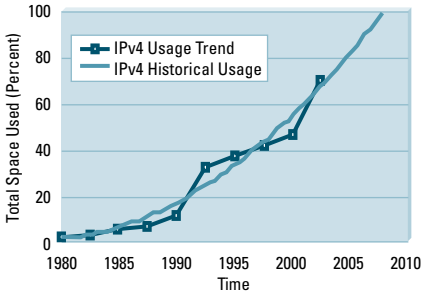
# IPv6 At–A–Glance

**Courtesy of Cisco Enterprise Marketing**

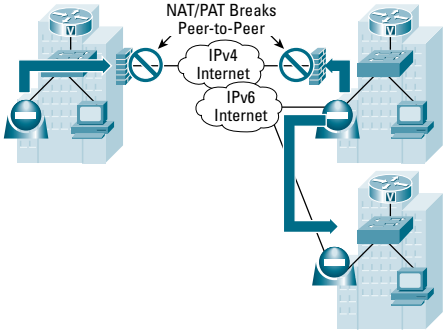
## Should I care about IPv6?

The addressing scheme used for the TCP/IP protocols is IP IPv4. This scheme uses a 32-bit binary number to identify networks and end stations. The 32-bit scheme yields about 4 billion addresses, but because of the dotted decimal system (which breaks the number into 4 sections of 8 bits each) and other considerations, there are really only about 250 million usable addresses. When the scheme was originally developed in the 1980s, no one ever thought there would be a shortage of addresses. However, the advent of the Internet and the trend of making many devices such as cell phones and PDAs Internet compatible (which means they need an address) has made using all the IPv4 addresses a virtual certainty. The chart below shows the trend of address space usage.




## What problems need to be solved?

Network Address Translation (NAT) and Port Address Translation (PAT) were developed as solutions to the diminishing number of available IP addresses. NAT and PAT allow a company or user to share a single or a few assigned IP addresses among several private addresses (which are not bound by an address authority). Although these schemes preserve address space and provide anonymity, these benefits come at the cost of individuality, which conflicts with the reason for networking (and the Internet)—allowing peer to peer collaboration through shared applications.




IPv6 not only provides a solution to the shortage of addresses, it also allows for the restoration of a true end-to-end model where hosts can connect to each other unobstructed and with greater flexibility. Allowing each host to have a unique global IP address, maintain connectivity even when in motion, and to natively secure host communications are the critical elements in IPv6.

## IPv6 Addresses

The 128-bit address used in IPv6 allows for a greater number of addresses and subnets (enough space for 10^15 end points, 340,282,366,920,938,463,463,374,607,431,768,211,456 total). IPv6 was designed to give every user multiple global addresses that can be used for a wide variety of devices including cell phones, PDAs, IP-enabled vehicles, and consumer electronics. In addition to providing more address space, IPv6 has the following advantages over IPv4:

- Easier address management and delegation
- Easy address autoconfiguration
- Embedded IPsec (encrypted security)
- Optimized routing
- Duplicate Address Detection (DAD) feature

## IPv6 Notation

The following diagram demonstrates the notation and shortcuts for IPv6 addresses.

128 bits are expressed as 8 fields of 16-bits in Hex notation

2031:0000:130F:0000:0000:09C0:876A:130B

As a shorthand, leading zeros in each are optional:

2031:0:130F:0:0:9C0:876A:130B

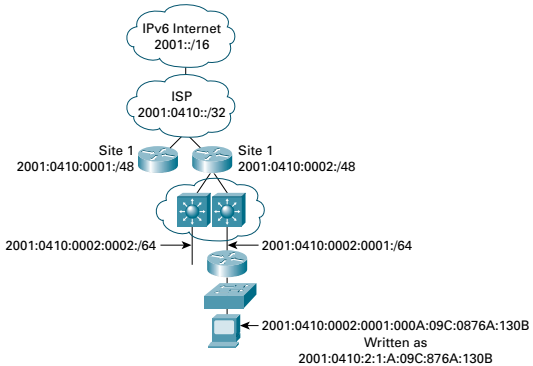
Also, successive fields of 0 can be represented as ::,

2031:0:130F::9C0:876A:130B

The :: shorthand can only be used once per address

2031:0:130F::9C0:876A::130B

An IPv6 address uses the first 64 bits in the address for the network ID and the second 64 bits for the host ID. The network ID is separated into "prefix" chunks. The diagram below shows the address hierarchy.




## IPv6 Autoconfiguration

IPv4 deployments use one of two methods to assign IP addresses to a host: static assignment (which is management intensive) or DHCP/BOOTP (which automatically assigns IP addresses to hosts upon booting onto the network).

IPv6 provides a feature called "stateless autoconfiguration" that is similar to DHCP. Unlike DHCP however, stateless autoconfiguration does not require the use of a special DHCP application or server when providing addresses to simple network devices (such as robotic arms used in manufacturing). Using DCHP, any router interface that has an IPv6 address assigned to it will become "provider" of IP addresses on the network to which it is attached. There are safeguards built into IPv6 that prevent duplicate addresses. This feature is called Duplicate Address Detection.

## IPv6 Security

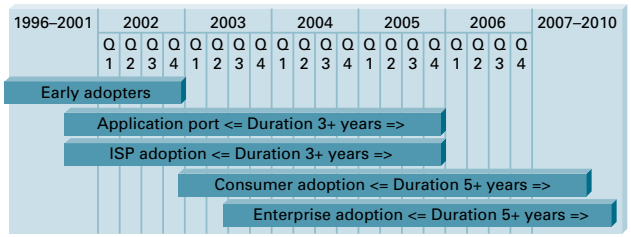
IPv6 has embedded support for IPsec. Currently the host OS can configure an IPsec tunnel between the host and any other host that has IPv6 support. With IPv4 the vast majority of IPsec deployments use a client-server model whereby an IPsec terminating device handles the authentication and encryption and decryption functions. With IPv6 IPsec, the host could create an IPsec tunnel between an IPsec headend device or directly to another host.

## IPv6 Mobility

IPv6 supports a greater array of features for the mobile user, whether the mobile device is a cell phone, PDA, laptop computer, or a moving military vehicle. Mobile IPv6 supports a more streamlined approach to routing packets to and from the mobile device and also supports IPsec between the mobile device and other network devices and hosts.

## IPv6 Transition

Although some early adopters have shifted to IPv6, the majority of users will not start migrating until 2004. The migration will take the better part of 5 years.




E-Europe, E-Japan, North-America IPv6 Task Force, ...



KB/LW4330 05/03