Internet Protocol Version 6

[1]Siddharth Syal, [2]Sebu Elias, [3]Krishnapriya S
Student
SRM University,Chennai

***Abstract* - As technology progress, more and more devices get added to the network. Due to this exponential growth the current addressing mode IPv4 is running out of addresses. So, out of this concern was born IPv6, which provides a much wider addressing range to accommodate more devices. IPv6 restores end-to-end connectivity and ensures the growth of the Internet. It offers advanced level of security and speed as it can avoid many of the factors causing address collisions in v4 and time consuming operations like NAT, making the network much faster and efficient as every device can have its own public IP address.**

***IndexTerms* – Internet Protocol, IPv6, NAT, addressing, deployment, network**

I. Introduction

IPv6 or Internet Protocol version 6 is the next generation of the internet protocol and will eventually replace the current internet protocol version 4. The IPv6 was developed in order to solve the problem of IPv4 address exhaustion. The current IP version 4 is a 32 bit number which is divided into 4 octets while the new IP version 6 will be of 128 bits consisting of eight 16-bit blocks. The new IPv6 will remove the need for network address translation (NAT)[1] and the concept of private and public IPs will also be removed. The IPv6 will allow us to have $3.4x10^{38}$ addresses which is way more than the IP addresses that can be obtained using the IP version 4. The number of addresses offered by the IPv6 is enough to allocate each device a public IPv6 address. The internet protocol version 6 also helps to have a better approach to various upcoming technologies like Internet of Things in which can control various things like home lighting, microwaves by just connecting them to the network.

II. Features of IPv6

The introduction of Internet Protocol Version 6 will provide more functionalities to the existing topologies and network infrastructure. IPv6 brings along various new features that are not present in the current IP version 4 which will make the network protocols [2] easier to understand and implement. The IPv6 brings various features like:

- Larger address space
- Better security using IPsec
- End-to-end connectivity
- Auto Configuration
- Simplified Header
- Faster routing decisions
- Any cast support
- No broadcast

Larger address space- The upcoming IPv6 will offer a larger address space which will be enough for each device to have its own public IP address. The IPv6 will offer the 3.8×10^{38} addresses which will not get exhausted even after allocating an IPv6 address to every particle on the earth.

Better security using IPsec – The IPv6 will offer better data security as it will have a mandatory feature called IPsec. The IPsec is the security feature which is currently optional in IPv4. This feature will help in better data confidentiality, data integrity and authentication so that the data transmitted between peers that are connected is not tampered. Moreover IPsec ensures that the data does not fall into wrong hands as it uses authentication before transmitting the data between the peers. The IPsec supports Data Encryption Standard 56-bit and triple Data Encryption Standard 128-bit for encryption purposes. The IPsec works under two encryption modes – Transport and Tunnel. In transport mode the data which is transmitted is only encrypted with the header portion left untouched while in the tunnel mode the data along with the header is encrypted so that the data and the header cannot be tampered easily.

End-to-End Connectivity – The new IPv6 will offer better end-to-end connectivity as the IPv6 will not use address translation mechanisms like Network Address Translation (NAT) as each device which will be connected to the internet will have its own public IPv6 addresses so that peers can directly connect to each other on the internet while facing the limitations that are offered by the firewalls and organization network policies.

Auto Configuration – The IPv6 supports plug and play option which means that if we connect any device to the IPv6 network the device will be able to configure itself automatically. The IPv6 supports auto configuration feature that will help host to configure the network details automatically in the absence of DHCP server.
Simplified Header – The IPv6 has a simplified header in which the unwanted details and the options field is moved to the end of the header making it more simple to understand while making sure that the important information stays on the top.
Better Routing – The IPv6 will also make better routing decisions and routing functionality. As the IPv6 header is simplified and the unwanted information and options field has been moved to the end of the header, the router will not have to process much information which is present in the header and can take the routing decisions faster and more efficiently.
Any cast Support - The new IPv6 supports the any cast feature which will help to send the IP datagrams to the nearest host having the mentioned destination address.
No Broadcast - The IPv6 does not support broadcast as it uses multicast to communicate to various hosts that are connected to the network. This feature will also reduce the network traffic and the processing load on the devices that are connected to the network.

III. Addressing in IPv6

Unlike the IPv4 which has the 32-bit addresses [4], the IPv6 has 128-bit addresses and offers 3.8 x 10^{38} addresses. IPv6 addresses are denoted by eight groups of hexadecimal quartets separated by colons in between them. For example 2001:cdba:0000:0000:0000:0000:3257:9652 is a valid IPv6 address[4]. Moreover, in IPv6 we can also shorten the IPv6 address by removing the zeros that are present in the address. After removing the zeros, introduce double colons :: at that location which represent the zeros present in the IPv6 address. So after the removal of the zeros present in the address the new address is as follows 2001:cdba::3257:9652. The global unicast addresses in the IPv6 is just same as the IPv4 public address. The global unicast IPv6 address consist of three parts – Global routing prefix, Subnet ID, Interface Id.

IV. Security Concerns For IPv6

Like the IPv4, IPv6 also has various security concerns which may impose a direct threat on the networks that run on the IPv6 infrastructure. As in IPv6, any network address translation mechanism like NAT is not available so the host that are connected to the network will have their own public IP addresses which impose security threat for the hosts. The dual stack approach of conversion of IPv4 to IPv6 also imposes various security issues as the network administrator has to configure the network devices to run on two versions on the Internet Protocol. This type of approach will have various security concerns and will result in processing load on the network devices.

The IPv6 traffic can also be encapsulated in the IPv4 packets which result in greater security problems as various security mechanism like firewalls that filter the traffic based on the IPv4 packet might not be able to take the right decision. Since IPv6 is a new technology many network administrators don't have the complete knowledge for the implementation of IPv6 which is one of the major security concerns. The IPv6 packet size is compressed by removing IP options and uses Extension Header to deploy destination option, authentication option and more. These add to the IPv6 main header, which is 40 bytes, and together makes the IPv6 packets. As the traffic increase and many headers are being used, there is a possibility of over loading the firewall and gateway securities or even degrade the router's forwarding performance. This can serve as a potential venue for DDoS attack and et al.

V. Problems with IPv6

Each advancement comes with a baggage, as it is found in history. Be it the abandonment of the previously used hardware or the security issues introduced, the technology is too new to be fool proof. IPv6 comes with certain problems of its own, the security issues it has is still an upgrade over the existing IPv4. The problems arise mainly due to the advantages offered by the new version and the fact that the existing hardware might not have been prepared for the upgrade to the newer version.

IPv6 is not backward compatible - It is said to be the biggest engineering mistake in developing IPv6, as it is not compatible with the existing IPv4. The lack of proponents to help bridge this gap has been and will be one of the biggest reasons that IPv6 hasn't been deployed widely.
Current hardware will be rendered obsolete - Most of the current routers will not be compatible with IPv6, rendering them useless on their deployment.
Predicted growth in network segments - The adoption of IPv6 introduces significantly larger network segments. The prefix length of a subnet is /64 in IPv6, meaning devices close to 18 quintillion can be hosted on a single segment. This can grow LAN to virtually unlimited sizes, but it would in turn take years to scan one block for vulnerabilities, meanwhile in IPv4 it takes barely seconds.

VI. Deployment of IPv6

Currently the Internet works on the IPv4 version of the Internet Protocol suit. The upcoming IPv6 is deployed by limited companies and are deployed [6] dominantly using 6to4 Relaying (Tunneling) and Dual Stack, although Translation is also a viable method. Various companies like Microsoft, Cisco use 6to4 relaying over the current IPv4 network while companies like BSNL use Dual Stack mechanism to communicate via the IPv6 network.

Case Study 1 (Microsoft Corpnet using 6to4 Relaying)

Microsoft corporate intranet, also known as Corpnet, has been deploying IPv6 since 2001. Microsoft uses both Dual Stack mechanisms and 6to4 tunneling. Here we will concentrate on 6to4 tunneling. Since majority of the ISP uses IPv4 mechanism and the traffic through them is handled by v4, we use v6 on the sides. In 6to4 tunneling we have two sites that are connected over the IPv4 network with the help of ISP, while internally the organizations use the IPv6 network infrastructure and use various routing protocols like EIGRP and OSPF that can run on the IPv6 technology. In order to establish connectivity for both the sites we use various tunneling mechanisms like the GRE tunneling, 6to4 relay tunnel(ing), so that connectivity can be established between the sites that are connected via the IPv4 network. Microsoft uses the following topology (Fig 1.1) to connect to the sites that run IPv6 internally, while the external connections to those sites are made using the IPv4 technology.

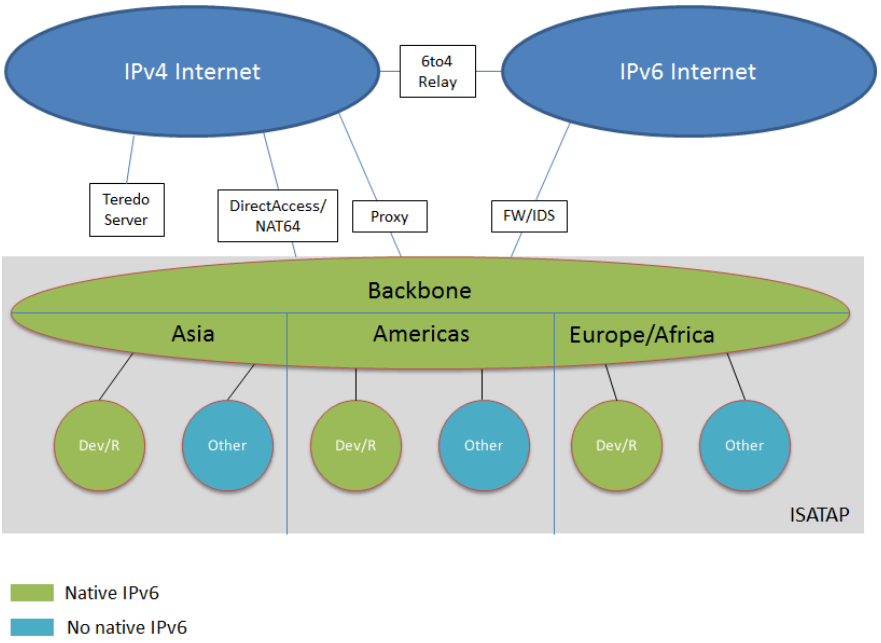

Fig 1.1 Implementation Of Microsoft Corpnet

Microsoft has received four 32-bit global address prefixes—a 31-bit prefix allocated RIPE, a 32-bit prefix from ARIN, and a 32-bit prefix from APNIC—and uses 64-bit prefixes at the subnet level.
The 32-bit global address prefixes were requested due to current ISP policies, which do not allow an organization to advertise smaller portions of your address space (with a longer address prefix) to Internet routers. To assure an adequate supply of address space going forward, Microsoft requested 32-bit prefixes, rather than a series of 48-bit prefixes.

Case Study 2 (IIT Kanpur using Dual Stack)

IIT Kanpur has a large network 15000 nodes and internet bandwidth of 3Gbps. Unlike 6to4 relaying, here we do not require all the devices to be compatible with v6, thus helping in transition from v4 to v6, which helps in the beginning phase and especially the testing phase of implementing v6. On traffic, a node prefers v6 over v4 whenever both signals are available, but on the event of receiving only v4 signals, it is limited with the option of v4 and the dual stack is well capable of processing it as well. But this is considered to be very expensive. Routers especially must be included in the dual stack as it will be the first device to receive traffic from outside of the network. This includes taking IPv6 addresses from APNIC, makes an IPv6 address allocation policy and plan the addressing for the whole network. IPv6 routing can then be enabled for the entire network in all Layer 3 switches and routers along with enabling static/dynamic routing, followed by upgrading DNS to support IPv6 address resolution along with other services like, web server, mail server etc. To provide internet access, Border Gateway Protocol routing is enabled for IPv6 peering with upstream IP. The final step is to test the available services like Internet access, Email, VoIP etc. and migrate them to both IPv4 and IPv6.

VII. Conclusion

Every technology has its own pros and cons, so does the IPv6 has. The major benefit of using IPv6 technology over IPv4 is that it provides us with better address space, so that every device can be given public IP of its own. Although security concerns of IPv6 can be upgraded in principle, it is likely to be replaced later when implemented at a larger scale.

VIII. References

[1] Cisco CCNA Routing and Switching By Wendell Odom
[2] Routing TCP/IP, Volume II (CCIE Professional Development by Jeff Doyle
[3] IPv6 - Address Types & Formats (http://www.tutorialspoint.com/ipv6/ipv6_address_types.htm)
[4] IPv6 addressing (http://en.wikipedia.org/wiki/IPv6_address)
[5] Pros and Cons of IPv6 (http://ireport.cnn.com/docs/DOC-993739)
[6] IPv6 Deployment (http://www.6net.org/book/deployment-guide.pdf)