header	No checksum field in IPv6 header.
7.	Address Resolution Protocol {ARP} is available to map IPv4 addresses to MAC addresses.	Address Resolution Protocol {ARP} is replaced with a function of Neighbor Discovery Protocol.
8.	Internet Group Management Protocol {IGMP} is used to man-	IGMP is replaced with Multicast Listener Discovery {MLD} messages.

	age multicast group membership.	
9.	Broadcast messages are available.	Broadcast messages are not available. Instead a link- local scope "All nodes" multicast IPv6 address {FF02::1} is used for broadcast similar functionality.
10.	Manual configuration{static} of IPv4 addresses or DHCP {Dynamic configuration} is required to configure IPv4 addresses.	Auto-configuration of addresses is available.
11.	Option fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.

Table 1.0

5.0 SUMMARY

The rapid explosion of the internet and existence of high speed wireless and broadband networks have contributed towards depletion of IPv4.The IPv4 protocol created more than three decades ago with approximately an address space of 4 billion cannot cater to the needs of modern internet. The IANA (Internet Assigned Numbers Authority) allocated the last chunk of IPv4 addresses on Feb 3, 2011 to the Regional Internet Registries announcing end of IPv4 addresses. The address depletion has posed a serious problem on the growth of internetworks. The short term solutions like PPP/DHCP (address sharing), CIDR (classless inter-domain routing) and NAT (network address translation) do not seem to help considering the number of devices that are getting connected to the internet daily. Also as the protocol was developed long time back, the features related to mobility, security and QoS (Quality of Service) are handled by additional protocols which cannot be integrated within the protocol. For example Internet Protocol Security (IPSec) is a protocol suit which provides network security by encrypting and protecting the data being sent. Internet Protocol Security (IPSec) provides security for IPv4 packets, but Internet Protocol Security (IPSec) is not built-in and use of IPSec in IPv4 has compatibility issues with NAT. Looking at IPv4, standards do exist for real time data delivery, known as QoS (Quality of Service) but the traffic load relies on just 8 bit TOS (type of service) field and identification of the payload data. The TOS in IPv4 has limited domain and with the passage of time has been redefined with different interpretations. Also payload identification is not possible when IPv4 packet is encrypted using a TCP or UDP port.

REFERENCES

[1] IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No1, May 2012, www.IJCSI.org 314Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved. Security assessment of internet protocol version 4{IPv4}

[2] Vinton G. Cerf, Robert E. Kahn, "A Protocol of Packet network Intercommunication", IEEE Transactions on Communications, Vol. 22, No.5, May 1974 pp. 637-648"IPv6 Headers", Online:http://www.cu.ipv6tf.org/literatura/chap3.pdf , chapter 3, pp. 40-55, Des 12 1997.

[3] S. Deering, R. Hinden, Internet Protocol Version 6 (RFC2460), 1998Ipv4/Ipv6 Translation Technology, Masaki Nakajima, Nobumasu Kobayashi,2004

[4] Charles M. Kozierok, "TCP/IP Guid A COMPREHENSIVE , ILLUSTRATED INTERNET NTERNET PROTOCOLS REFERENCE", Online: http://nostarch.com/download/tcpip_ch25.pdf, chapter 25, pp.373-381, October 2005.

[5] Hitesh Ballani, Paul Francis, Cornell University, Ithaca, NY, "Understanding IP Anycast", Online: http://pias.gforge.cis.cornell.edu/unpub/anymeasure.pdf.http://inetcore.com/project/ipv4ec/index_en.html.

[6] Online :http://www.omnisecu.com/tcpip/ipv6/differences-between-ipv4-and- ipv6.php."IPv6 Headers", Online: http://www.cu.ipv6tf.org/literatura/chap3.pdf, chapter 3, pp. 40-55, Des 12 1997. T. Dunn, "The IPv6 Transition," IEEE Internet Computing, Vol.6, No.3, May/June 2002, pp.11-13 IPv6 users' site: http://www.ipv6.org.http://www.juniper.net/techpubs/en_US/

[7] En.m.wikipedia.org/wiki/internet protocol: Google searchGoogle search : www.cisco/ipj.com: PDF INTERNET PROTOCOL JOURNAL

About Authors

1. Aluko T.S
E-mail: aluko.temitope@ogitech.edu.ng
Department of Computer Science, Ogun State Institute of Technology, Igbesa

2. Olusanya O.J
E-mail: olusanya.olabanji@ogitech.edu.ng
Cisco Department, Ogun State Institute of Technology, Igbesa

3. Oloyede O.E
E-mail: oloyede.emmanuel@ogitech.edu.ng
Cisco Department, Ogun State Institute of Technology, Igbesa

4. Ebisin A.F
E-mail: ebironke16@gmail.com
Department of Computer Science, Ogun State Institute of Technology, Igbesa