Technical Comparison between IPv4 & IPv6 and Migration from IPv4 to IPv6

Ashis Saklani[1], S. C. Dimri[2]

Assistant Professor, Department of Computer Science, H.N.B Garhwal Central University, Srinagar Garhwal, Uttarakhand, India

Professor, Head of Department, Department of Computer Applications, Graphic Era University, Dehradoon, Uttarakhand, India

Abstract: ***These days IPv6 over IPv4 tunnels are widely used to form the Global IPv6 Internet. This paper demonstrates the two tunnels and shows when to immigrate from IPv4 to IPV6.Then the risks of immigration are discussed step by step.***

Keywords: Nat, IPv6, IPv4, IETF, DHCP

1. Introduction

Now days IPv6 over IPv4 tunnels are widely used to connect large regional IPv6 networks, because it is relatively hard to construct an international or cross-continent native IPv6 network. This makes the characteristics of IPv6 over IPv4 tunnels very vital to the performance of the global IPv6 Internet. Migrating from IPv4 to IPv6 in an instant is impossible because of the huge size of the Internet and of the great number of IPv4 users. Moreover, many organizations are becoming more and more dependent on the Internet for their daily work, and they therefore cannot tolerate downtime for the replacement of the IP protocol. As a result, there will not be one special day on which IPv4 will be turned off and IPv6 turned on because the two protocols can coexist without any problems. The migration from IPv4 to IPv6 must be implemented node by node by using auto configuration procedures to eliminate the need to configure IPv6 hosts manually. This way, users can immediately benefit from the many advantages of IPv6 while maintaining the possibility of communicating with IPv4 users or peripherals. Consequently, there is no reason to delay updating to IPv6.In this paper we are going to investigate the IPV6 and the IPV4 and when to decide to immigrate to IPV6.

2. Brief History

In 1991, the IETF decided that the current version of IP, called IPv4, had outlived its design. The new version of IP, called either IPng (Next Generation) or IPv6 (version 6), was the result of a long and tumultuous process which came to a head in 1994, when the IETF gave a clear direction for IPv6. IPv6 is designed to solve the problems of IPv4. [1].It does so by creating a new version of the protocol which serves the function of IPv4, but without the same limitations of IPv4. IPv6 is not totally different from IPv4: what you have learned in IPv4 will be valuable when you deploy IPv6.The differences between IPv6 and IPv4 are in five major areas: addressing and routing, security, network address translation, administrative workload, and support for mobile devices. IPv6 also includes an important feature: a set of possible migration and transition plans from IPv4. Since 1994, over 30 IPv6 RFCs have been published. Changing IP means changing dozens of Internet protocols and conventions, ranging from how IP addresses are stored in DNS (domain name system) and applications, to how datagram's are sent and routed over Ethernet, PPP, Token Ring, FDDI, and every other medium, to how programmers call network functions. The IETF, though, is not so insane as to assume that everyone is going to change everything overnight. So there are also standards and protocols and procedures for the coexistence of IPv4 and IPv6: tunneling IPv6 in IPv4, tunneling IPv4 in IPv6, running IPv4 and IPv6 on the same system (dual stack) for an extended period of time, and mixing and matching the two protocols in a variety of environments.

3. Internet Protocol Version 4 (IPV4)

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet. IPv4 is still by far the most widely deployed Internet Layer protocol. It uses a 32 bit addressing and allows for 4,294,967,296 unique addresses. [2] Even though the name seems to imply that it's the fourth generation of the key Internet Protocol, version 4 of IP was the first that was widely used in modern TCP/IP. IPv4, as it is sometimes called to differentiate it from the newer IPv6, is the Internet Protocol version in use on the Internet today, and an implementation of the protocol is running on hundreds of millions of computers. It provides the basic datagram delivery capabilities upon which all of TCP/IP functions and it has proven its quality in use over a period of more than two decades.

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 than are possible with IPv4. Like IPv4, IPv6 is an internet-layer protocol for packet switched 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.

5. Limitations of IPv4

Since the 1980s it has been apparent that the number of available IPv4 addresses is being exhausted at a rate that was not initially anticipated in the design of the network. This was the driving factor for the introduction of class full networks, for the creation of CIDR addressing. [3] But despite these measures the IPV4 addresses are being consumed at an alarming rate and it is estimated that 2010 would be the last year for IPV4, some sources say they may last until 2012. Primary reason for IPV4 exhaustion is huge growth in number of internet users, mobile devices using Internet connection and always on devices such as ADSL modems and cable modems. This brings us to the development and adoption of IPV6 as an alternate solution.

6. 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.[4],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. 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. 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. With IPv6, multicast is a requirement. IPv6 also defines a new kind of service, called "anycast." Like multicast, anycast has groups of nodes which send and receive packets. But when a packet is sent to an anycast 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 anycast technology. Another aspect of VPNs built into IPv6 is QoS (Quality of Service). IPv6 supports the same QoS features as IPv4, including the DiffServ 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. 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.

7. 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 deployments 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 [5]:

- Your IPv4 network or NAT implementation needs to be fixed or extended.
- You are running out of address space.
- You want to prepare your network for applications that are based on advanced features of IPv6.
- 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.
- 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.

8. 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 [6].The key goals of the migration are as follow:

- IPv6 and IPv4 hosts must interoperate.
- The use of IPv6 hosts and routers must be distributed over the Internet in a simple and progressive way, with a little interdependence.
- 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:
- Possibility of a progressive and nontraumatic transition: IPv4 hosts and routers can be updated to IPv6, one at a time, without requiring other hosts or routers to be updated simultaneously.
- 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.
- Addressing simplicity: When a router or a host is updated to IPv6, it can also continue to use IPv4 addresses.
- Low initial cost: No preparatory work is necessary to begin the migration to IPv6. Mechanisms used by SIT include the following [7]:
- A structure of IPv6 addresses that allows the derivation of IPv6 addresses from IPv4 addresses.
- 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.
- A technique to encapsulate IPv6 packets inside IPv4 packets (tunneling) to allow IPv6 packets to traverse clouds not yet updated to IPv6.

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. The SIT approach guarantees that IPv6 hosts can interoperate with IPv4 hosts initially on the entire Internet. When the migration is completed, this interoperability will be locally guaranteed for a long time. This capability allows for the protection of investments made on IPv4; simple devices that cannot be updated to IPv6—for example, network printers and terminal servers—will continue to operate with IPv4 until they are no longer used. The possibility of a gradual migration allows manufacturers to integrate IPv6 in routers, operating systems, and network software when they think that implementations are stable and users to begin the migration at a time they consider the most appropriate. As with any migration, there are risks involved. The risks may be described as follows:

- If there is a problem, many users may be affected. A phased approach to migrate a few users at a time may be a 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.
- 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.
- 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.

9. Conclusion

Migrating from IPv4 to IPv6 in an instant is impossible because of the huge size of the Internet and of the great number of IPv4 users. Moreover, many organizations are becoming more and more dependent on the Internet for their daily work, and they therefore cannot tolerate downtime for the replacement of the IP protocol. As a result, there will not be one special day on which IPv4 will be turned off and IPv6 turned on because the two protocols can coexist without any problems. In this paper we investigate when to immigrate from IPv4 to IPv6 and the risks of this immigration.

References

[1] "IPv6 Headers", Online: http://www.cu.IPv6tf.org/literatura/chap3.pdf, chapter 3, pp. 40-55, Des 12 1997.

[2] S. Deering, R. Hinden, Internet Protocol Version 6 (RFC2460), 1998

[3] IPv4/IPv6 Translation Technology, Masaki Nakajima, Nobumasu Kobayashi,2004

[4] The Benefits of Using Internet Protocol Version 6 (IPV6) by Amer N.AbuAli, Ismail Ghazi Shayeb, Khaldoun Batiha,Haifa Yabu Aliudos, Vol. 5. n. 6, pp. 583-587.

[5] Patrick Grossetete, Ciprian P. Popoviciu, Fred Wettling,"Global IPv6 Strategies: From Business Analysis to Operational Planning" Online: http://media.techtarget.com/searchNetworking/downloads/IPv4_or_IPv6.pdf, 1st Edition, chapter 2, pp. 18-53, May 15, 2008.

[6] Charles M. Kozierok, "TCP/IP Guid A Comprehensive, Illustrated Internet Protocols reference", chapter 25, pp.373-381, October 2005.

[7] Hitesh Ballani, Paul Francis, Cornell University, Ithaca, NY, "Understanding IP Anycast".

[8] Xuan Zhang et al : 2010 Information security risk management framework for cloud computing environments,

[9] Mehnet Yeldiz et al: 2010 A layered security approach for cloud computing infrastructure,

[10] Clancy, T.C., Kiyavash, N., Lin, D.J.:2003 Secure smartcard-based fingerprint authentication. In: Proceedings ACM SIGMM 2003 Multimedia, Biometrics Methods and Workshop, pp. 45-52

[11] Neil Timothy Spring, Efficient discovery of network topology and routing policy in the Internet, Ph Dissertation, University of Washington, year 2004, Available from www.cs.umd.edu/-nspringlpapers/nspring-thesis

[12] Yehuda Mek, Anat Bremler-Barr, and Shemer Schwarz, Improved BGP Convergence via Ghost Flushing, INFOCOM 2003. Twenty-Second Annual Joint Conferences of the IEEE Computer and Communications. IEEE Societies Publication Date: 30 March-3 April 2003 Volume: 2, On page(s): 927-937 vol 2.

Author Profile

Ashis Saklani has done M.Tech in Computer Science from Karnataka University and MCA from Graphic Era Institute of Technology (Now Graphic Era University) Dehradoon in 2004.He is CISCO and Microsoft Certified Professional. He worked as a VPN Support Engineer at HCL Infinet, Noida. Presently he is working as Assistant Professor, at H.N.B Garhwal Central University, Srinagar, Uttarakhand, India.

Dr. S. C. Dimri is a Research scholar. He has built many Milestones in the Horizon of Network Security, Computer Networks and Operational Research. Presently he is working as HOD (Head of Department) in Computer Application Department. Graphic Era University, Dehradoon, Uttarakhand, India