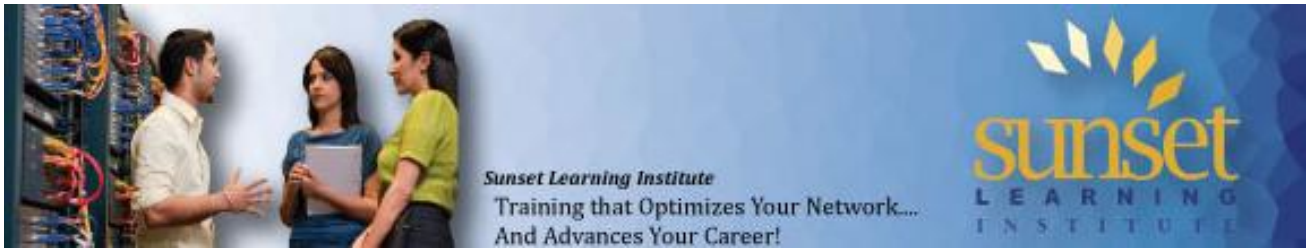


Migration from IPv4 to IPv6

Tuan Nguyen, Sunset Learning Institute Cisco Instructor

The current version of the Internet Protocol IPv4 originally developed in the 1970's and officially published in 1981 (RFC 791) severed its purpose until the early 1990's. By 1992 Internet expansion and the uptake of address space exposed limitations as to the number of actual address spaces that would be available with the increase number of devices being added to the world wide web, pushing the IPv4 standard to its threshold. As these limitations were recognized changes were initiated by the Internet Engineering Task Force (IETF) in 1994 for an upgrade to IPv6 (RFC 2460). Currently IPv6 network penetration is low however it is expected to grow, as IPv4 depletion is eminent.

As the number of interconnect computers, the cloud, use of BYODs and other devices grow dramatically, the need for change will drive service providers to make the switch. The difference between IPv4 and IPv6 is in the address format where IPv4 use 32 bit (4 bytes) address while IPv6 uses 128 bit (16 bytes). IPv6 allows for much longer address(s) so it is possible to technically overcome the IPv4 address depletion issues and include service features without rewriting the protocol.

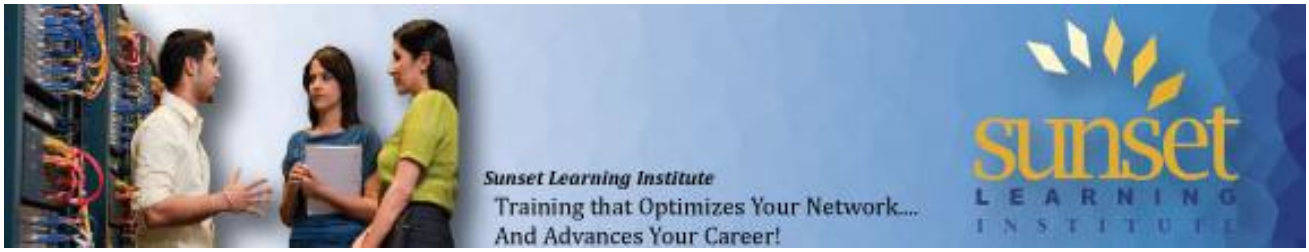
One of the reasons for slow movement to IPv6 is the cost of migration to the new format with no immediate revenue exchange for the upgrade. However this is short sighted as the depletion of address spaces and the advent of more internet devices and the growth of the cloud, service providers who do not migrate are going to find it difficult to efficiently service the higher demand placed on their networks. IPv6 has built in security features, stronger flow control and easier authentication functionality. In short, IPv6 is the future and holds the promise of end-to end security, QOS and simplified management while increasing the networks capacity to service more users.

Top 10 Features that make IPv6 "greater" than IPv4

#1 – IPv6 provides a substantially larger IP address space than IPv4

Every computer or online device that needs to connect to the Internet requires a globally unique IP address. IPv4 uses 32 bits for an IP address that allows about 4 billion unique IP addresses. When IPv4 was introduced in the 1970s and accepted as the protocol for the Internet, they did not foresee this explosion in the popularity of the Internet or the extent to which online technologies would become all pervasive. It was therefore firmly believed that these 4 billion addresses would be sufficient to cover any future growth of the Internet.

IPv6 uses 128 bits for IPv6 addresses which allows for 340 billion billion billion billion (3.4x1038) unique addresses. To get an idea of the scale involved, consider the entire IPv4 space as being contained in an iPod, then the new IPv6 space would be the size of the Earth. From these numbers, it can be seen that with IPv6, it is possible to provide billions of addresses to each person and ensure that any device that has to be connected to the Internet will have a unique IP address.



The first advantage of an enhanced address space is that in the absence of NAT, there is less complexity in the network hardware and software, and configuring a network becomes much simpler. Secondly, it makes it possible to truly envisage a networked home wherein the different gadgets and appliances would be on the network which would require that each such device have a unique IP address. Finally, the large availability of IP addresses removes any obstacles that existed previously in the full deployment of wireless and mobile devices.

#2 – Ipv6 provides better end-to-end connectivity than IPv4

The most exciting applications to emerge in recent days are peer-to-peer applications such as multi-player online games, video-conferencing (streaming media), file sharing and VoIP. In peer-to-peer networking, a group of computers can communicate directly with each other and do not need a central server. Peer-to-peer applications demand end-to-end connections between unique IP addresses.

IPv6 with its large address space no longer requires NAT and can ensure true end-to-end connectivity. This means peer-to-peer applications like VoIP or streaming media can work very effectively and efficiently with IPv6.

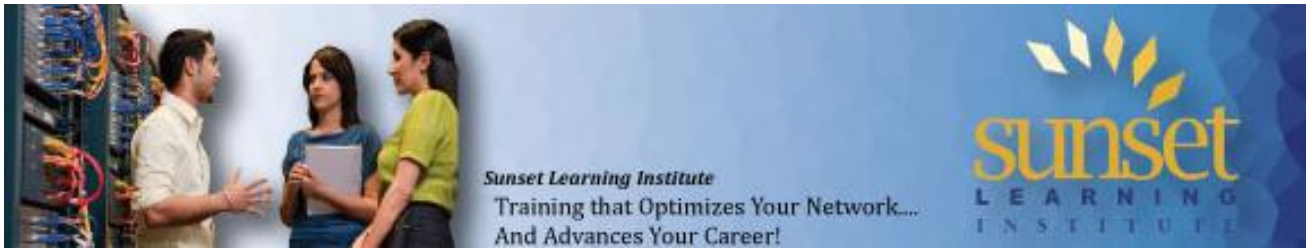
#3 – Ipv6 has better ability for autoconfiguring devices than IPv4

Whenever a node plugs in and wants to be part of a network, IP address information and router information is required to properly configure the node and get it running. In the past, when there were fewer devices and computers in a network running IP, almost all of them were statically configured and IP addresses were manually assigned. However, with the rapid proliferation of personal computers (PC) and other IP-enabled devices, for efficient device management and reusing of resources, it became absolutely essential to consider some kind of autoconfiguration.

IPv4 uses the stateful address autoconfiguration protocol, Dynamic Host Configuration Protocol (DHCP). In the stateful autoconfiguration model, a host obtains the interface addresses as well as other required information such as the configuration information and parameters from a server. The DHCP server maintains a manually administered list of hosts and keeps track of which addresses have been assigned to which hosts.

IPv6 offers automatic configuration and more importantly, simple configuration mechanisms. Known as plug-and-play autoconfiguration, these capabilities are way beyond what IPv4 currently offers. IPv6 offers DHCPv6, which is an autoconfiguration similar to IPv4 DHCP and offers stateful address autoconfiguration. In addition, IPv6 also offers stateless or serverless address autoconfiguration.

In stateless autoconfiguration, a host can automatically configure its own IPv6 address and does not need any assistance from a stateful address server. Entire IPv6 prefixes rather than just an address are delivered to a device. This particular feature enables routers to easily autoconfigure their interfaces and can be used very effectively in broadband access networks to dynamically provide customer gateways.



#4 – <u>Ipv6 contains simplified Header Structures leading to faster routing as compared to IPv4</u>

The present IP uses a Datagram service to transfer packets of data between point to point using routers. The IPv4 packet header structure contains 20 bytes of data, such that it contains within the header, all possible options thereby forcing intermediate routers to check whether these options exist and if they do, process them before forwarding them. In the IPv4 packet header, these options have a certain maximum permitted size.

When compared to IPv4, IPv6 has a much simpler packet header structure, which is essentially designed to minimize the time and efforts that go in to header processing. This has been achieved by moving the optional fields as well as the nonessential fields to the extension headers that are placed only after the IPv6 header. Consequently, the IPv6 headers are processed more efficiently at the intermediate routers without having to parse through headers or recompute network-layer checksums or even fragment and reassemble packets. This efficiency allows for reduced processing overhead for routers, making hardware less complex and allowing for packets to be processed much faster.

Another feature of the IPv6 header structure is that the extension header allows for more flexible protocol inclusions than what IPv4 does. In contrast, IPv6 extension headers have no such restriction on the maximum size. They can be expanded to accommodate whatever extension data is thought necessary for efficient IPv6 communication. In fact, a typical IPv6 packet contains no extension header and only if intermediate routers or the destination require some special handling, will the host sending the packets add one or more extension headers depending on the requirement. This new extension header makes IPv6 fully equipped to support any future need or capabilities.

#5 – <u>Ipv6 provides better security than IPv4 for applications and networks</u>

The Internet has functioned for the last three decades with IPv4 as the underlying protocol. However, because of this end-to-end model, IPv4 was designed with almost no security in mind and assumes that the required security will be provided at the end nodes. For example, consider an application such as email that may require encryption services - under IPv4, it is the responsibility of the email client at the end nodes to provide those services. Today, the Internet faces threats such as Denial of Service Attacks, Malicious code distribution, Man-in-the-middle attacks, Fragmentation attacks and Reconnaissance attacks.

In IPv6, **IPSec** is a major protocol requirement and is one of the factors in ensuring that IPv6 provides better security than IPv4.

IPSec contains a set of cryptographic protocols for ensuring secure data communication and key exchange. The main protocols used are:

1.**Authentication Header** (AH) protocol, which enables authentication and integrity of data.

2.**Encapsulating Security Payload** (ESP) protocol, which enables both authentication and integrity of data as well as privacy of data.

3.**Internet Key Exchange** (IKE) protocol. This protocol suite helps to initially set up and negotiate the security parameters between two end points. It then also keeps track of this information so that the communication stays secure till the end.

Thus, IPv6 ensures that there are end-to-end security mechanisms that will provide authentication and encryption abilities to all applications and thereby eliminates the need for applications themselves to have integrated support for such abilities. The added benefit of using the same security mechanisms for all applications is that setting up and administering security policies becomes a lot simpler. IPv6 allows for complete end-to-end security thereby allowing for a new set of personalized services to be deployed such as mobile e-commerce services that rely on secure transactions.

#6 – Ipv6 gives better Quality of Service (QoS) than IPv4

The present IP uses a Datagram service to transfer packets of data between point to point using routers. The IPv4 packet header structure contains 20 bytes of data, such that it contains within the header, all possible options thereby forcing intermediate routers to check whether these options exist and if they do, process them before forwarding them. In the IPv4 packet header, these options have a certain maximum permitted size.

QoS is given a special boost in the IPv6 protocol with the IPv6 header containing a new field, called Flow Label field that defines how particular packets are identified and handled by the routers. The Flow Label field allows packets that belong to a particular flow, in other words, that start from a particular host and head to a particular destination, to be identified and handled quickly and efficiently by the routers.

The **Flow Label Field** thus ensures that there is more efficient delivery of information from one end to another without the possibility of it being modified by intermediate systems. This ensures a high degree of QoS especially for peer-to-peer applications like VoIP and other real-time applications.

#7 – Ipv6 provides better Multicast and Anycast abilities compared to IPv4

In a multicast technique a packet is copied from one stage down to another in a hierarchical tree-like structure, instead of sending it from the source directly. This means that there are fewer packets in the network thereby optimizing bandwidth utilization and also reducing the resources required at each network node. This multicast technique is particularly useful when streams of information have to be made available to a wide variety of connected devices and not just one single destination. For example multicast technique is used to relay audio data, video data, news feeds, and financial data feeds and so on.

IPv6 extends the multicasting capabilities of IPv4 by offering a large multicast address range. Obviously, this limits the degree to which the information packets have now to be propagated and significantly improves the network efficiency.

IPv6 also improves dramatically on the concept of anycast services, which is available, though in a very minimal form in IPv4. In anycast services, packets are not sent to all the nodes in the network but only to the nearest reachable member. A typical application where anycast would be of tremendous use is say, while discovering a server of a given type e.g. a DNS server, among a group of servers. It will also

provide redundant paths to other servers so that if for some reason, the route to the primary server becomes unavailable, in the next session, a connection will be provided to the next server in the group.

#8 – <u>Ipv6 offers better mobility features than IPv4</u>

When we consider IP mobility features we are essentially considering features that would be useful for:

Mobile devices, which can change their location but would like to retain existing connections. **Mobile networks** that provide mobility to a group of devices.

Ad-hoc networking in which some of the dives stay connected to the network or in the vicinity of the network only for the short duration of a communications session.

When a mobile node is not at home, it conveys information about its present location, also called, care-of-address to the home agent. Now if a node wants to communicate with this mobile mode, it will first send the information packets to the home address. The home agent receives these packets and using a table, sends these packets to the care-of-address of the mobile node.

With IPv6, mobility support is mandatory by the use of Mobile IPv6 (MIPv6). Route optimization is a built-in feature for mobile IPv6. Further, features like Neighbor Discovery and Address Auto-configuration allow mobile nodes to function in any location without needing the services of any special router.

MIPv6 can be used to achieve seamless mobility by allowing handovers between different access technologies say from example from a cellular network to a wireless network, with minimum interruption to ongoing connections. There is no ingress-filtering problem in Mobile IPv6 because the correspondent node uses the care-of address as the source address.

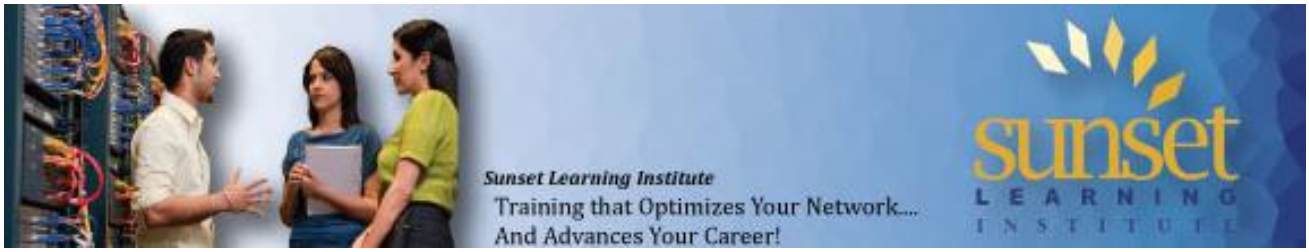
These devices increasingly demand delivery of converged voice, video and data, which is made possible through a standard called the IP Multimedia Subsystem (IMS) standard. However IMS requires that each mobile device have a unique IP address, which is a persistent IP address in order to ensure full bi-directional services.

IPv6 through its large address space ensures that each mobile device can have its own unique IP address. Further, Mobile IPv6 makes use of the extension headers to add powerful capabilities such as route optimizations between mobile nodes, when roaming between different 3G networks.

#9 – <u>Ipv6 offers ease of administration over IPv4</u>

When an existing network is to be expanded or two networks to be merged, or when service providers are changed, a network needs to be renumbered, as a new address scheme will be assigned to it.

IPv6 provides capabilities so that network renumbering can happen automatically. Thus, network renumbering with IPv6 will no longer requires manual reconfiguration of each host and router and makes for smoother switchovers or mergers.



Another useful administrative feature of IPv6 is its multihoming technique. In this simultaneous connections are established to two ISPS. When service to one ISP is lost, there is a back-up connection to the Internet. This ensures far greater reliability of services, as there is more than one path from the host to the destination.

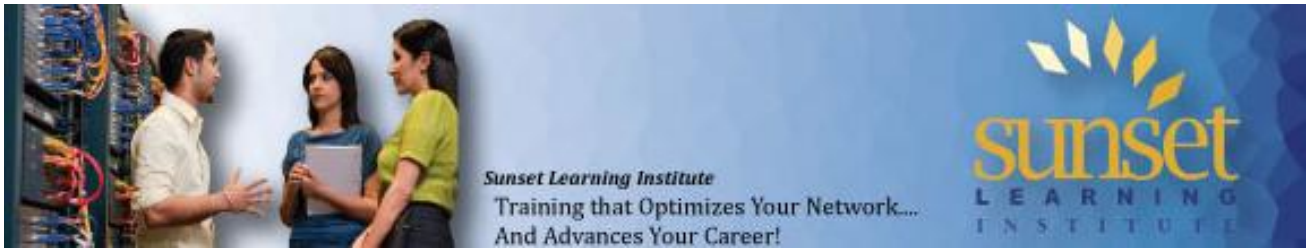
#10 – Ipv6 follows the key design principles of IPv4, thereby permitting a smooth transition from IPv4

IPv4 has been successfully deployed the world over for many years now and its popularity is a testament to the success of its design. IPv6 follows many of the same design features that made IPv4 so successful. This makes it possible to have a smooth transition from IPv4 to IPv6. There are many commercially attractive applications in the market today that require IPv6 and may tempt many to go in for a rapid transition to IPv6. However, IPv4 applications will be used for some time to come and the process of transition from IPv4 to IPv6 must be a gradual one.

A successful IPv4 to IPv6 transition mechanism is one in which IPv6 elements are incorporated into the network while at the same time compatibility is maintained with the pre-existing, large base of IPv4 hosts and routers. Thus, for some time to come, IPv6 hosts and routers must interact and function with the existing IPv4 network infrastructure.

A number of such transition mechanisms have been defined that allow for the two networks to co-exist till such a time that a complete migration to IPv6 is not feasible.

Using **Dual IPv4/IPv6 Stack** implementations such as **Tunneling,** Dual IPstack Using Network Address and Protocol Translators.



Things you should know before migrating from IPv4 to IPv6

Internet Service Provider (ISP) – Make sure your ISP is providing IPv6 services - For web and email you can run them dual-stack, create A and AAAA records for them, and they should work. Things like logfile analysis need to be made v6-aware. Ideally you need IPv6 PTR records, especially for email.

Network Infrastructures - Your routers need to support IPv6. If not, you can run a 6to4 tunnel but that's not really production grade unless you have a contract with a tunnel provider. Generally, computers and routers etc. have been IPv6-capable for a while. Switches don't care.

The Firewalls - You need to duplicate your firewall rules in IPv6. If you are running NAT because you could not get enough IPv4 addresses, you could just drop it and run v6. If you are relying on NAT for security, you need to add firewall rules.

DHCP - IPv6 routers advertise routes and addresses so everything gets online, but you need DHCP6 to tell them what DNS to use. You can end up with things working but not having well-defined addresses - i.e. you can lose track of what's on your network unless you keep track of what ports everything's plugged into and do MAC authentication on wifi.