IMPLEMENTATION OF PBR IN IPV6 ROUTING TRANSITION MECHANISMS

T.Ramya[1], S.Seethalakshmi[2], B.Swarnalakshmi[3], P.Geetha[4]
[1, 2, 3]BE Student, Dept of ECE, P.R.Engineering College, Thanjavur.
[4]Associate Professor, Dept of ECE, P.R.Engineering College, Thanjavur.

Abstract
The internet is a worldwide publicly accessible system of interconnected computer networks, since IPV4 in network enables data sharing between two or more computers which minimize time and energy wastages.The existing IPv4 network has the limitations of more latency, less security, less address space and, no auto configuration facility. IPv6 network is proposed in our project that overcomes all the limitation available in existing network. When any organization wants to implement ipv6 network in his service area, it is not possible to implement all of sudden in entire area. It needs slowly migration from ipv4 to ipv6 without much affecting service. The dual stack and tunneling concept is proposed in this project to transmit ipv6 packet through ipv4 Network that enables and achieves fully convergence in ipv6 network. I have used the simulation software GNS-3 and VPCS 2.0. To configure PBR on an interface, use the following commands beginning in global configuration mode are defines a route map to control where packets are output. This command puts the router into route-map configuration mode.

Keywords: IPV4, IPV6, Dual stack and tunneling concept, GNS-3 & VPCS 2.0, PBR.

1. Introduction

A Network in the world of computers is said to be a collection of interdepended hosts, via some shared media which can be wired or wireless. A computer network enables its hosts to share and swap the data and information over the media. Network can be a Local Area Network (LAN) connected across an office or Metro Area Network (MAN) spanned across a city or Wide Area Network (WAN) which can be connected across cities and colonies [5]. Internet Protocol is a set of technical rules that conclude how computers relate over a network. There are currently two versions: Internet Protocol version 4 (IPv4)and Internet Protocol version 6 (IPv6) [6]. However, IPv6 has no built-in backwards compatibility with IPv4, which means IPv6 networks cannot communicate with IPv4 in nature. Essentially IPv6 has created a parallel, independent network that coexists with its counterpart IPv4. If an IPv4 network wants to further support IPv6 communication, it has to carry out dedicated addressing and routing for IPv6, and update the network devices to enable IPv6. Currently IPv6-capable applications and IPv6-accessible contents are still the minority [7]; the majority of network resources, services and applications still remain in IPv4. Therefore IPv4 network will probably last for a long time. On the other hand, the continuous demands for new IP addresses are driving IPv6 towards a large-scale deployment. Therefore, IPv4 and IPv6 will coexist for a long period, and the transition process will be gradual. During this period, we need to manage the availability of both IPv4 and IPv6 and solve the issues arising in DNS, QoS, security and other aspects under the dual-stack environment.

1.1. Architecture of Networking

In networking different autonomous computers are connected to each other over a communication network, amount all the hosts, one host act as a master or server node which performs task allotment to the sub nodes that are applicable or able of performing the task.

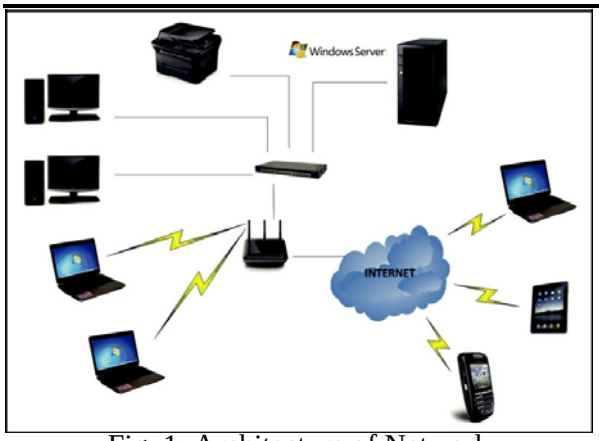

Fig. 1: Architecture of Network

1.2. IPv4

IPv4 is the first version of Internet Protocol to be widely used, and accounts for most of today's Internet traffic. There are just over 4 billion IPv4 addresses. In Mobile IPv4, a node that receives the data packets resides on the specific network nominated to it by its corresponding IP address. IPv4 is the most demand addressing protocol used on the Internet and most individual networks today. With the advent of wide variety of devices and upcoming technologies, the limited addresses of IPv4 are not capable to handle with the current internet. IPv6 was mainly developed to resolve the addressing issues as well the security concerns which are lacked by IPv4. One of the major challenges in the internet is to deploy IPv6 [1].

1.3. IPv6

Internet Protocol version 6 (IPv6) is a new generation protocol of the basic internet protocol. Internet Protocol (IP) is a common language of the Internet, every device connected to the Internet must support it. The current version of Internet Protocol version 4 (IPv4) has several shortcomings which are unavoidable and complicate such exhausted address space, security issues, non availability of auto-configuration and in some cases present a barrier to, the further development of the Internet. While that is a lot of IP addresses, it is not enough to last forever. IPv6 is the sixth revision to the Internet Protocol and the successor to IPv4.

2. PROTOCOL SPECIFICATION: IPV4 VS. IPV6

The basic protocol specification of IPv6 was proposed in 1998, and related standards have been developed ever since. IPv6 has different address architecture from IPv4, as well as a series of new features [7].

2.1. *Addressing*

The most obvious advantage of IPv6 over IPv4 is its larger address space. The 128-bit IPv6 address length provides approximately $3.4 * 10^{38}$ available addresses, while IPv4 only provides $4.3 * 10^{9}$ addresses due to the 32-bit limit. The IPv6 address length is selected based on the lesson of IPv4 address exhaustion. The vast address space is believed to be enough for the foreseeable future. A typical IPv6 uncast address is composed of two parts: 64-bit network prefix and a 64-bit interface identifier. The interface identifier is unique within a subnet prefix and used to identify interfaces on a link. Unlike in IPv4, the subnet size in IPv6 is fixed to 2^{64}. The 64-bit network prefix length provides great flexibility in network management. By recommendation a /32 prefix is provided for an ISP, while a prefix between /56 and /64 is given to an end-consumer site [8]. This leaves the ISPs at least /24 space to organize their networks, and the global Internet /32 space to manage global routing. Therefore address allocation can be simplified and route aggregation can be achieved efficiently, under which circumstances it is feasible to build a hierarchical addressing and routing architecture. Besides, the vast address space along with the 64-bit subnet size also eliminates the major demands for NAT.

2.2. New features in IPv6

In order to inherit the merits of IPv4 smoothly, IPv6 improves some beneficial features of IPv4 up to its own standard, and goes further with introducing additional features that are not presented in IPv4:

(1)Stateless address auto-configuration. Besides manual con-figuration and stateful configuration (DHCP), IPv6 provides a third, stateless configuration manner. IPv6 hosts can lever-age ND (Neighbor Discovery) Protocol [10] to configure themselves automatically when connected to a network. In a standard procedure, the host generates a link-local address by appending an interface identifier to the well-known link-local prefix, and then verifies the uniqueness of the ad-dress by sending out a Neighbor Solicitation message. When the verification is confirmed, the host assigns the

link-local address to the interface, and then either sends out a link-local Router Solicitation message to retrieve a corresponding Router Advertisement message from a router, or wait for periodical Router Advertisement that contains network-layer configuration parameters.

(2) Simplified protocol header. As is shown in Figure 1, some insignificant fields such as IHL and TOS, as well as the fragmentation-related fields are removed or moved to optional extension headers. Header Checksum is also removed and the responsibility is left to the link layer and the transport layer. The IPv6 header simplifies the processing on routers.

.

(3) Moving fragmentation from routers to end hosts. IPv6 hosts are required to either perform path MTU discovery and fragment packets before sending them out, or only send packets no bigger than the minimum MTU (1280 bytes). This feature also simplifies the processing on routers.

2.3 Issues with IPv4-IPv6 coexistence

Due to the significant differences in the protocol format and behavior, IPv4 and IPv6 are not inter-operable. To further support IPv6, an ISP has to create an essentially a parallel, independent network. As to end hosts, modern computer operating systems have already implemented dual-protocol stacks for access to both networks

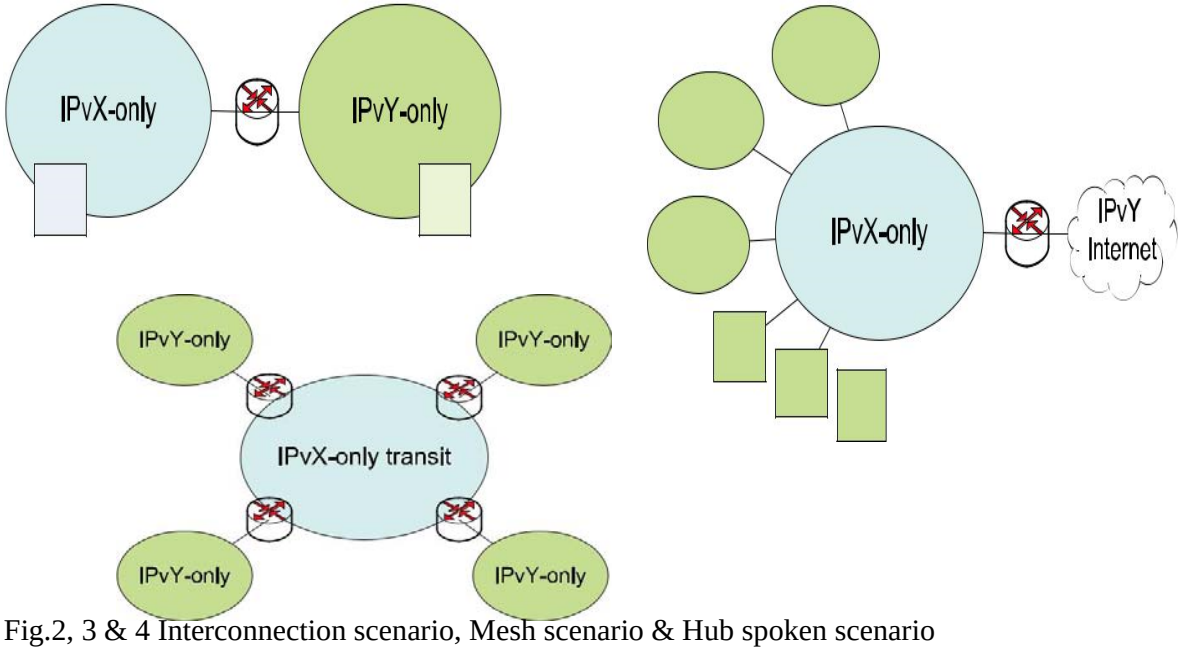

Fig.2, 3 & 4 Interconnection scenario, Mesh scenario & Hub spoken scenario

3. TRANSLATION MECHANISMS

3.1. Basic Principle of Translation

IPv4-IPv6 translation is used to achieve direct communica-tion between IPv4 and IPv6. The basic principle of translation is shown in Figure 5. The idea is to convert the semantics between IPvX and IPvY, turning IPvX packet into IPvY if the packet is destined to IPvY network, or turning IPvY packet into IPvX if the packet is destined to IPvX network. Usually, translation happens on the IPvX-IPvY border, so the translator would be an AFBR (Address Family Border Router). Suppose Host1 (H1) in IPvX network is the communication initiator, and Host2 (H2) in IPvY network is the remote end. H1 has to learn the in-protocol address (IPvX) used by H2 before the communication starts. Later the data packets with this address as destination will be forwarded to the translator, translated into IPvY and forwarded to H2. On the other hand, the IPvY source address for these packets, i.e. the IPvY address used by H1, is assigned or calculated by the translator during the translation. Along with these addressing operations, routing support should guarantee that the IPvX packets destined to H2 IPvX address and the IPvY packets destined to H1 IPvY address are forwarded through the translator. IPv4-IPv6 trans-lation is similar to IPv4 NAT on some certain level. However, applying

translation to large-scale networks and asymmetric IPv4-IPv6 address space is much more challenging than that to the scenario of ordinary IPv4 NAT.

3.2. Stateless Translation

SIIT (Stateless IP/ICMP Translation Algorithm) [11] is an early stateless translation mechanism. It proposes the basic principle of IPv4-IPv6 stateless translation and the algorithm for IP/ICMP semantic conversion (Figure 6). The SIIT address scheme is based on the assumption that every IPv6 host in a network possesses an IPv4 address. The IPv6 address of each IPv6 host is generated by adding the IPv6 prefix 0:ffff:0:0:0/96 before the IPv4 address. This type of IPv6 addresses is called IPv4-translated address, which is assigned to an IPv6 host and potentially matches an IPv4 address. On the other hand, the IPv6 address of an actual IPv4 host is generated by adding a different IPv6 prefix ::ffff:0:0/96 before the IPv4 address. This type of IPv6 addresses is called IPv4-mapped address, which is mapped from an IPv4 address to represent an IPv4 host in an IPv6 network. However, SIIT specifies neither how an IPv6 host retrieves an IPv4-translated address, nor how an IPv6/IPv4 host learns the IPv4-mapped/IPv4-translated address of the remote end. Routing support for the address mapping rules is not specified either. Following the two address mapping rules, the address translation can be performed by algorithmic mapping.

4.TUNNELING MECHANISMS

4.1 Basic Principle of Tunneling

Tunneling is used to achieve heterogeneous traversing. The basic principle of tunneling is shown in Figure 9. To deliver IPvY packets across the IPvX network in the middle, we deploy two tunnel endpoints on the border of the IPvX net-work. When the ingress endpoint (Tunnel endpoint 1) receives an IPvY packet from the IPvY network, it encapsulates the IPvY packet with IPvX protocol header and puts the whole IPvY packet into the payload of the new IPvX packet. Then the IPvX packet is forwarded through the IPvX network. When the egress endpoint (Tunnel endpoint 2) receives the encapsulated IPvX packet, it decapsulates the packet, extracts the original IPvY packet and forwards it to the IPvY network. When performing the encapsulation, Endpoint 1 should fill in the IPvX destination address in the encapsulation header properly, which guarantees that the encapsulated packet will be forwarded to endpoint 2? Usually the IPvX address of endpoint 2 is figured out and used as the encapsulation desti-nation address. Tunneling is actually a generic technology; under the scope of IPv6 transition, tunneling can achieve communications between IPv4 networks/hosts across an IPv6 network (IPv4-over-IPv6), and communications between IPv6 networks/hosts across an IPv4 network (IPv6-over-IPv4).

4.2 Host-to-host Tunnel Mechanisms

6over4 (Transmission of IPv6 over IPv4 Domains without Explicit Tunnels) [9] is a tunnel mechanism between hosts, used to achieve IPv6 communication between isolated IPv6-capable hosts across an IPv4-only network. The idea of 6over4 is leveraging IPv4 multicast to build a virtual “LAN” among IPv6-capable hosts. In other words, it is an IPv6 Ethernet-over-IPv4 multicast tunnel. While it does not require any address scheme or binding, the control plane complexity is actually quite high: the host and the network infrastructure have to fully support IPv4 multicast; special efforts are required to enable IPv6 LAN protocols such as SLAAC and ND to work on the virtual LAN. Subsequently the failure mode would be quite complex.

5. MECHANISM USAGE & DEPLOYMENT STRATEGY

The former two sections provide an overview of the main-stream IPv6 transition mechanisms that have been proposed. Table III maps the proper mechanisms into all the scenarios of heterogeneous inter-connection and heterogeneous travers-ing. However, these mechanisms are still not designed in a very practical environment of ISP networks. It still causes confusions for operators when selecting among so many mechanisms and making deployment plans. This section will discuss how to choose and deploy the transition mechanisms.

5.1 *Transition Requirements in ISP networks*

A practical ISP network contains ISP backbone and edge networks. The backbone network is usually connected with provider ISPs, customer ISPs, peer ISPs, and edge networks inside the ISP, typically all through BGP. The border routers of the backbone form an iBGP

mesh. The scale of the backbone network is usually limited; therefore IPv4 address shortage is not a concern. The routers in the backbone usually have the highest upgrading priority. An edge network (regional and access network, campus network, etc.) is attached to the backbone in the upward direction and faces end users in the downward direction. The edge network is relatively independent from the backbone and provides the infrastructure services by itself. The edge network has the aggregating characteristic, all along from end users to the backbone entrance. Due to the large population of end users, most often the edge network will not provision public IPv4 addresses freely in the recent future. Typically, a large number of routers, access devices and servers in the existing edge network cannot support IPv6 well. A considerable, costly upgrade is needed to support native IPv6. Besides, although the mainstream operating systems on end user devices are IPv6-ready, not a lot of applications are actually IPv6-capable.

5.2 Typical Case Study

CERNET2 backbone: CERNET (China Education and Research Network) is one of the earliest ISPs which have activated IPv6. The IPv6 project of CERNET was launched in Sept 2003 and has been providing IPv6 transport service for campus networks since Jun 2004. Currently, the CERNET2 backbone is a pure IPv6 network containing 20 PoPs and 1 IXP. The clients include over 100 campus networks. A CERNET campus network provides native dual-stack access for end users, with the IPv4 and IPv6 campus gateways separated. The IPv4 gateway connects to CERNET IPv4 backbone, while the IPv6 gateway connects to CERNET2 IPv6 backbone. It is of great significance that CERNET2 can provide IPv4 transport besides IPv6 transport. On one hand, the operator can transfer a portion of IPv4 traffic from CERNET to CERNET2, reducing the load of CERNET IPv4 backbone and leveraging the CERNET2 infrastructure. On the other hand, in a long term CERNET2 backbone will replace CERNET backbone and become the major backbone eventually. At that time, it will be a basic requirement of CERNET2 to support IPv4 transport.

6. CONCLUSION

In IPv4 route devices could not able to connect after 255 routers because there is a behavior of internet protocol address (IPv4) address they could ping up to 255 routers only and secondly ipv4 address are 4.3 billion and when these all address will used in future then it cannot use IPv4 because of limited numbers.So to solve these above problems a new method is used instead of using IPv6 because it is difficult to change the whole world network from IPv4 to IPv6. Given that IANA has eventually run out IPv4 address space, the Internet is bound to enter the IPv6 era. Nevertheless, IPv4 networks will coexist with IPv6 networks for a long time during the transition. The IPv6 transition process should be steady and smooth. Therefore, the IPv4-IPv6 coexisting networks should sustain the availability of both IPv4 and IPv6, and support IPv4-IPv6 interconnection as well.

This paper analyzes the basic problem of heterogeneous traversing and heterogeneous interconnection in IPv6 transition, introduces the principle of tunneling and translation techniques, and reviews the mainstream tunneling and translation mechanisms. The aspects of address scheme and routing, heterogeneous addressing, data forwarding, performance, security and scalability are studied for these mechanisms. The paper also summarizes the pros and cons, and subsequently application scenarios of every mechanism. A series of mechanisms including Softwire Mesh, 6RD, DS-Lite, 4over6, MAP, IVI and NAT64 are recommended as feasible solutions to filling in their respective application scenarios. Based on these recommendations, this paper studies the characteristics and transition requirements of practical ISP networks, and proposes the transition strategies for both backbone and edge networks by selecting and deploying the recommended mechanisms. During the IPv6 transition process, the above problems are the essential challenges that need to be overcome. They are all non-neglect able problems in promoting IPv6, and hopefully they are solvable with the combination of techniques and business means. With the continuous development of IPv6 techniques, IPv6 transition techniques, and the step-by-step follow-ups of vendors, ISPs, ICPs and end users, IPv6 will finally accomplish the transition process and take charge of the future Internet.

References

[1] Dipti Chauhan, Sanjay Sharma,"A Survey on Next Generation Internet Protocol:IPv6", International Journal of Electronics and Electrical Engineering Vol. 2, No. 2, June, 2014

[2] Ramesh Chand Meena, Mahesh Bundele,"A Review on Implementation Issues in IPv6 Network Technology", International Journal of Engineering Research and General Science, Vol. 3, Issue 6, November-December, 2015

[3] Srinidhi K S, Smt. R. Anitha, A.V.Srikantan,"Tunnel based IPv6 Transition with automatic bandwidth management", International Journal of Computer Science and Mobile Computing, Vol. 3 Issue. 6, June- 2014, pp. 360-366, 2014.

[4] Mohd.Khairil Sailan, Rosilah Hassan, Ahmed Patel,"A Comparative Review of IPv4 and IPv6 for Research Test Bed", International Conference on Electrical Engineering and Informatics, 5-7 August 2009

[5] [Online] Available: http://www.arin.net.com

[6][Online]Available:http://www.google/wikipedia.com

[7] "IPv6 Adoption Monitor," University of Pennsylvania, Comcast and Tsinghua University, Tech. Rep., 2010. [Online]. Available: http://mnlab-ipv6.seas. Upenn .edu /monitor

[8] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," 2001, IETF RFC 3056.

[9] B. Carpenter and C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels," 1999, IETF RFC 2529.

[10] G. Tsirtsis and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)," 2000, IETF RFC 2766.

[11] E. Nordmark, "Stateless IP/ICMP Translation Algorithm(SIIT)," 2000, IETF RFC 2765.

[12] K. Tsuchiya, H. Higuchi, and Y. Atarashi, "Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)," 2000, IETF RFC 2767.