Mechanisms of Tunneling IPv6 in IPv4 networks

Nirjhar Vermani

Abstract— In IpV4 major requirement is that all the IP networks should have unique network number, even if they are or if they are not connected with the internet, which results in the consumption of more addresses, due to this consumption IP addresses in IPV4, are becoming exhausted. Secondly the structure of IPV4 is of classes which had address spaces with different size and studied independently. To manage this problem internet experts focus on the use of Classless Inter Domain Routing (CIDR) and Dynamic Host Configuration protocol (DHCP) to manage the address space. But due to the growth in usage of internet CIDR and DHCP are not working properly as an alternative. It is becoming challenging to retain the large routing tables, network authentication and security of the network which is the major requirement in the current cyber age.

Index Terms— Sub netting, IPV6, IPV4, Tunneling, Teredo, Routing, DHCP, Tunel Broker

INTRODUCTION:-

IPV4 is the version number 4 of the internet protocol, ituses 32 bit addressing scheme and has exclusive 232=4294967296 IP addresses, and it is the first version which is deployed on the internet broadly. The main usage of the IPv4 is on the Ethernet and it doesn't assure the delivery of the packets or about the sequence in which the packets are transported and about the delivery of same packet again and again.so it works on the concept of performing its best effort to deliever the data from source to destination. It has a checksum in its header which detects and then removes the corrupted data.

In IpV4 major requirement is that all the IP networks should have unique network number, even if they are or if they are not connected with the internet, which results in the consumption of more addresses, due to this consumption IP addresses in IPV4, are becoming exhausted.

Secondly the structure of IPV4 is of classes which had address spaces with different size and studied independently. To manage this problem internet experts focus on the use of Classless Inter Domain Routing (CIDR) and Dynamic Host Configuration protocol (DHCP) to manage the address space. But due to the growth in usage of internet CIDR and DHCP are not working properly as an alternative. It is becoming challenging to retain the large routing tables, network authentication and security of the network which is the major requirement in the current cyber age.

IPV6 AS AN ALTERNATIVE:-

IPV6 or IPng (Internet Protocol of Next generation) is the version number 6 of the internet protocol, it uses 128 bit addressing scheme and has exclusive 2128 =3.4028236692093846346337460743177e+38 IP addresses, which are enough to keep internet alive for a long period of time. Though a new version known as IPV6 (Internet Protocol version number 6) has also been introduced and also its deployment is under process but still the progress is very slow.

IPv6 was introduced as an alternative to solve the problems or at least minimize the problems which we are facing in

- *Nirjhar Vermani is currently working with Cueblocks Technologies as Network Administrator in Chandigarh,India, PH-9815601715. E-mail: nirjhar18@gmail.com*

the internet protocol version 4.so in ipv6 first of all larger space for addresses was introduces which is assumed to be enough for next 30 or 35 years, unique addressing with a complete hierarchy of addresses has been introduced which depends on the prefix of address instead of classes as in ipv4,it helps in keeping the well-organized routing in the core and in outcome is the small routing tables, and this efficiency in routing tables also helps in maintaining better security and authentication in networks.

TRANSITIONS FROM IPV4 TO IPV6:-

Internet is running successfully on the IPv4 from last 20 years or so, but now there is a time to move forward toward the new IP version 6 because the unallocated addresses in ipV4 is expected to be allocated in next 5 or 6 years, and then IPV4 alone cannot fulfill the requirements of ever growing cyber population, so IPv6 transition has been accepted as the most promising solution for now.

DIFFICULTIES IN TRANSITION:-

Major difficulty in the transition phase is that from last 20 years or so internet is running on IPv4 so it is very hard to transferthis huge internet from ipv4 to ipv6 and it can only be done gradually. Experts are continuously researching about the transition and its effects on the users and internet service providers, and what will be the best scenario and effective mechanisms for transition and how this will arise or solve security issues.**"One of the problem faced by organizations especially website operators ,wanting to deploy IPv6 is the lack of information on IPv6 adoption and the quality of service provided by the IPv6 internet."[EvaluatingIPv6AdoptionintheInternet]**

Solution:-

Experts are concerned about what are the best mechanisms for deploying ipv6 over ipv4 network so until now there are few mechanisms to deploy the internet protocol version 6 on internet protocol version 4,such as:-

- Dual Stack
- Tunneling
- Translation

In this paper our main focus will be on the tunneling mechanism to deploy IPv6 on Ipv4, as well as a detailed and comparison study on tunneling mechanisms and protocols.

TUNNELING:-

One of the transition mechanisms is tunneling, in this mechanism IPv6 packets are encapsulated in to the Ipv4 packets, and then on Ipv4 network these encapsulated packets are used by IPv6 nodes for communication on the network of IPv4.**"Tunneling provides a convenient way for an IPv6 island to connect to the other IPv6 islands across an ocean of IPv4 networks" [Deploying Internet Protocol Version 6 (IPv6) Over Internet Protocol Version4 (IPv4) Tunnel]**

Tunneling can be done in two ways:-

- **Automatic tunneling**

IPv6 addresses are taken which are compatible for Ipv4, and then a route is established on the prefix of ipv6 address toward the destination of the tunnel. Due to which a packet coming from source have a destination address of ipv4 then it is passed through this tunnel.

- **Configured Tunneling**

Here entry point of the tunnel is manually configured with the end point of tunnel, and IPv6 addresses are taken and then encapsulated with the IPv4 packets for communication between the nodes of IPv6 on the Ipv4 network.

A combination of automatic and configured tunneling can also be used to route IPv6 packets across a v4 network. 6to4 and 6over4, Teredo, ISATAP,are other tunneling mechanisms. **"We expect tunnels to continue to play an important role in IPv6 networks, as IPv4 network infrastructure will remain widely deployed for many years"[IPv6-in-IPv4tunneldiscovery:methodsand experiment 2004]"**

6TO4:-

It is a transition mechanism which allows Ipv6 packets transportation on Ipv4 network and for this first encapsulation of IPv6 packets in to ipv4 packets takes place so that ipv6 packets can be delivered from source to destination over ipv4 network which is considered as non-broadcast multi access (NBMA) and remote access to IPv6 network is done through Ipv4 network for encapsulated Ipv6 domains. In this mechanism translation of addresses from ipv6 to ipv4 takes place automatically and requires no manual configuration for address translation that is why 6to4 method comes under the category of automatic tunneling**."The 6to4 mechanism is the most widely extensively used automatic tunneling technique. It includes a mechanism for assigning an IPv6 address prefix to a network node with a global IPv4 address."[IPv4/IPv6 Transition Mechanisms].**

In 6to4 automatic tunneling mechanism the network of Ipv4 is considered as a link layer which serves for Ipv6 packets communication, and the Ipv4 networks deliver ipv6 packets encapsulated in to ipv4 from source to destination.

End point address of the tunnel can be determined when encapsulated packets of IPv6 are passed through the router configured for 6 to 4 tunnel mechanism. During this traffic delivery tunnel is automatically created without a need of any manual configuration

Globally unique unicast address is determined by the prefix value present in prefix of address format in 6to4 mechanism. In this process it is must for a site to have an ipv6 address which should be global and unique, only then an ipv6 prefix is assigned.

6OVER4:-

It is a mechanism designed for IPv6 remote hosts present on physical link having no direct link with routers configured on IPv6, it provide a virtual link which allows these remote host to use Ipv4 multicast address to communicate with other Ipv6 hosts.For making interface ID of Ipv6 an Ipv4 address is being used by hosts on 6over4.Ipv6 prefix used in 6 over 4 is same as it is in simple Ipv6 prefix and it can be configured manually.

During the encapsulation of Ipv6 packets, IP address of the source Ipv4 packet is same as of the 6over4 configured sending host interface. Whereas Ipv4 address destination will be the next hop for the Ipv6 address packet, due to which it is not must for the next host to be 6over4, next host can or cannot be on 6over4 mechanism. So in 6 over 4 first ipv4 addresses is assigned to the host, after that host makes a local link address. Then host performs duplicate address detection process, and once it is done then it generated an ipv6 neighbor discovery message and transmits it using multicast.

Domain which want to use 6 over 4 to form a virtual link should have Ipv4 multicast compatibility and an aces to one of the public Ipv4 network otherwise virtual link will not be established, because the basic function of ipv4 multicast address is discover of the neighbor. If next neighbor will be discovered, only then the Ipv6 hosts on 6 over 4 achieve connectivity. Host on 6 over 4 identify themselves by the routers who have ipv6 enabled on them, in some cases if such routers are not available then 6 over 4 hosts identify other hosts who are linked with local address.Host on 6 over 4 identify themselves by the routers who have ipv6 enabled on them, in some cases if such routers are not available then 6 over 4 hosts identify other hosts who are using local link address.

Through this mechanism IPv6 connectivity can be achieved even when Ipv6 addresses are not compatible with Ipv4, this mechanism is suitable for both type of network either on ipv4 network or on a network having both ipv4 and ipv6.so it is better for those networks which are in transition from ipv4 to ipv6 to use 6over4 tunneling mechanism but a condition to use this mechanism is that it should be used in same link.

ISATAP:-

Automatic tunneling mechanism contains a protocol names as ISATAP (intra site automatic tunnel addressing protocol), as it is a protocol of automatic tunneling mechanism so for ipv6 connectivity it don't require any major manual configurations. **"ISATAP is a technique that uses IPv4 as a layer 2 for IPv6, and it has a technique for generating an Ipv6 host ID from the underlying IPv4 address". [ObservationsofIPv6Addresses].** Protocols of Ipv6 consider the protocols of ipv4 as link layer protocols which allow remote hosts to make a virtual connection with each other as neighbors. Clients in the ISATAP domain are assigned the Ipv6 addresses by the ISATAP routers. ISATAP use Unicast address as its prefix address. Like other mechanisms of tunneling, in ISATAP Ipv6 packets encapsulates in to Ipv4 and then de-capsulation of packets is also similar.Ipv6 hosts connected with ISATAP router encapsulate the packets which are de-capsulated when reached to ISATAP router. When ISTAP router received the encapsulated packet, it then de-capsulate them and then forward them on the Ipv4 network for further processing. Filtering of packets is takes place on both entry points, one of the coming Ipv6 encapsulated packets and other on Ipv4 packets. **"The weak point of this solution is that this was proposed in the intranet users but not for internet users. Therefore this method should work with other mechanisms in order to support IPv6 transition over the internet properly" [New Ipv6 Transition Mechanism based on End to End tunnel]**

ISATAP server provides a prefix of length 64 bits to its hosts, after that hosts make their own ISATAP address and interface identifier. This interface identifier is used by the hosts to identify other interface attached to them. Once other interfaces are identified then ISATAP host become capable of connecting other hosts through tunnel. ISATAP hosts can connect to other Ipv6 networks which are outside of the domain by the help of some similar transition mechanism like 6 over4.

TUNNEL BROKER:-

Tunnel broker is a mechanism which creates a tunnel automatically; it creates a tunnel server up to the hosts, firsts hosts have to register to DNS and to provide information such as total life time needed to create a tunnel from tunnel server to host. Also IPv6 and IPv4 addresses are provided to DNS. This mechanism has IPv6 backbone in its backend and it provide services to Ipv4 users to connect with the Ipv6 backbone by creating a tunnel.Tunnel broker allow remote host to communicate with Ipv6 backbone. No manual configuration is needed in this mechanism to setup, manage, or maintain tunnel as tunnel broker do it effectively and efficiently. All traffic is passed through the tunnel server so it is easy for tunnel broker in handling request and providing effective communication. It treats Ipv4 network as Non broadcast multiple data kink layer and does not require Ipv4 network to be multicast supported.

Dual stack routers act as tunnel broker and tunnel server, being a tunnel broker a dual stack router is always located in IPv4 network and connected with Ipv6 backbone. It perform neighbor discovery In Ipv4 network.It serves for remote Ipv6 hosts for creation or deletion of tunnels. Dual stack router act also as tunnel server and like tunnel broker it is also connected with IPv6 and Ipv4 network, it receives messages from tunnel broker, according to that message it takes action to create, remove, or modify the tunnels. Remote Dual stack IPv6 router acts as a tunnel client on Ipv4 network, and allow hosts to connect with Ipv6 network.

TEREDO:-

Teredo is the first transition mechanism which provides IPv6 connectivity to those hosts which are behind NAT; otherwise all of the other mechanisms don't provide connectivity to the Nat hosts as all these mechanisms require IPv4 address to be always public. Teredo enables hosts behind the IPv4 Nat to connect with the IPv6 network, for this encapsulation of Ipv6 packets takes place and then these encapsulated packets are tunneled over UDP.UDP post number for Teredo server is 3544.

Teredo consists of Teredo relay, Teredo server and the last one is Teredo client. Each part has its own functionality. Teredo server deals with Teredo clients and provides them IPv4 address. When a client gets an IPv4 address, it builds and Ipv4 address embedded Ipv6 address server automatically. Teredo server is always stateless due to which they provide effective services to large number of clients. Teredo relay provide a connection between a Teredo client and Ipv6 hosts. For this communication first of all Teredo server checks for an appropriate relay for a Teredo client, once an appropriate relay is choose then a connection clients and Ipv6 host is established. Selection of an appropriate relay depends upon the following criteria:-

- Total distance between a relay and a client
- Total number of clients getting services from the relay.

Teredo client is a node or a host which is behind a NAT and it needs IPv6 connectivity. Teredo client contains information such as IPv6 address, Total number of Teredo peers, Date and time about the interaction of Teredo client and Teredo server. Address mapping between internal and external port number and IP address takes place when a packet is passed outside of the NAT or inside of the NAT, but the packets sent outside of the NAT are always IPv6 encapsulated.

There is a Qualification process in Teredo mechanism, for a successful IPv6 connection Teredo client has to pass this qualification process, it consist of following steps:

- Teredo client sends a router solicitation (RS) message through its link local address to the link local address of the Teredo server.
- After sending RS message clients wait for an advertisement message from Teredo server, if a Teredo client doesn't receive an advertisement message from Teredo server with in a given time frame of 45 second then it resend RS message to Teredo server, Total number of resending RS message is limited to 3.
- Once an RS message is received by the Teredo server, it prepared an advertisement message for the Teredo client along with the information of its IPv4 address.

- When the authenticated message is received on the Teredo client side, it has to be authenticated first and then to pass through NAT, if both become successful then Teredo client received that advertisement message sent by Teredo server, and Qualification process become successful and over.

If the advertisement message sent by Teredo server failed to pass through Nat or validation then server again sends an advertisement message to Teredo client. Bubble packets are used in qualification process; it keeps track of the external nodes and record IP address and port number of these nodes for NAT mapping Table.

ESCORT PROTOCOL:-

Architecture of Escort protocol is similar to the structure of Teredo protocol; but with an addition of ID/Locator split thought, this addition has made it more secure and reliable for use by the clients especially in mobile environment. There are many limitations in the Domain name System (DNS) and IP addresses in the current internet world. DNS is suitable for dynamic environment when fast updating of host information is needed. IP address also has limitations because of its use as locator in network layer and in application layer as identifier. Due to this 2 way use of IP address as Identifier and locator has made it difficult to create a multi homing, secure mobile environment. So the concept of ID/Locator split has been introduced recently and **"ID/locator split architecture uses distinct sets of values for IDs and locators, and allows the network layer to change locators without requiring the upper layers to change IDs to ensure that the communication sessions associated with the IDs are not interrupted".**Now by ID/Locator adoption escort address are divided I to two, one work on transport layer to identify the network interfaces and is known as host identity address and the second address works on the network layer as a locator. This way secure mobile environment has been achieved.

Escort is also composed of various components such as Escort relay, Escort server and Escort client. A dual stack IPv6/Ipv4 node act as an escort server and it has dual connection, one with the Ipv6 network and the other connection with IPv4 network and it provides a tunnel between Ipv6 and Ipv4 network for the transportation of packets between these two networks. Escort clients register tunnels with Escort server by sending a request for registration of a tunnel, Escort server receives the request and run an authentication procedure to validate the request. If Escort server validates the request only then Escort client become qualified for the registration of the tunnel and then Escort server provide its mac address and host identity address and Mac address. Escort server identify the type of Nat on the Escort client side, after identification Escort client sends internal Ipv4 address, post number and host identity address, this information is recorded by the Escort server before registration of the tunnel. Escort server removes the address configuration and resolution issues for the Escort clients. When an Escort client successfully registered a tunnel then it provides this tunnel for connection between Ipv6 hosts behind NAT and Ipv4 network. Routers configured with IPv6/IPv4 act as Escort relay and deliver traffic between Ipv6 host and IPv4 client. Escort Server chooses an appropriate relay for communication between host and clients. Teredo protocol is similar to Escort but Teredo has security issues and unable to operate with the symmetric NAT, on the other hand Escort **"provides more security, supports mobility and multi-homing, and has the capability of traversing symmetric NATS."[escort]**

Escort address is represented by 16 bit prefix and it is same for all escort addresses, and value of flag field is 0x00000000 and it represents host address. Interfaces are identified by an interface id of 48 bit mac address. There are two types of packets in Escort protocol; one is Data packet which deals with transmission of data (packet) between client and server, client and relay and relay and relay and the other one is Keep-Alive packet which keeps track of the time between the state of tunnel and Escort client and also Map and manage NAT tables.

COMPARISON AND RECOMMENDATIONS:-

The above discussion about different mechanisms is to compare and then to choose a mechanism or a scheme of mechanisms which when u se to deploy IPv6 over Ipv4 network then it doesn't give us a major issues in a specific environment.

The most feasible mechanism is that which provide security and do not create security issues when IPv6 is deployed, it should be feasible in a given scenario and handy so that when IPv6 is deployed then the users of the network do not notice any change. Performance is another important factor which a choose mechanism should fulfill and it should be compatible with the existing system equipment's to provide a maximum performance without a decline or issues in performance. Deployment of IPv6 using the selected mechanism should be easy to maintain and manage.

If we compare the different mechanism mentioned in the paper then 6to4 tunneling mechanism is the one which work well only on the border routers and it is deployed there to provide connectivity between Ipv6 sites to an Ipv4 network. It does not work for individual hosts and perform best only at the edge routers of the site or domain. It is recommended for small sites because of its connectivity on edge routers are feasible but for a small site, deployment of 6to4 tunneling mechanism on large site makes it difficult to control and manage. Many Security threats are noted in different researches and experiments such as Denial of service attack is very common in this mechanism due to which one malicious node results in the blockage of communication between other connected nodes. These security threats and its lack of maintenance and control on large sites are still under research. The other mechanism which can be used for deploying IPv6 is 6over4which is very useful to deploy IPv6 on Ethernet or any virtual links but its major condition is that all the routing should be IPv4 multicast and the Ipv4 network should be public, if these two conditions are fulfilled in any scenario then 6over4 can be used as tunneling mechanism to deploy IPv6.if the IPv4 network is not public and multicast address is not supported then Ipv6 link-local address cannot be established in a particular scenario. Another tunneling mechanism Tunnel Broker which is easy to manage and maintain as an automatic tunnel is created between client and server due to which traffic pass through a tunnel and security management is also easy in this mechanism because client and server contact directly for creation of tunnel and security is pre-configured to prevent unauthorized access but the research has shown that the major problem in tunnel broker is that due to creation of a tunnel between a client and server management becomes easy but it makes a single point of failure, occurrence of any problem in tunnel results in whole system breakdown, and other **"problem observe in this mechanism is latency, and the obvious impact that a high value means to the users IPv6 experience".[6to4 versus tunnel broker],**so this risk of single point of failure, delay and communication bottle neck can be somehow afforded in smaller sites but in larger sites it cannot be accommodate. Other mechanism ISATAP comes under the automatic tunneling category and no specific configurations are needed here as well, and recommended for small sites and it serves as a gateway for the clients of ISATAP subnet, configurations are easy and cost effective but security threats such as spoofing is also present here due to a gateway between ISATAP subnet and clients. Teredo is another protocol which is better other mentioned mechanisms because it provide a connectivity to those hosts which are behind the NAT as well, but main drawback of the Teredo is that it cannot handle symmetric NAT. Moreover security threats are also here, **"if network controls are bypassed due to the use of IPv6 via Teredo, the burden of controls shifts to the Teredo client host. Since the host may not have full control over all the nodes on the network, security administrators sometimes prefer to implement security controls on the network.",[Symantec]** Now the latest tunneling mechanism named as Escort has been introduced, which work well with the symmetric NAT and also have managed the Dual role of IP address by introducing the concept of ID/Locator which has made it more secure and feasible for mobile environment, but this protocol is still under the research and I have not found much information on this protocol so its drawbacks and more advantages are still unknown till further research and deployment.

Based on above comparison it is clear that no such mechanism exist until now which can be used to deploy IPv6 in to Ipv4 network with full security, performance and scalability. Different mechanisms are present which are suitable for different scenarios for deploying IPv6 but no single mechanism exist which work well in all scenarios, or different mechanisms can be used together to achieve the desired result. Many research and experiments are under progress and lot more has to be done to finally find a feasible solution to replace Ipv4 with Ipv6 using transition mechanism.

CONCLUSION:-

From past 20 years internet has worked well onIPv4 but now IPv4 addresses are going to exhaust in coming 5 or 6 years, due to which transition from IPv4 to a new protocol Ipv6 is very necessary to keep the internet world alive, it is very difficult to move internet from Ipv4 to Ipv6 due to its huge database, Transition is in progress but it will take a long time.

Several transition mechanisms have been introduced and deployed; out of which one is tunneling mechanisms which are deployed in several scenarios and until now no such mechanism is found which is feasible completely for deploying IPv6 over Ipv4.New tunneling mechanisms are coming and are under research and experiments to remove the drawbacks present in them so that the transition process from IPv4 to IPv6 becomes possible without any security, compatibility and performance issues.

REFERENCES:-

1. Jun Bi, Jianping et.al, "IPv4/IPv6 Transition Technologies and Univer6 Architecture", International Journal of Computer Science and Network Security, VOL.7, January 2007

2. Lydia Parziale, David T. Britt et.al,"TCP/IP Tutorial and Technical Overview", IBM Red Books, December 2006.
3. Mun , K. Lee,"UNDERSTANDING IPv6", Text Book ,Publish Date: 19 May, 2005;
4.
5. "IPv6 – The Next Generation of Networking ", Hewlett-Packard, 2007.

WEB RESOUCES:-

6. http://packetlife.net/blog/2010/mar/15/6to4-ipv6-tunneling/
7. http://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/automatic-6to4-tunnel
8. http://publib.boulder.ibm.com/infocenter/zos/v1r10/index.jsp?topic=/com.ibm.zos.r10.hale001/ipv6d0121000298.htm
9.
10.
11. [1].Hong,Ko,et.al,"New Ipv6 Transition Mechanism on End-To-End Tunnel", 1stint'l. Conf." Next Generation Network", July 9-13, 2006.
12. [2]. HailinAnWanmingLuo et.al," A new IPv6 Tunneling Protocol: Escort", International Symposium onComputer Network and Multimedia Technology, 2009.
13.

14. [3]. Friacas, Baptista,et.al, "6TO4 versus TUNNELBROKERS",int'l. Multi-Conference on
15. "Computing in the Global Information Technology", August 2006.
16.
17. [4].Dr. James Hoagland,"The Teredo Protocol:Tunneling Past Network Security and Other Security Implications", 28, November, 2006
18.
19. [5].Kafle,Otsuki, et.al, "An ID/Locator Split Architecture for Future Networks",IEEE Communications Magazine, 2010.

20. [6].D.Shalini,K.Sankaranarayanan,"IPv4/IPv6 Transition Mechanisms",European Journal of Scientific Research, 2009
21.
22. [7].Colitti,et.al, "IPv6-in-IPv4tunneldiscovery: methods and experimental results", IEEE transaction on Network and Service Management, 2004.
23.
24. [8].Samad, Yusuf,et.al, "Deploying Internet Protocol Version 6 (IPv6) Over Internet Protocol Version4 (IPv4) Tunnel", student conf. on Research and Development proceeding,2002.
25.
26. [10].Colitti, H.Gunderson et.al, "Evaluating IPv6 Adoption in the internet",11thintern'l conference" Passive and active measurement",2010

27. [11].DavidMalone, "ObservationsofIPv6Addresses",9th int'l conf."Passive and active network measurement", 2008.
28.