
Transitioning to IPv6
Overview of:
Issues,
Strategies,
Tools &
Timelines

Issues: What's wrong with IPv4?

- Nothing. It works well, but:
- We're simply *running out* of the 4.3 billion IPv4 addresses.
- When will IPv4 addresses be depleted?
  - Estimates vary – several years ago it was 2020-2025
  - Two years ago it was 2017
  - Today it looks like 2012, though some say by 2011.
  - This is especially true in Asia and other countries where demand for Internet-connected devices is skyrocketing.

Will there be enough IPv6 addresses?

- Since IPv6 addresses are 128 bits long, the theoretical address space if all addresses were used is 2^{128} addresses. This number, when expanded out, is 340,282,366,920,938,463,463,374,607,431,768,211,456, which is normally expressed in scientific notation as about $3.4*10^{38}$ addresses. That's about 340 trillion, *trillion*, ***trillion*** addresses. As I said, it's pretty hard to grasp just how large this number is. Consider:
- It's enough addresses for many trillions of addresses to be assigned to every human being on the planet.
- The earth is about 4.5 billion years old. If we had been assigning IPv6 addresses at a rate of 1 billion per second since the earth was formed, we would have by now used up less than one ***trillionth*** of the address space.

IPv6 Design Goals

- Larger Address Space
- Better Management of Address Space: IPv6 should not only include more addresses, but a more capable way of dividing the address space and using the bits in each address.
- Elimination of "Addressing Kludges": Technologies like NAT are effective "kludges" that make up for the lack of address space in IPv4. IPv6 eliminates the need for NAT.
- Easier TCP/IP Administration: resolve labor-intensive requirements of IPv4 like IP address configuration. DHCP only partially solved the problem. Auto-configuration of hosts and renumbering of IP addresses
- Modern Design For Routing: IPv6 created specifically for efficient routing including future flexibility
- Better Support For Multicasting: (included in IPv4, but slow)
- Better Support for Security
- Better Support for Mobility
- Support for Quality of Service

IPv4 versus IPv6

IPv4	IPv6
Addresses are 32 bits (4 bytes) in length.	Addresses are 128 bits (16 bytes) in length
Address (A) resource records in DNS to map host names to IPv4 addresses.	Address (AAAA) resource records in DNS to map host names to IPv6 addresses.
Pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
IPSec is optional and should be supported externally	IPSec support is not optional
Header does not identify packet flow for QoS handling by routers	Header contains Flow Label field, which Identifies packet flow for QoS handling by router.
Both routers and the sending host fragment packets.	Routers do not support packet fragmentation. Sending host fragments packets

IPv4	IPv6
Header includes a checksum.	Header does not include a checksum.
Header includes options.	Optional data is supported as extension headers.
ARP uses broadcast ARP request to resolve IP to MAC/Hardware address.	Multicast Neighbor Solicitation messages resolve IP addresses to MAC addresses.
Internet Group Management Protocol (IGMP) manages membership in local subnet groups.	Multicast Listener Discovery (MLD) messages manage membership in local subnet groups.
Broadcast addresses are used to send traffic to all nodes on a subnet.	IPv6 uses a link-local scope all-nodes multicast address.
Configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

Summary of IPv6 Advantages over IPv4

- Improved mobility
- Potentially better multicast capabilities
- Easier extensibility
- More efficient packet processing
- Cleaner security capabilities
- Real driver: having enough addresses to support the continued growth of the Internet and IP services into the forseeable future.

What's the rest of the world doing?

- Japan and South Korea -*Japan was first country to move forward with a concerted, government-supported IPv6 initiative – all driven by the consumer electronics industries. South Korea is not far behind Japan.*
- China and India – *China has a government-let and funded IPv6 mandate called the China Next-Generation Internet (CNGI). China highlighted its progress with IPv6 at the 2008 Olympics – Lighting control systems and security cameras throughout Olympic venues operated over IPv6. India's economy is not expanding as fast as China's so has only recently begun its expansion. IPv6 is not yet being as aggressively pushed as it is in China, but the motivations to do so are the same.*
- Europe - *More IPv6 address allocations have been made to Europe than to any other region of the world. This is chiefly due to the number of individual European countries active in the IPv6 arena. One major driver is mobile telephony and telco's investments in 3G technology. The EU planned for 25 percent of Internet users to be using IPv6 by 2010.*
- Developing Nations – *Mobile networks chief driver*

Strategies

- Planning for IPv6
- Deploy the technology incrementally
- Backup your design assumptions with practical testing
- Establish sensible, liberal timelines
- Consider the relative lack of extensive experience with the protocol and the resulting dearth of IPv6 deployment best practices.
- Inventory – everything IPv6 with touch (routers, servers and hosts; OS versions, Security Systems, Management systems and back office systems. User applications must also be inventoried.

Methodology

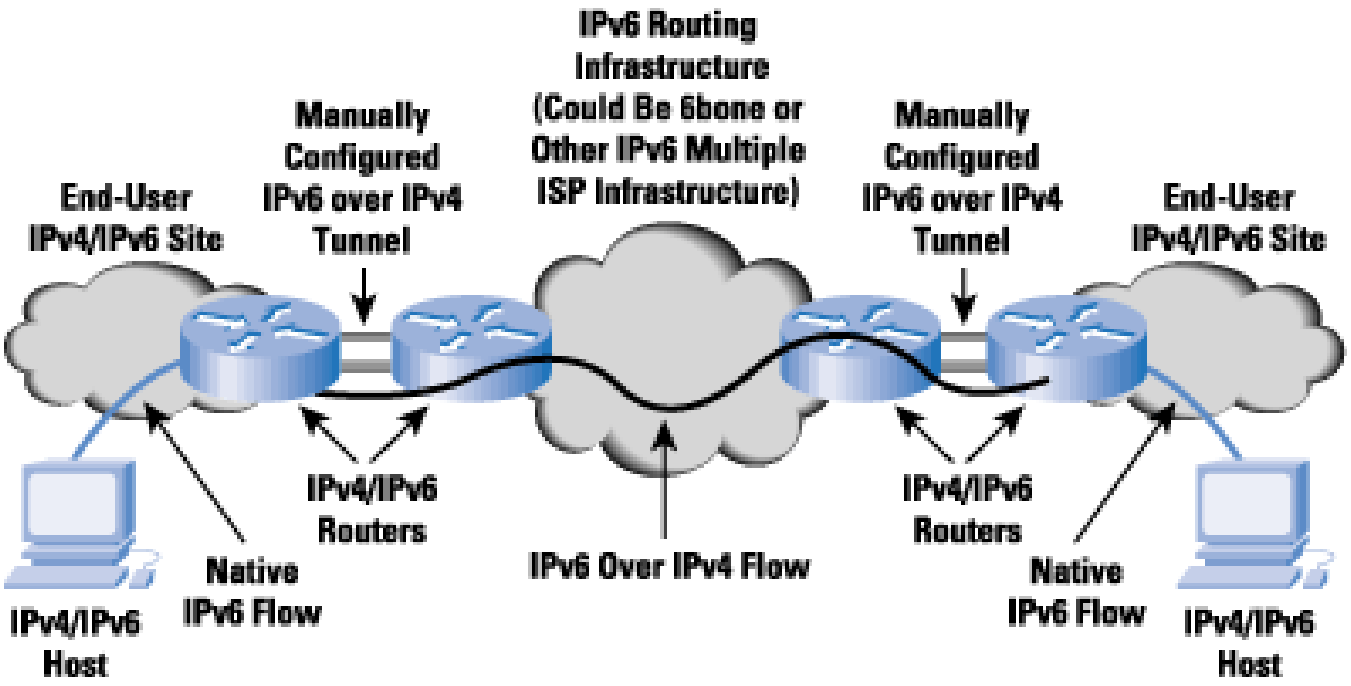
Three approaches for IPv6 Network deployment

- Core to Edge: implement first in the routers forming the core of the network – usually using dual stacked interfaces. *Advantage – easiest place to start as most routers already support IPv6 or can be upgraded easily. Also, generally safest approach as it allows operations and engineering personnel time to become acquainted with the protocol before it reaches users.*
- Edge to Core: Manual tunnels are used to connect edge devices across the core. *Advantageous when IPv6 must be turned up quickly or when network must otherwise demonstrate early IPv6 capability. Also valuable when core consists of legacy routers which cannot support IPv6 but can support a tunneling technology or can only be upgraded with difficulty.*
- IPv6 Islands: *Certain segments throughout network (single devices to complete sites) are converted. Islands can be interconnected with manual or automatic tunnels or a combination of the two.*

Technologies

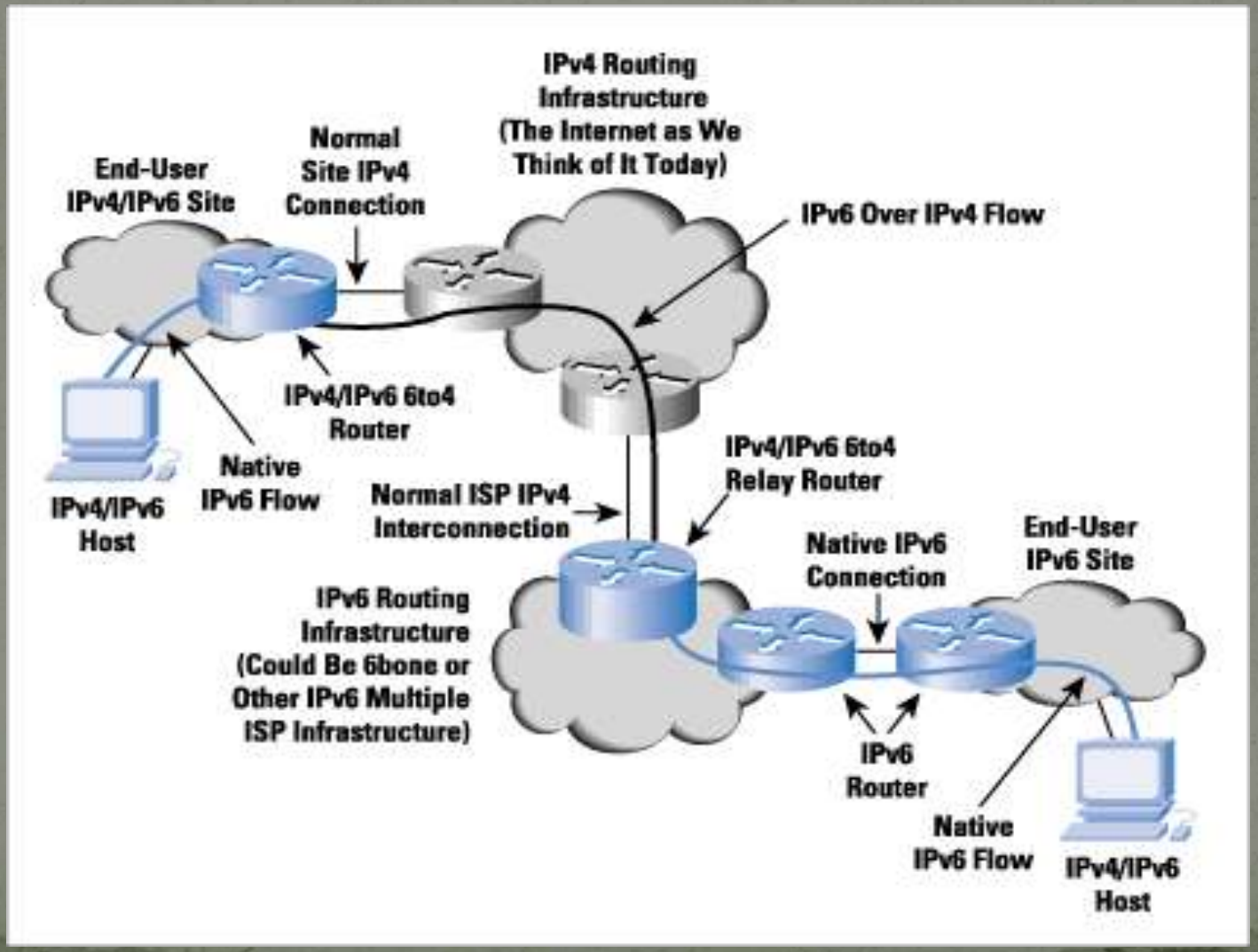
- Dual Stack Devices – Routers and other devices programmed with both IPv4 and IPv6 implementations.
- IPv4/IPv6 Translation- Dual Stack devices may be designed to accept requests from IPv6 hosts, convert them to IPv4 datagrams, send the datagrams to the IPv4 destination and then process the return datagrams similarly.
- IPv4 Tunneling of IPv6
- IPv6 Tunneling of IPv4 (6to4)
- Teredo protocol – IPv4 to IPv6 transition mechanism, entirely automatic and works for hosts that do not have static IPv4 address (most ISP customers). But, Teredo grabs a new IPv6 address on each restart, making persistent connections and running servers impossible.

Tunneling example



Both example End-User site's IPv6 addresses are carried in the global DNS, and are based on routable Aggregatable Global Unicast Address Public Topology prefixes (for instance, from the 6bone Testbed 3FFE::/16 TLA, or the production allocation 2001::/16 TLA).

More complex tunneling example: 6 to 4 Relay (dual stack router)



Security issues

- Security practitioners need education/training on IPv6
- Security tools need to be upgraded
  - IPv6 is NOT backwards compatible. Routers, firewalls and intrusion-detection systems may require software and/or hardware upgrades in order to 'speak' IPv6.
- Existing equipment may require additional configuration
- Tunneling protocols create new risks
  - Protocols allow the encapsulation of IPv6 traffic in an IPv4 data stream for routing through non-compliant devices. Therefore, it's possible that users on your network can begin running IPv6 using these tunneling protocols before you're ready to officially support it in production. Block IPv6 tunneling protocols (including SIT, ISATAP, 6to4 and others) at your perimeter.
- IPv6 auto-configuration creates addressing complexity
  - Two autoconfiguration techniques:
    - **Statefull** auto-configuration uses DHCPv6, a simple upgrade to current DHCP.
    - **Stateless** auto-configuration –allows systems to generate their own IP addresses and checks for address duplication. Easier for a system administrator, but raises challenges when tracking use/abuse of network resources.

Timelines

2012	• **RIR IPv4 free pools predicted to be fully consumed**
2011	• IANA IPv4 free pool predicted to be fully consumed
2009	• APNIC launches: ICONS IPv6 Wiki • APNIC holds Plenary: IPv6 in 3D at its Open Policy Meeting (APNIC27 in Manila) • APNIC highlights the importance of adopting IPv6 at APEC TEL 39 in Singapore • APNIC presents IPv6 Program at CommunicAsia 2009 in Singapore • APNIC coordinates round table discussions with the governments of Indonesian and Hong Kong as part of its outreach activities to multi-stakeholders • APNIC presents Expanding the Internet: IPv4 to IPv6 Transition at various Global IPv6 Summit conferences, NOGs and regional meetings in the AP region • APNIC develops a range of IPv6 publications to disseminate information to the wider AP community

Tutorials & other resources

- http://host.comsoc.org/freetutorial/cisco2/cisco2.html