Introduction to Computer Networking

Dale Callahan, Ph.D., P.E.

MODULE 6: IP Addressing Scheme

6.1 Review

As explained in module 4, an IP address is a 32-bit number (4 bytes) that is used to identify a host within a network. A packet that is transmitted over the network holds the source and destination address that allows the intermediate routers to forward the packet to the proper destination. The most common example is a web page request that is sent to the server when a user types in the URL for a website. The Domain Name Server (DNS) resolves the destination IP address from the URL typed in the browser and sends the IP address of the source computer to the server.

An IP address consists of two parts: the network part of the address and the host part of the address. The network part of the address allows a packet to be guided across several networks and the host part of the addresses helps in determining the exact host within the network. Every packet that traverses the Internet contains the network address within its header. Apart from the network address, there is a need to identify every machine uniquely over the network in order to deliver the packet to the right destination. This address is termed as the host address

6.2 IP Address Classes and Formats

The IP addresses are divided into four classes based on their size. The classes are Class A, Class B, Class C, and Class D [18].

Class A addresses are used for large networks and the first bit in the IP address is zero. The remaining 7 bits of the first byte are the network bits while the remaining 24 bits are for the host. Thus, a class A network can support up to 16,777,214 hosts.

0	7 bits for Network Address	24 bits for Hosts Address

Figure 32. Class A Address Format

Class B addresses are used for medium sized networks and the first two bits of the IP address are 10. The remaining 14 bits of the first two bytes are reserved for the network address. The last 16 bits are reserved for the host address. Class B address can support up to 65,534 hosts.

10	14 bits for Network Address	16 bits for Hosts Address

Figure 33. Class B Address Format

Class C addresses are suited to a small network of less than 256 hosts. The first 3 bits in the IP address contains 110. The remaining 21 bits are assigned to the network portion of the address. Thus, a Class C address can typically support up to 254 hosts.

110	21 bits for Network Address	8 bits for Hosts Address

Figure 34. Class C Address Format

Class D addresses are called as Multicast addresses and contains 1110 as the first 4 bits in the IP addresses. The remaining 28 bits are used to define multicast addresses.

1110	28 bits for Multicast Address

Figure 35. Class D Address Format

IP address is represented in a dot quad notation. The format is **xxx.xxx.xxx.xxx** where xxx represents a decimal number that defines the IP address. This IP address is also represented as a name called as Domain Name.

The size of the Internet is growing significantly and there is a need for a new IP scheme. Hence, a newer version of IP, called as IPv6, will be used to accommodate huge networks. IPv6 allows addresses of 128 bits instead of 32 bits. IPv6 has still not been completely implemented over the Internet. IPv4 is dominant in most networks.

6.3 IP Address Scheme

The IP addressing scheme plays a large role in making network decisions. The size of the network impacts the IP address space that needs to be allocated to the organization. There may be a need for subnetting the IP space in smaller subnets if a large number of computers need to be supported in a network. Subnetting assists in better management of a large network and provides more control for a network administrator.

6.3.1 Subnets

Consider an IP address of 132.100.0.0 that is assigned to a medium sized company. The IP scheme chosen by the company requires that the IP address be divided in to 4 separate networks with maximum number of hosts that can be supported by the subnets.

The IP address provided is a class B address and hence the first 2 bytes remain fixed. We need to use the last two bytes in the IP address to create 4 subnets as per the demand. These last two bytes can be divided in a way that some bits can be assigned to the network and rest to the hosts within that network.

The IP 132.100.0.0 address when expressed in binary is represented as follows:

Octet 1	Octet 2	Octet 3	Octet 4
10000100	01100100	00000000	00000000

In order to have 4 subnets we require at least 2 bits as $2^2 = 4$. Thus if we use 2 bits of the third octet, we will have out IP address in the following format:

132.100.00 | 000000.00000000
Network | Host

The four combinations out of the two bits in the third octet would create 4 following subnets:

1. 132.100.11 | 000000.00000000 → 132.100.192.0
2. 132.100.10 | 000000.00000000 → 132.100.128.0
3. 132.100.01 | 000000.00000000 → 132.100.64.0
4. 132.100.00 | 000000.00000000 → 132.100.0.0

But all '1' subnets and all '0' subnets are known as illegal subnets. As a result we need to discard the two networks out of the 4 obtained above. Thus we have only two networks available for subnetting if we use two bits out of the third octet.

Hence, we add another bit and use three bits in the network portion of the address. So we have $2^3 = 8$ combinations available with three bits. But two of the networks will be an all ones and zeros network and will be discarded. Thus, the total number of networks possible can be calculated by using the following formula:

$$2^{\text{number of bits}} - 2 = \text{number of available networks}$$

Hence, with three bits we have; $2^3 - 2= 8 - 2 = 6$ networks available for subnetting. The six networks are:

1. 132.100.110 | 00000.00000000 → 132.100.192.0
2. 132.100.101 | 00000.00000000 → 132.100.160.0
3. 132.100.100 | 00000.00000000 → 132.100.128.0
4. 132.100.011 | 00000.00000000 → 132.100.96.0
5. 132.100.010 | 00000.00000000 → 132.100.64.0
6. 132.100.001 | 00000.00000000 → 132.100.32.0

Now, we have 5 bits in the third octet and 8 bits in the fourth octet for the hosts. Thus we have 13 bits, which gives us $2^{13} = 8192$. This leaves us with 8192 - 2 = 8190 hosts - two of them are all zero and all ones combination that is considered illegal. We can use any four out of the six networks as per the requirements.

6.3.2 Subnet Masks

Subnet masks specify the part of the IP address that is used to distinguish sub networks. In subnet masks, every bit in the IP address that is used for the network is assigned a '1' while the rest of the host portion is assigned a '0'. A router uses the subnet mask to filter out the network address from the IP address. A Boolean 'AND' operation is performed with the incoming IP address and the subnet mask and the network address is used to forward the packet to the right interface card [18].

Consider an IP address 132.100.192.12 that belongs to the first network address 132.100.192.0 obtained above. The subnet mask for this IP is:

IP Address	10001000.01100100.11000000.00001100	132.100.192.12
Subnet Mask	11111111.11111111.11100000.00000000	255.255.224.0
Router's extraction of Network ID	10001000.01100100.11000000.00000000	132.100.192.0

6.3.3 Broadcast Address

A broadcast address is created for a subnet when all the bits in the host portion of the subnet are set to '1'. Consider the subnet address 132.100.192.0; the broadcast address for this subnet will be 132.100.255.255 with a subnet mask of 255.255.224.0. The

$$\underbrace{10001000.01100100.11}_{\text{Network ID}} \mid \underbrace{111111.11111111}_{\text{Host ID}} = 132.100.255.255$$

The broadcast address is used to send a message to all the computers within that subnet [24].

6.3.4 Wildcard Mask

Wildcard masks are opposite of subnet masks such that all the network bits are represented as '0' while host bits are represented by '1' [18].

The network 132.100.192.0 will have a wildcard mask as follows:

IP Address	10001000.01100100.11000000.00000000	132.100.192.12

Subnet Mask	11111111.11111111.11100000.00000000	255.255.224.0
Wildcard Mask	$\underbrace{\text{00000000.00000000.000}}_{\text{Network ID}}\underbrace{\text{11111.11111111}}_{\text{Host ID}}$	0.0.31.255

The wildcard mask for 132.100.192.0 is 0.0.31.255.

6.3.5 Start address of a subnet

The start address for a host in a subnet can be obtained by placing a ‘1’ at the end of the last octet [18]. Thus for the address 132.100.192.0, the first address is obtained as follows:

$$\underbrace{\text{132.100.192.}}_{\text{Network ID}}\underbrace{\text{00000001}}_{\text{Host ID}} \qquad \text{255.255.224.0}$$

Hence, the first address for a host is 132.100.192.1 with subnet mask of 255.255.224.0.

6.3.6 End address of a subnet

The end address for a host in a subnet can be obtained by placing a ‘0’ at the end of the last octet and replacing the other host bits by ‘1’ [18]. Thus for the address 132.100.192.0, the first address is obtained as follows:

$$\underbrace{\text{132.100.110}}_{\text{Network ID}}|\underbrace{\text{11111.11111110}}_{\text{Host ID}} \qquad \text{255.255.224.0}$$

Hence, the end address for a host is 132.100.223.254 with subnet mask of 255.255.224.0.

6.3.7 Internal addresses

Some IP addresses are used only for private purposes and cannot be reached from outside the Internet. The class A address 10.0.0.0 to 10.255.255.255 can only be used for private purposes. Similarly, 172.168.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255 are private addresses that may be used inside a network and may not be visible to users outside the network [18].