Chapter Four

Internet Protocol (IP) and IP Addressing

4.1 Basics of IPv4

One of TCP/IP's distinguishing features is its universal addressing scheme whereby each computer on a TCP/IP network has an address that uniquely identifies it. This universal addressing scheme extends even to the world-wide Internet, connecting more than two million computers that are connected to thousands of separate networks.

It's IP's responsibility to deliver datagrams among the TCP/IP networked computers. To make such deliveries possible, each computer has a unique IP address. The IP address contains sufficient information to uniquely identify a network and a specific computer on the network.

In short, an IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask. The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 - 11111111 binary.

Network Classes

Because a computer's IP address must uniquely identify not only the computer but also the network the computer is attached to, the IP address is split between a network identifier (net id) part and a host identifier (host id) part. The split between these two identifiers isn't the same for all IP addresses. The class of the address determines how many bits of the IP address are reserved for network identification and how many are reserved for host identification. There are five classes of IP address with only the first three relevant to the majority of users. Classes A, B, and C are for general-purpose use; classes D and E are reserved for special purposes.

CLASSES	Network ranges	No. of possible networks	Hosts per Network	Default subnet mask
A	1 –126	126	16,777,214	255.0.0.0
B	128-191	16,382	65,534	255.255.0.0
C	192-223	2,097,150	254	255.255.255.0
D	224-239			
E	240-255			

SPECIAL IP ADDRESSES

In the Internet addressing architecture, the Internet Engineering Task Force (IETF) and the Internet Assigned Numbers Authority (IANA) have reserved various Internet Protocol (IP) addresses for special purposes. Some of the special IPv4 addresses are:

IP addresses	also called	Description
0.0.0.0 /0	Default route	
0.0.0.0/32	This host	
10.0.0.0-10.255.255.255	Private IP address	Used for local communications within a private network
127.0.0.0-127.255.255.255	Loopback address	Used for loopback addresses to the local host

169.254.0.0-169.254.255.255	APIPA (Automatic Private IP Addressing)	Assigned automatically if the host does not get an IP from a DHCP server provided that the device is set to obtain an IP address automatically
172.16.0.0-172.31.255.255	Private IP Address	Used for local communications within a private network
192.168.0.0-192.168.255.255	Private IP Address	Used for local communications within a private network
224-239	Class D	Reserved for multicast assignments
240-255	Class E	Reserved for future use
Network Addresses and Broadcast Addresses in a subnet		

.1.1 Types of IP address

Public and Private IP Addresses

All hosts that connect directly to the Internet require a unique public IP address. Because of the finite number of 32-bit addresses available, there is a risk of running out of IP addresses. One solution to this problem was to reserve some private addresses for use exclusively inside an organization. This allows hosts within an organization to communicate with one another without the need of a unique public IP address. RFC 1918 is a standard that reserves several ranges of addresses within each of the classes A, B and C. As shown in the table, these private address ranges consist of a single Class A network, 16 Class B networks and 256 Class C networks. This gives a network administrator considerable flexibility in assigning internal addresses.

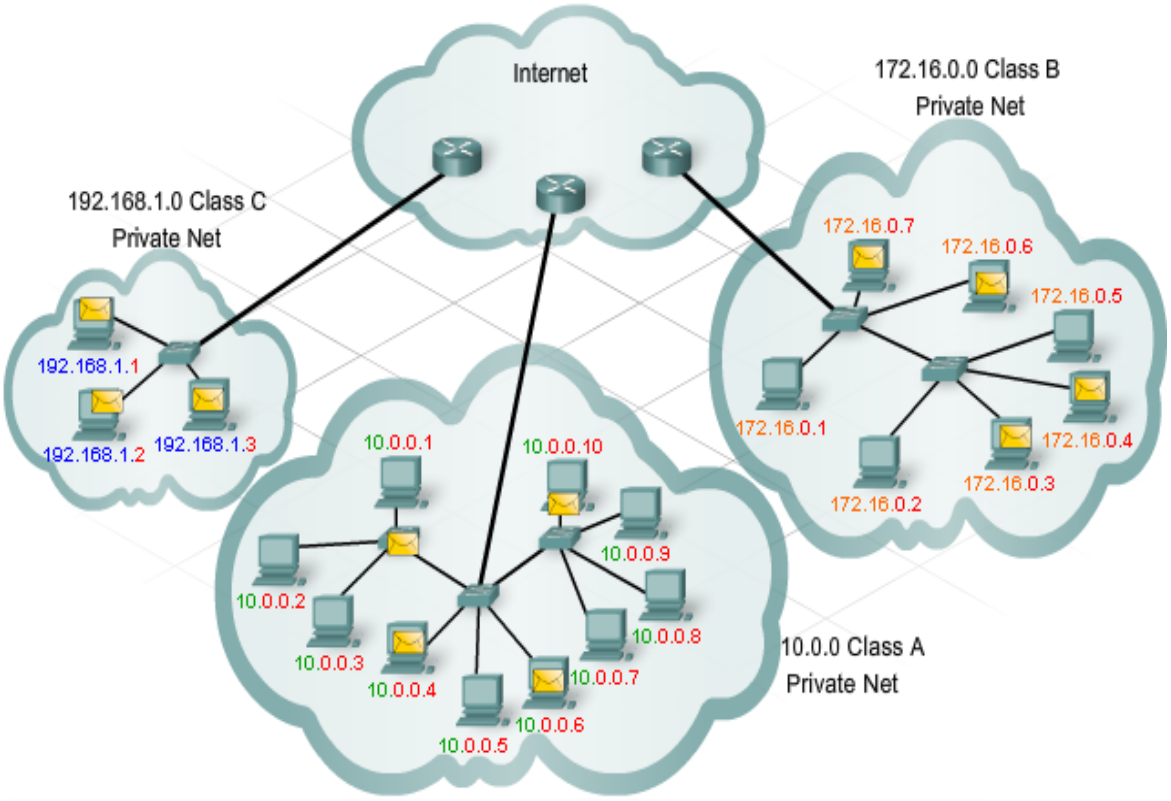
A very large network can use the Class A private network, which allows for over 16 million private addresses. On medium size networks, a Class B private network could be used, which provides over 65,000 addresses per network. Home and small business networks typically use a single class C private address, which allows up to 254 hosts per network.

The Class A network, the 16 Class B networks, or the 256 Class C networks can be used within any size organization. Typically, many organizations use the Class A private network.

Calss	Network Address	Number of Networks	Number of Addresses
A	10.0.0.0-10.255.255.255	1	16,777,216
B	172.16.0.0 – 172.31.255.255	16	1,048,576
C	192.168.0.0 – 192.168.255.255	256	65,536

Private addresses can be used internally by hosts in an organization as long as the hosts do not connect directly to the Internet. Therefore, the same set of private addresses can be used by multiple organizations. Private addresses are not routed on the Internet and will be quickly blocked by an ISP router.

The use of private addresses can provide a measure of security since they are only visible on the local network, and outsiders cannot gain direct access to the private IP addresses.



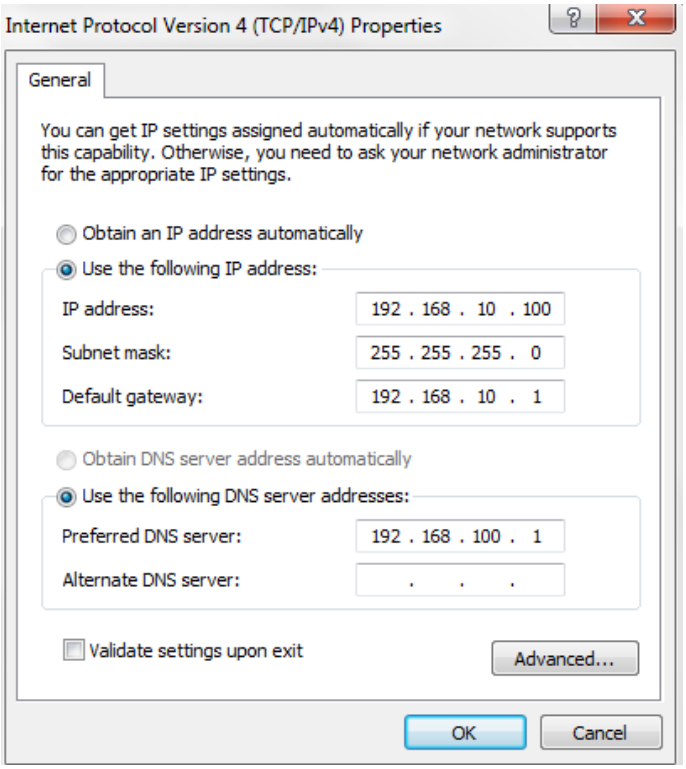
.1.2 IP Address Assignment

IP addresses can be assigned for devices either statically or dynamically.

Static IP Address Assignment

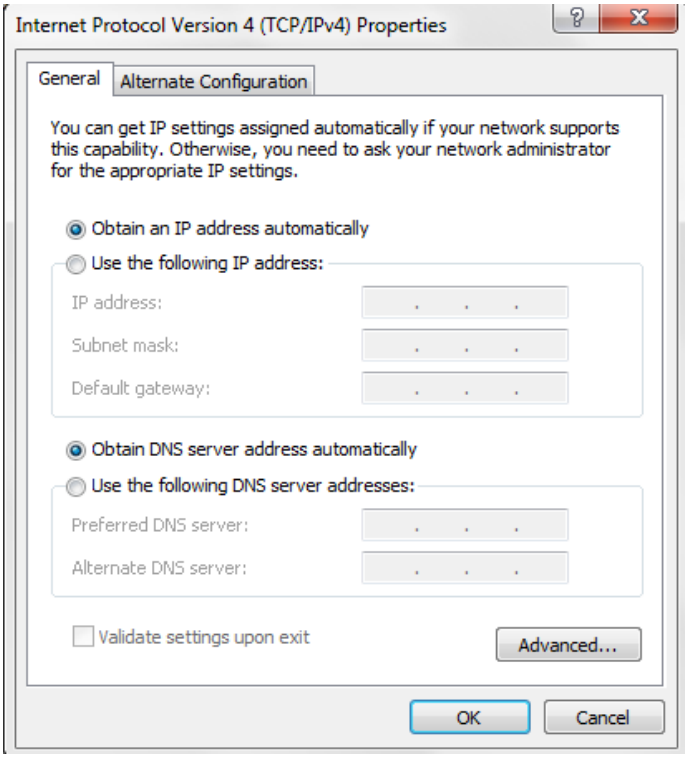
With a static assignment, the network administrator must manually configure the network information for a host. At a minimum, this includes the host IP address, subnet mask and default gateway. Static addresses have some advantages. For instance, they are useful for printers, servers and other networking devices that need to be accessible to clients on the network. If hosts normally access a server at a particular IP address, it would not be good if that address changed. Static assignment of addressing information can provide increased control of network resources, but it can be time consuming to enter the information on each host. When entering IP addresses statically, the host only performs basic error checks on the IP address. Therefore, errors are more likely to occur.

When using static IP addressing, it is important to maintain an accurate list of which IP addresses are assigned to which devices. Additionally, these are permanent addresses and are not normally reused.



Dynamic IP Address Assignment

On local networks it is often the case that the user population changes frequently. New users arrive with laptops and need a connection. Others have new workstations that need to be connected. Rather than have the network administrator assign IP addresses for each workstation, it is easier to have IP addresses assigned automatically. This is done using a protocol known as Dynamic Host Configuration Protocol (DHCP). DHCP provides a mechanism for the automatic assignment of addressing information such as IP address, subnet mask, default gateway, and other configuration information. DHCP is generally the preferred method of assigning IP addresses to hosts on large networks since it reduces the burden on network support staff and virtually eliminates entry errors. Another benefit of DHCP is that an address is not permanently assigned to a host but is only leased for a period of time. If the host is powered down or taken off the network, the address is returned to the pool for reuse. This is especially helpful with mobile users that come and go on a network.



.1.3 Introduction to Subnetting

Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

Class A

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly. For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2^1=2) with (2^{23}-2) 8388606 Hosts per Subnet. A class A address starts from 1 to 127. Network equipment identifies a class A address because the very first bit on the first octet has to have a 0 in the column. It cannot have a 1 in the column. So the first network number is 1. The last possible network number is 127 (check by adding all the values together). Network number 127 cannot actually be used because the value 127.0.0.1 is reserved for troubleshooting. Why can't we have 10.255.255.255 as a host? Because when all the binary values have a 1 on the host part of the address this tells the network that it is a broadcast.

Class B

By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and (2^{16}-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Class B addresses have to have the first two binary columns reserved with a 1 and a 0 next to it. So the first network number is 128. The last available class B network number is 191 (add the values). For Class B addresses we use the first two octets for the network address. So for the address 130.24.5.2. 130.24 is the network number and 5.2 is a host on that network. The rule is still that the first number you see though will always be between 128 and 191. If we use the powers of two rule for the first two octets we will see that we can have a possible 16384 networks. 2^16= 16384 We are not allowed to use the first two bits of the first octet because they are reserved for showing the 10 value remember? So this leaves us with 6+8 digits. 2^14 gives us 16384 networks. We have the full two octets to use for hosts so 8+8 gives us 2^16 = 65534 hosts per class B network.

Class C

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. A class C address has the first three bits reserved so the networking device can recognize it. The first three bits show as 110. So the first network number is 192. And the last is 223. An example of a class C address is 200.2.1.4. 200.2.1 is the network address and .4 is a host on that network. So we can see that there are lots of available network numbers to assign to companies however, we have a limited amount of numbers free to use on our networks. For networks we have to take the 011 from the first octet giving us 5+8+8= 21. 2^21 = 2097152 For the hosts we have 2^8 giving us 255.

Class D and Class E Addresses

Class D addresses are reserved for multicast traffic and cannot be used on your network. Multicast traffic is traffic send to multiple hosts using one IP address. A live webcast of a rock concert would be an example of multicasting. Class E addresses are reserved for experimental use only.

Before subnetting:

- In any network (or subnet) one can use most of the IP addresses for host addresses.
- Two hierarchy (Network and Host)
- One loses two addresses for every network or subnet.

1. Network Address - One address is reserved to that of the network.
2. Broadcast Address – One address is reserved to address all hosts in that network or subnet.

For example, a Class B address of **172.16.0.0/16** is used to assign 2^{16}-2=**65, 534** IP addresses for hosts. Suppose the organization needs 1000 IP addresses and if the technician uses this Network address without subnetting we will lose a number of IP addresses.

During subnetting:

- Applying a mask which is larger than the default subnet mask, will divide your network into subnets. This is possible by borrowing bits from the host portion to network.
- Three hierarchy (Network, Subnet and Host) addresses will be created.

Example: Network address **172.16.0.0 with /16 network mask** can be subnetted as follow.

- Default network mask: 255.255.0.0 or /16

Network	Network	Host	Host
11111111	**11111111**	**00000000**	**00000000**

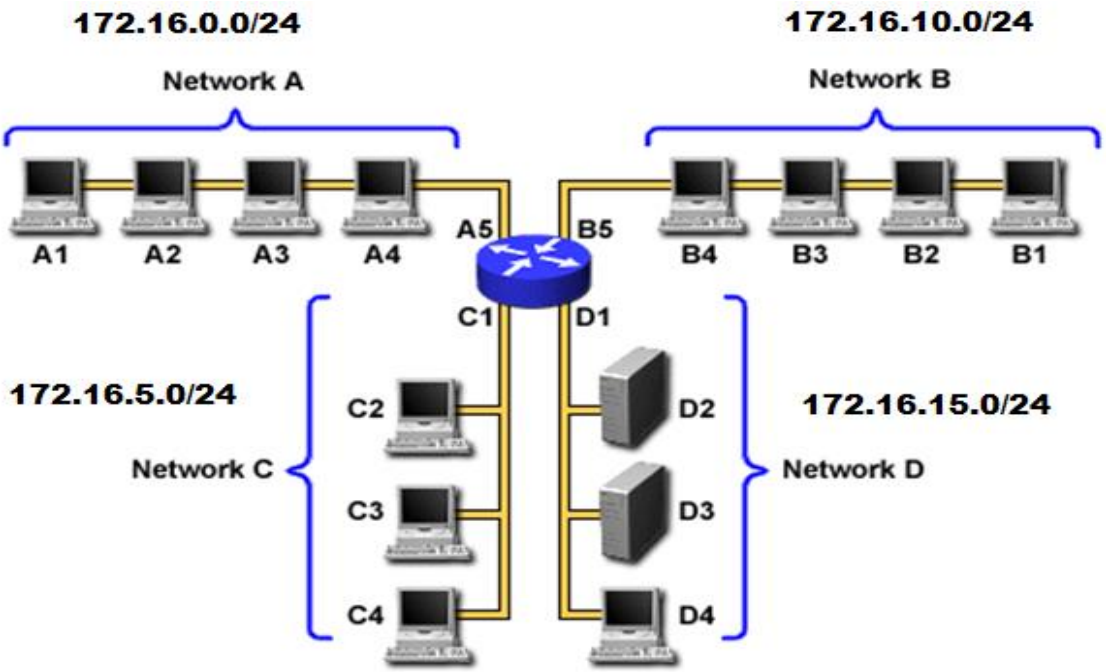
- The above /16 network mask is subnetted using a new subnet mask 255.255.255.0 or /24 as follow:

Network	Network	Subnet	Host
11111111	**11111111**	**11111111**	**00000000**

Important formulas:

- Nº of possible Networks: $\mathbf{2^N}$ (N is the number of bits for the network/subnet portion)
- Nº of hosts per networks: $\mathbf{2^H - 2}$ (H is the number of bits for the host portion)

With the new subnet mask you will have 256 networks/ subnets addresses and each subnet will support 254 hosts which is manageable for the network administrator. Out of the total subnets, for instance, four of them are used for the following network topology: Netwok A: 172.16.0.0/24, Netwok B: 172.16.10.0/24, Netwok C: 172.16.5.0/24 and Netwok D: 172.16.15.0/24.



In the following sections you will learn how to create subnetting.

i. **Creating subnets based on the network requirement**

Steps:

1. Determine the number of networks required and convert it into binary.
2. Reserve bits in the mask and find the increment
3. Find the network ranges based on the increment

Example:

Assume that the organization has a network address of 192.168.100.0/24 and if this organization asks you to make this a Class C address in to nine valid networks, show that how you do the subnetting.

Solution

1. Determine the number of networks required and convert it into binary
   9 networks= 0000**1001**
   We need only **4 bits** to denote 9 in binary.
2. Reserve bits in the mask and find the increment
   Default mask: /24=255.255.255.0=11111111.11111111.11111111.00000000
   Reserve bits in the mask: 11111111.11111111.11111111.**1111**0000
   New subnet mask: 255.255.255.240 or /28
   Increment=lowest bit in the network portion (Italic one) i.e. **16.**
3. Find the network ranges based on the increment

Subnet	Network Address (0000)	Range of Valid Hosts (0001–1110)	Broadcast Address (1111)
0 (0000)	192.168.100.**0**	192.168.100.**1**–192.168.100.**14**	192.168.100.**15**
1 (0001)	192.168.100.**16**	192.168.100.**17**–192.168.100.**30**	192.168.100.**31**
2 (0010)	192.168.100.**32**	192.168.100.**33**–192.168.100.**46**	192.168.100.**47**
3 (0011)	192.168.100.**48**	192.168.100.**49**–192.168.100.**62**	192.168.100.**63**
4 (0100)	192.168.100.**64**	192.168.100.**65**–192.168.100.**78**	192.168.100.**79**
5 (0101)	192.168.100.**80**	192.168.100.**81**–192.168.100.**94**	192.168.100.**95**
6 (0110)	192.168.100.**96**	192.168.100.**97**–192.168.100.**110**	192.168.100.**111**
7 (0111)	192.168.100.**112**	192.168.100.**113**–192.168.100.**126**	192.168.100.**127**
8 (1000)	192.168.100.**128**	192.168.100.**129**–192.168.100.**142**	192.168.100.**143**
9 (1001)	192.168.100.**144**	192.168.100.**145**–192.168.100.**158**	192.168.100.**159**
10 (1010)	192.168.100.**160**	192.168.100.**161**–192.168.100.**174**	192.168.100.**175**
11 (1011)	192.168.100.**176**	192.168.100.**177**–192.168.100.**190**	192.168.100.**191**
12 (1100)	192.168.100.**192**	192.168.100.**193**–192.168.100.**206**	192.168.100.**207**
13 (1101)	192.168.100.**208**	192.168.100.**209**–192.168.100.**222**	192.168.100.**223**
14 (1110)	192.168.100.**224**	192.168.100.**225**–192.168.100.**238**	192.168.100.**239**
15 (1111)	192.168.100.**240**	192.168.100.**241**–192.168.100.**254**	192.168.100.**255**

For the organization you can take the first 9 sub networks i.e. (From subnet 0-8 both inclusive)

192.168.100.**0/28**
192.168.100.**16/28**
192.168.100.**32/28**
192.168.100.**48/28**
192.168.100.**64/28**
192.168.100.**80/28**
192.168.100.**96/28**
192.168.100.**112/28**
192.168.100.**128/28**

ii. Creating subnets based on the host requirement

Steps:

1. Determine the number of host required per networks and convert it into binary.
2. Reserve bits in the mask and find the increment
3. Find the network ranges based on the increment

Example:

Assume that the organization has a network address of 172.16.0.0/16 and this organization asks you to divide this Class B address in to subnets. The organization needs each sub network to support 400 hosts. Show that how you do the subnetting.

Solution

1. Determine the number of hosts required per network and convert it into binary
   400 hosts per networks= 110010000
   We need only **9 bits** to denote 400 in binary.
2. Reserve bits in the mask and find the increment
   Default mask: /16=255.255.0.0=11111111.11111111.00000000.00000000
   Reserve bits in the mask: 11111111.11111111.1111111***0*.00000000**
   New subnet mask: 255.255.254.0 or /23
   Increment=lowest bit in the network portion (Italic one) i.e. **2.**
3. Find the network ranges based on the increment

Subnet	Network Address	Range of Valid Hosts	Broadcast Address
0	172.16.**0.0**	172.16.0.1-172.16.1.254	172.16.**1.255**
1	172.16.**2.0**	172.16.2.1-172.16.3.254	172.16.**3.255**
2	172.16.**4.0**	172.16.4.1-172.16.5.254	172.16.**5.255**
3	172.16.**6.0**	172.16.6.1-172.16.7.254	172.16.**7.255**
.	.	.	.
.	.	.	.
.	.	.	.
127	172.16.**254.0**	172.16.254.1-172.16.255.254	172.16.**255.255**

.1.4 VLSM (Variable Length Subnet Masks)

VLSMs allow you to use different masks for each subnet, and thereby use address space efficiently. With private address space, it is rarely necessary to shrink below a /24 subnet mask as space is plentiful. Use VLSM to:

- Create a larger subnet of more than 255 host addresses
- Create very small subnets for WAN links

Example: Given the 172.16.0.0/16 network and requirements below, develop a subnetting scheme with the use of VLSM:

- LAN1 must support 330 hosts
- WAN must support 2 hosts for a T1 circuit to a remote site
- LAN3 must support 6 hosts

The first step is to determine what mask allows the required number of hosts.

- LAN1 requires a /23 (255.255.254.0) mask to support 510 hosts
- WAN requires a /30 (255.255.255.252) mask to support 2 hosts
- LAN3 requires a /29 (255.255.255.248) mask to support 6 hosts

The easiest way to assign the subnets is to assign the largest first.

For example: You can assign the subnets in this manner:

- LAN1 —172.16.0.0/23 address range 0.0 to 1.255
- LAN3 —172.16.2.0/29 address range 0 to 7
- WAN —172.16.2.8/30 address range 8 to 11

.2 Overview of IPv6 address

So far, IPv4 has proven itself as a robust routable addressing protocol and has served us for decades on its best-effort-delivery mechanism. It was designed in the early 80s and did not get any major change afterward. At the time of its birth, Internet was limited only to a few universities for their research and to the Department of Defence. IPv4 offers around 4,294,967,296 (2^{32}) addresses. This address space was considered more than enough that time.

Given below are the major points that played a key role in the birth of IPv6:

- Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement to have a protocol that can satisfy the needs of future Internet addresses that is expected to grow in an unexpected manner.
- IPv4 on its own does not provide any security features. Data has to be encrypted with some other security application before being sent on the Internet.
- Data prioritization in IPv4 is not up-to-date. Though IPv4 has a few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism.
- It does not have a mechanism to configure a device to have globally unique IP address.

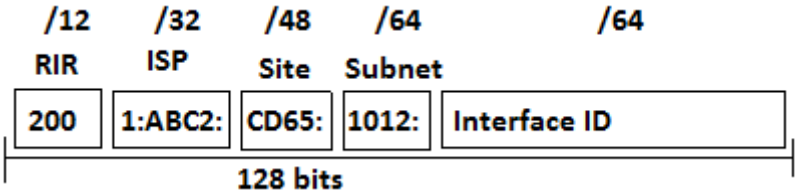
The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the assignment of IPv6 addresses. ICANN assigns a range of IP addresses to Regional Internet Registry (RIR) organizations. The size of address range assigned to the RIR may vary but with a minimum prefix of /12 and belong to the following range: 2000::/12 to 200F:FFFF:FFFF:FFFF::/64.

Each ISP receives a /32 address from a given RIR and provid/es a /48 address for each site. Every ISP can provide $2^{(48-32)}$ = 65,536 site addresses (note: each network organized by a single entity is often called a site).

Each site provides /64 address for each LAN and each site can provide $2^{(64-48)}$ = 65,536 LAN addresses for use in their private networks.

So each LAN can provide 2^{64} interface addresses for hosts.

Example:



.2.1 IPv6 Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols. For example, given below is a 128-bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ':' symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:

Rule 1: Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule 2: If two or more blocks contain consecutive zeroes, omit all of them and replace with double colon sign **::**, such as (6th and 7th block):

2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

2001:0:3238:DFE1:63::FEFB

.2.2 IPv6 features

IPv6 is not designed to be backward compatible with IPv4. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers some of the following features:

IPv6 features	**Description**
Larger Address Space	IPv6 uses 128 bits to address a device i.e. it can provide approximately 3.4×10^{38} different combinations of addresses.
Simplified Header	IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4.
End-to-end Connectivity	Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components.
Auto-configuration	IPv6 supports both stateful and stateless auto-configuration mode of its host devices.
Faster Forwarding/ Routing	The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.
IPSec	Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.
No Broadcast	IPv6 does not have any broadcast support. It uses multicast to communicate with multiple hosts.
Anycast Support	Multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.
Mobility	This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.
Enhanced Priority Support	In IPv6, Traffic class and Flow label are used to tell the underlying routers how to efficiently process the packet and route it.
Extensibility	IPv6 header is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

.2.3 IPv6 Address types

In IPv6, a destination address can belong to one of three categories: unicast, anycast, and multicast.

i. Unicast Address

A unicast address defines a single interface (computer or router). The packet sent to a unicast address will be routed to the intended recipient.

ii. Anycast Address

An anycast address defines a group of computers that all share a single address. A packet with an anycast address is delivered to only one member of the group, the most reachable one. An anycast communication is used, for example, when there are several servers that can respond to an inquiry. The request is sent to

the one that is most reachable. The hardware and software generate only one copy of the request; the copy reaches only one of the servers. IPv6 does not designate a block for anycasting; the addresses are assigned from the unicast block.

iii. ***Multicast Address***

A multicast address also defines a group of computers. However, there is a difference between anycasting and multicasting. In anycasting, only one copy of the packet is sent to one of the members of the group; in multicasting each member of the group receives a copy. As we will see shortly, IPv6 has designated a block for multicasting from which the same address is assigned to the members of the group. It is interesting that IPv6 does not define broadcasting, even in a limited version. IPv6 considers broadcasting as a special case of multicasting.

.2.4 Special IPv6 Addresses

The followings are some of the reserved IPv6 address for special purpose.

Reserved Address	**Description**
FF02::1	A multicast address to all nodes on a link (link-local scope)
FF02::2	A multicast address to all routers on a link
FF02::5	OSPFv3 All SPF routers
FF02::6	OSPFv3 All DR routers
FF02::9	A multicast address to all routing information protocol (RIP) routers on a link
FF02::A	EIGRP routers
FF02::1:FFxx:xxxx	All solicited-node multicast addresses used for host auto-configuration and neighbor discovery (similar to ARP in IPv4)
FF05::101	A multicast address to all Network Time Protocol (NTP) servers

.2.5 IPv6 Address Scopes

Address types have well-defined destination scopes:

IPv6 Address scopes	**Description**
Link-local address	- Only used for communications within the local subnetwork (automatic address configuration, neighbor discovery, router discovery, and by many routing protocols). It is only valid on the current subnet. - Routers do not forward packets with link-local addresses. - Are allocated with the FE80::/64 prefix -> can be easily recognized by the prefix FE80. Some books indicate the range of link-local address is FE80::/10, meaning the first 10 bits are fixed and link-local address can begin with FE80, FE90,FEA0 and FEB0 but in fact the next 54 bits are all 0s so you will only see the prefix FE80 for link-local address. - Same as 169.254.x.x in IPv4, it is assigned when a DHCP server is unavailable and no static addresses have been assigned - Is usually created dynamically using a link-local prefix of FE80::/10 and a 64-bit interface identifier (based on 48-bit MAC address).
Global unicast address	- Unicast packets sent through the public Internet - Globally unique throughout the Internet - Starts with a 2000::/3 prefix (this means any address beginning with 2 or 3). But in the future global unicast address might not have this limitation.
Site-local address	- Allows devices in the same organization, or site, to exchange data. - Starts with FC00::/7 (for used in private networks). They are analogous to IPv4's

	private address classes. Note: Site-local address used to start with FEC0::/10 (but it is deprecated now)

.2.6 TRANSITION FROM IPv4 TO IPv6

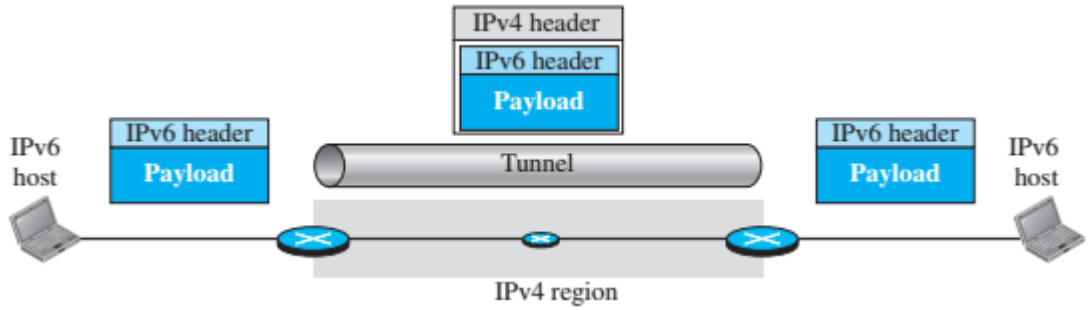
Three strategies have been devised for transition: dual stack, tunneling, and header translation.

i. *Dual Stack*

It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols during the transition. In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6. To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

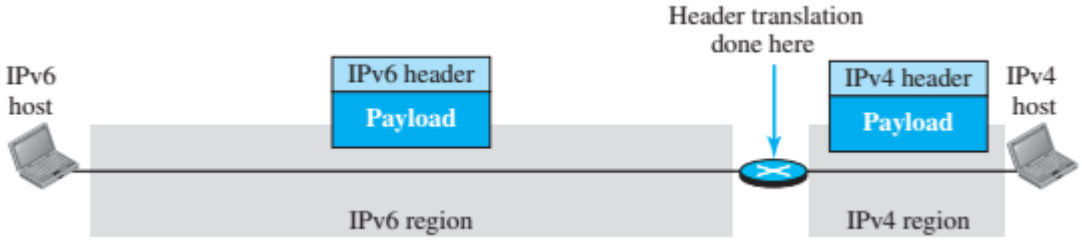
ii. *Tunneling*

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region. It seems as if the IPv6 packet enters a tunnel at one end and emerges at the other end. To make it clear consider the following figure.



iii. *Header Translation*

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6. Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver. In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header.



.3 Address mapping

Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP)

Anytime a node has an IP datagram to send to another node in a link, it has the IP address of the receiving node. The source host knows the IP address of the default router. Each router except the last one in the path gets the IP address of the next router by using its forwarding table. The last router knows the IP address of the destination host. However, the IP address of the next node is not helpful in moving a frame through a link; we need the link-layer address of the next node. This is the time when the ARP becomes helpful. The ARP protocol is one of the auxiliary protocols defined in the network layer. ARP accepts

an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.

Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address (FF:FF:FF:FF:FF:FF).

Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. The response packet contains the recipient's IP and link-layer addresses. The packet is unicast directly to the node that sent the request packet.

Reverse Address Resolution Protocol (RARP) is another network layer protocol that allows a host to find its Internet address given its physical address.

.4 Message types

.4.1 Internet Control Message Protocol (ICMP)

ICMPv4 is a network layer protocol. ICMP messages are divided into two broad categories: error-reporting messages and query messages. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbours. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.

The new ICMP, ICMPv6, follows the same strategy and purposes of version 4. ICMPv6, however, is more complicated than ICMPv4: some protocols that were independent in version 4 are now part of ICMPv6 and some new messages have been added to make it more useful. The ICMP, ARP, and IGMPv4 are combined into one single protocol, ICMPv6. We can divide the messages in ICMPv6 into four groups: error-reporting messages, informational messages, neighbour-discovery messages, and group-membership messages.

.4.2 Internet Group Message Protocol (IGMP)

The protocol that is used today for collecting information about group membership is the Internet Group Management Protocol (IGMP). IGMP is a protocol defined at the network layer; it is one of the auxiliary protocols, like ICMP, which is considered part of the IP. IGMP messages, like ICMP messages, are encapsulated in an IP datagram. There are only two types of messages in IGMP version 3, query and report messages. A query message is periodically sent by a router to all hosts attached to it to ask them to report their interests about membership in groups. A report message is sent by a host as a response to a query message.

In IPv6, this responsibility is given to the Multicast Listener Delivery protocol. MLDv1 is the counterpart to IGMPv2; MLDv2 is the counterpart to IGMPv3.

Further reading Assignment

1. IPv4 and IPv6 header formats
2. Types of ICMP error-reporting and query messages
3. ARP Caching and Proxy ARP
4. How DHCP works? What are DHCP message types?
5. NAT (Network Address Translation)
6. IPv6 autoconfiguration