TCP/IP Reference Model

(Transmission Control Protocol / Internet Protocol)

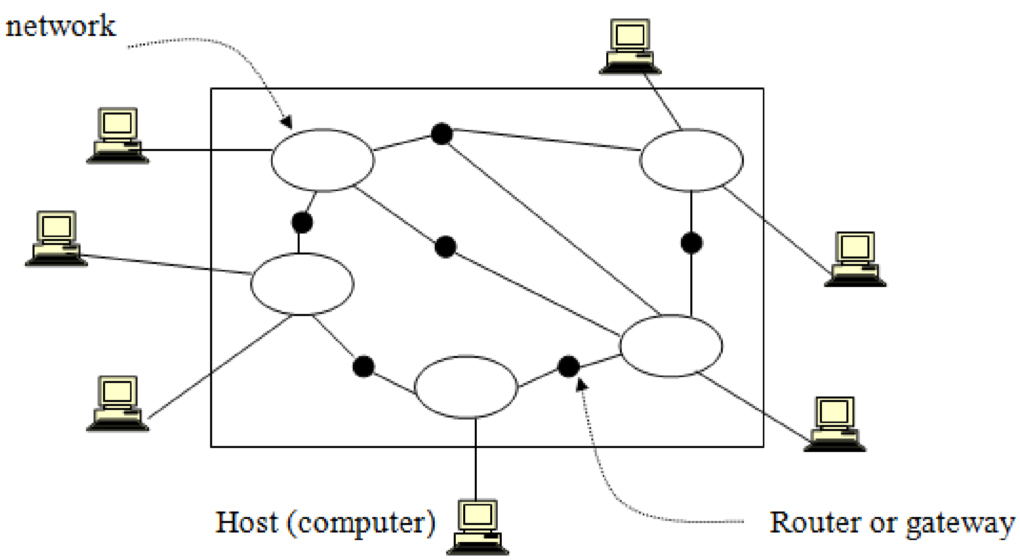
The TCP/IP is a set of protocols, or a protocol suite, that defines how all transmission are exchanged across the Internet. Named after its two most popular protocols, TCP/IP has been in active use for many years and has demonstrated its effectiveness on a worldwide scale.

The reasons for TCP/IP reference model are:

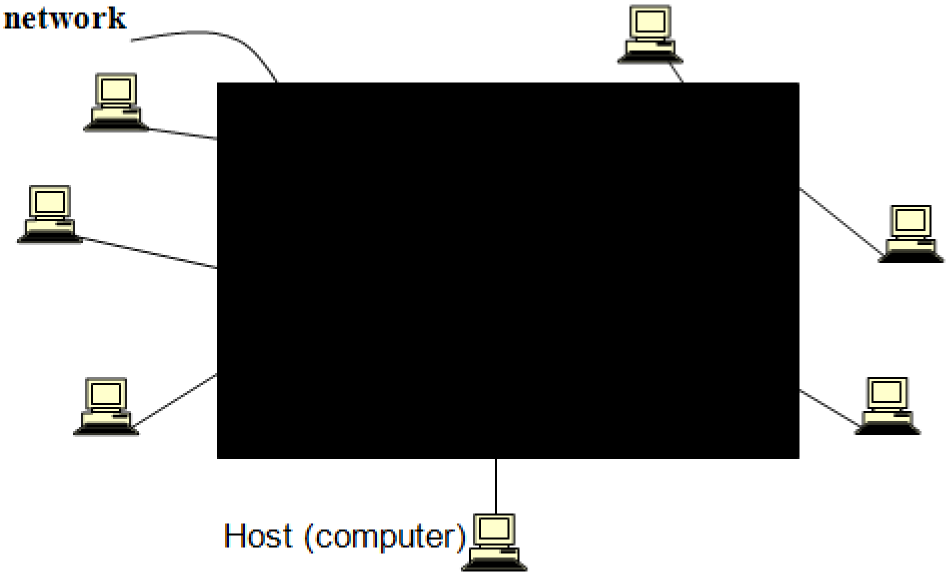
1- Connect multiple networks with modern technologies.
2- The connection must remain as long as the source and destination were functioning even if some machines or transmission lines suddenly put out of operation.
3- Flexible architecture.

TCP/IP and the Internet:

An internet under TCP/IP operates like a single network connecting many computers of any size and type. The Internet is an interconnection of independent physical networks (such as LANs) linked together by internetworking devices, as shown in figure below:



An actual internet

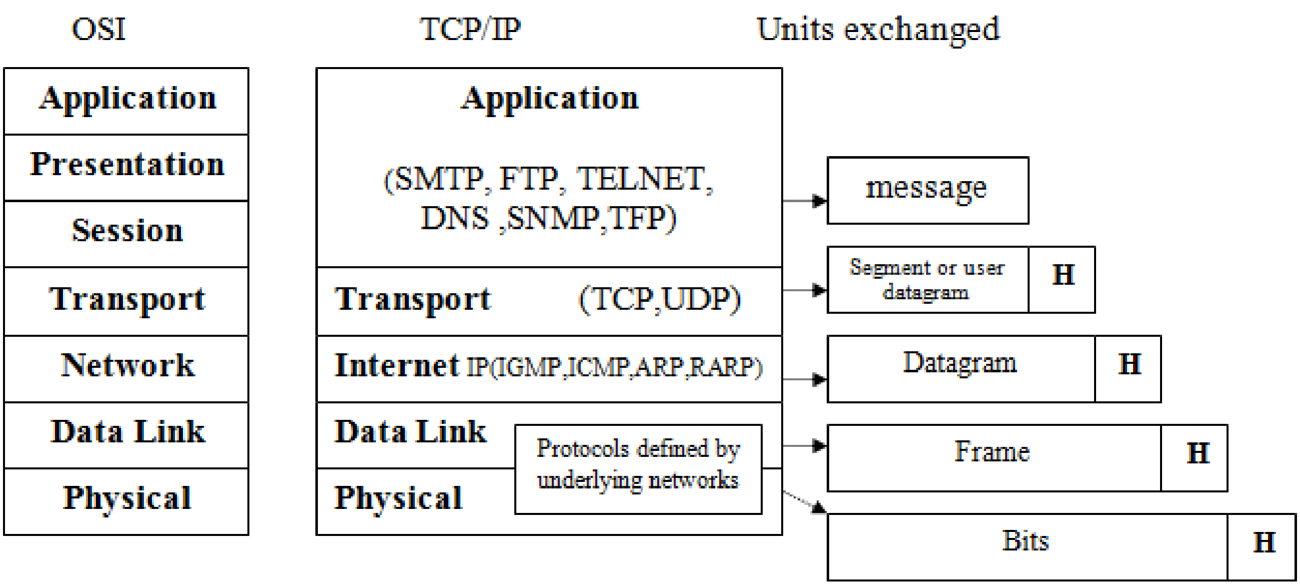


An internet seen by TCP/IP

To TCP/IP, the same internet appears quite differently, TCP/IP considers all interconnected physical networks to be one huge network.

TCP/IP and OSI:

TCP was developed before the OSI model. Therefore, the layers in TCP/IP suite do not match exactly with those in OSI model. The TCP/IP suite is made of five layers: (physical, data link, network, transport, and application) as shown below.



Layer 1 and Layer 2: Physical Layer and Data Link Layer (Host to network layer)

The TCP/IP suite does not really say much about what happens here. However, to be able to move physically from one network to another, the datagram must encapsulated in a frame in the data link layer of the underlying network and finally transmitted as signals along the transmission media.

Layer 3: Internetwork (Internet) (network) layer

This layer is the central element that holds the whole architecture. The glue that holds the Internet is the internet protocol (IP). At the internetwork layer, TCP/IP supports the IP. IP, in turn, contains four supporting protocols: ARP, RARP, ICMP, and IGMP.

Internetwork Protocol:

IP is the transmission mechanism used by the TCP/IP. It is an unreliable and connectionless datagram protocol. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. Transmission along physical networks can be destroyed for a number of reasons. Noise can cause bit errors; congested router may discard a datagram; and disabled links may leave no usable path to destination.

If reliability is important, IP must be paired with a reliable protocol such as TCP. IP transports data in packets called datagrams (datagrams are variable length packets can be up to 64k bytes but in practice they are usually around 1500 bytes), each of which is transported separately. Datagrams may travel along different routes and may arrive out of sequence or duplicated. IP does not keep track of the routes and has no ***facility for reordering datagrams once they arrive.***

The limited functionality of IP should not be considered a weakness; however, IP provides bare-bone transmission functions that free user to add only those facilities necessary for a given application and thereby allows for maximum efficiency.

ARP (Address Resolution Protocol):

The ARP associates an IP address with the physical address (in which each device identified by physical address usually imprinted on the network interface card (NIC).

RARP (Reverse Address Resolution Protocol):

The RARP allows a host discovers its internet address when it knows only its physical address.

Note: A host supposed to have its internet address stored on its hard disk. But, RARP supposes that the host is diskless, or it is being connected to the network for the first time, or you get new a new computer but you decide to keep the old NIC.

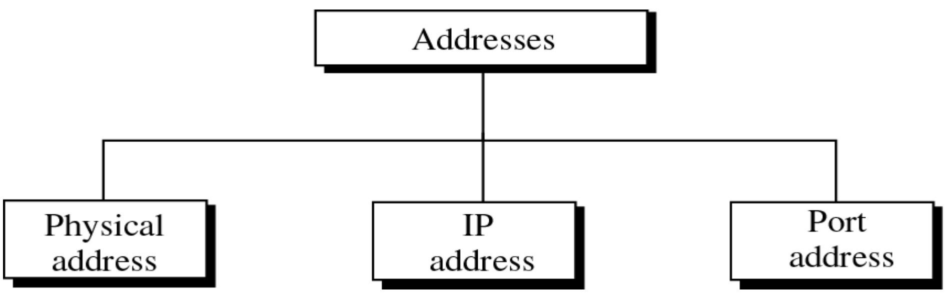
ICMP (Internet Control Message Protocol):

The ICMP is a mechanism used by hosts and routers to send notification of datagram problems back to the sender.

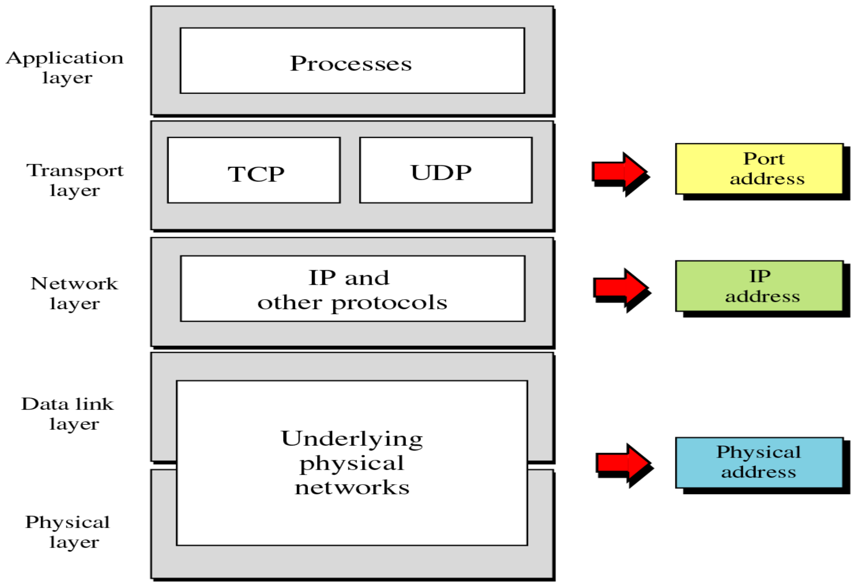
IGMP (Internet Group Message Protocol):

The IGMP has been designed to help multicast (multipoint) router identify the hosts in a LAN that are members of multicast group. It is a companion to the IP.

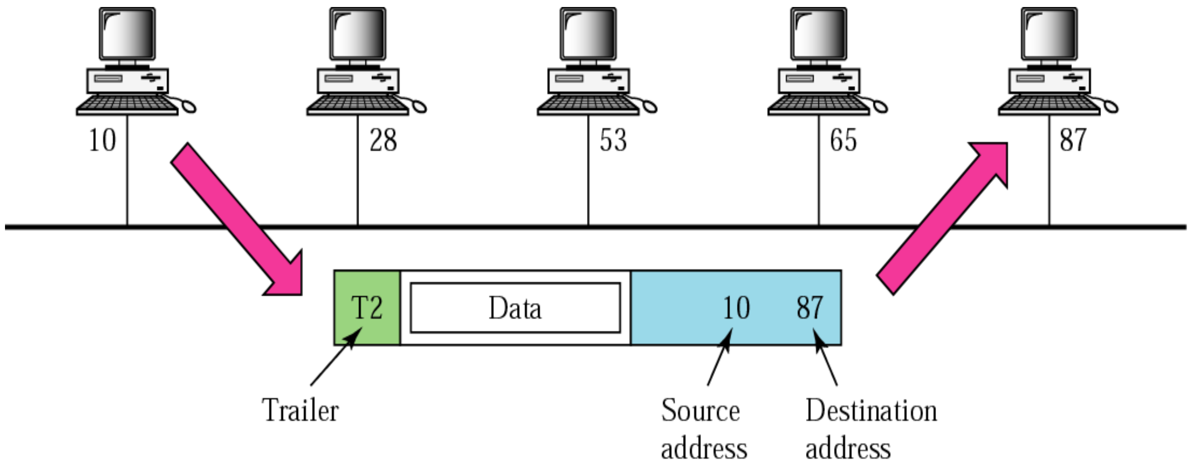
<u>Addresses in TCP/IP:</u>



<u>Relationship of layers and addresses in TCP/IP:</u>



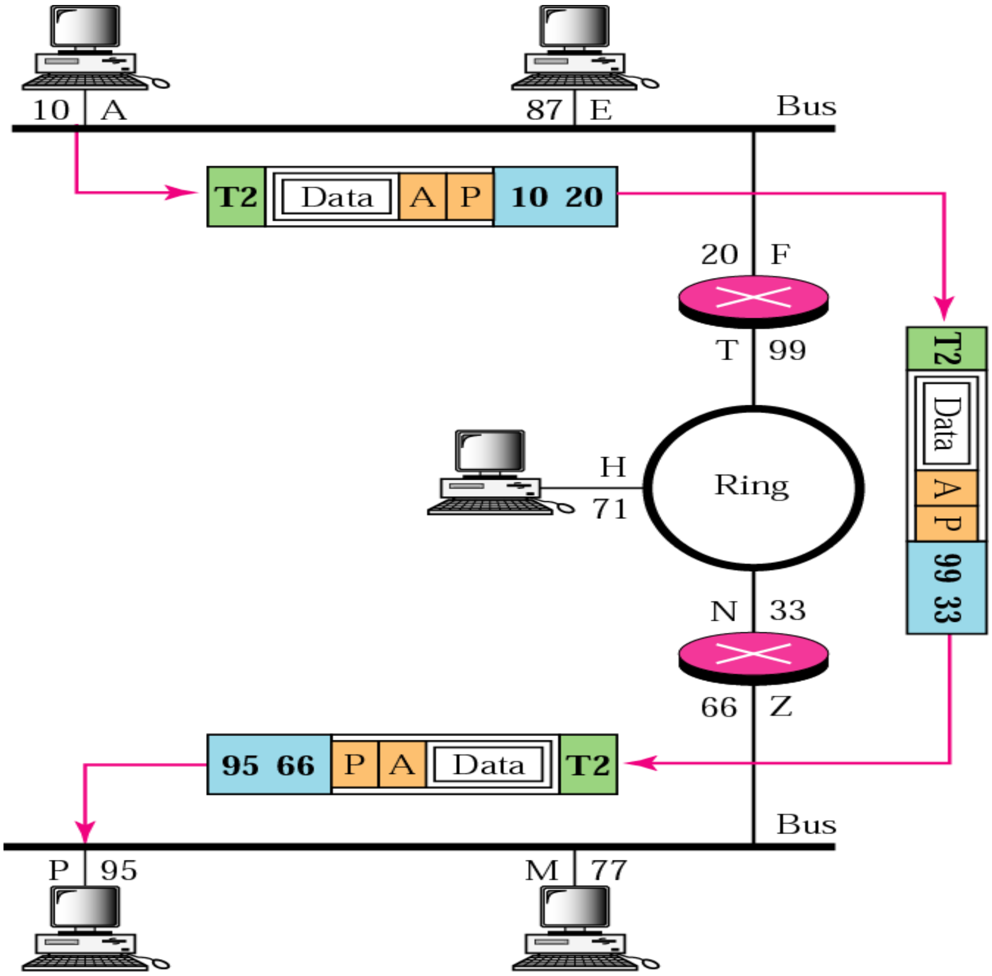
Physical addresses:



Most local area networks use a 48-bit (6 bytes) physical address written as 12 hexadecimal digits, with every 2 bytes separated by a hyphen as shown: 07-01-02-01-2C-4B

A 6-byte (12 hexadecimal digits) physical address

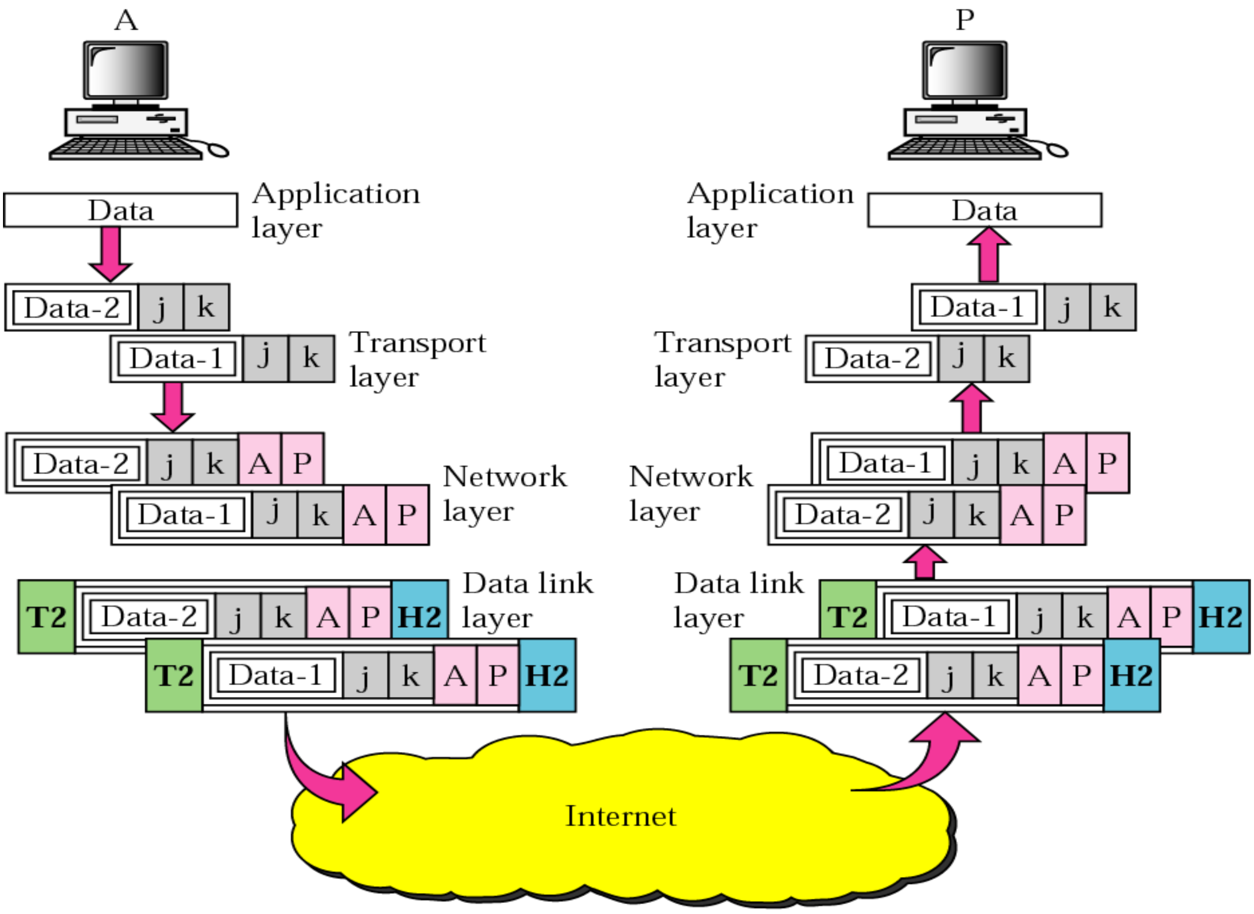
IP addresses:



an Internet address (in IPv4) is 32 bits in length, normally written as four decimal numbers, with each number representing 1 byte. The numbers are separated by a dot. Below is an example of such an address.

132.24.75.9

Port addresses:



a port address is a 16-bit address represented by one decimal number as shown below.

753 A 16-bit port address

IP Addresses:

An IP address is a 32-bit address. The IP addresses are unique.

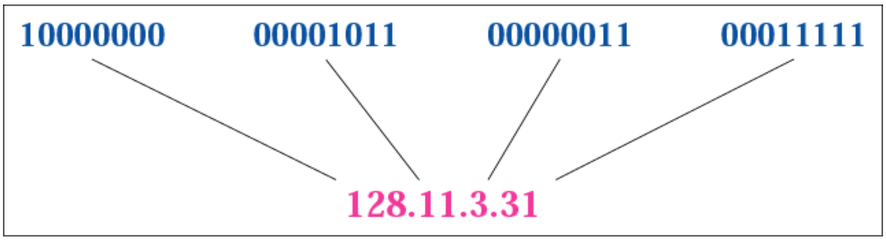
Rule:

If a protocol uses N bits to define an address, the address space is 2N because each bit can have two different values (0 and 1) and N bits can have 2N values.

The address space of IPv4 is 2^{32} or 4,294,967,296

Binary notation: **01110101 10010101 00011101 11101010**

Dotted decimal notation:



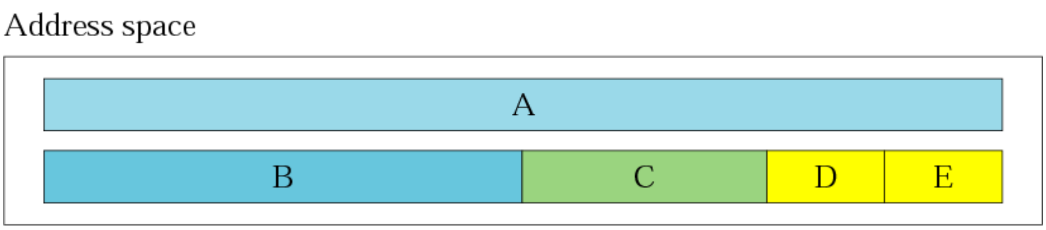
Hexadecimal Notation:

0111 0101 1001 0101 0001 1101 1110 1010

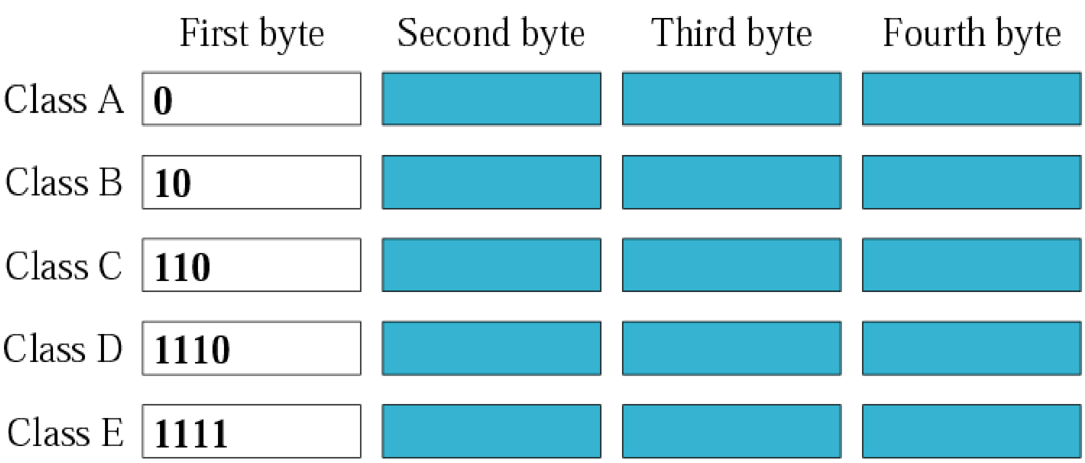
75 95 1D EA

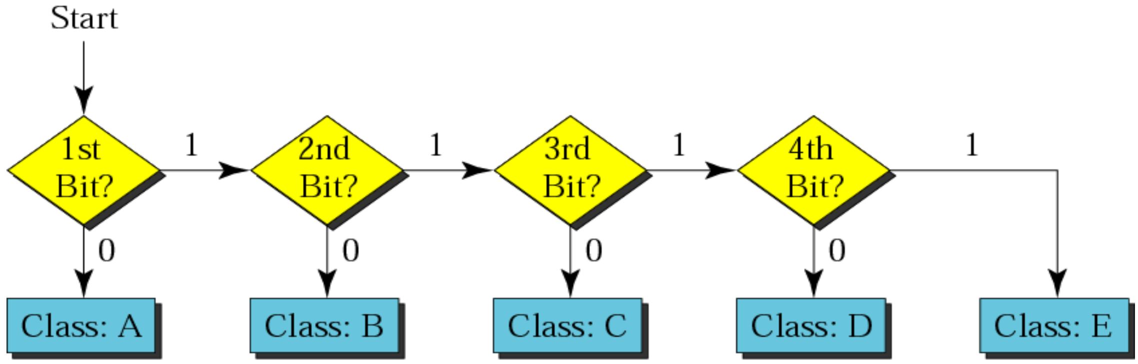
0x75951DEA

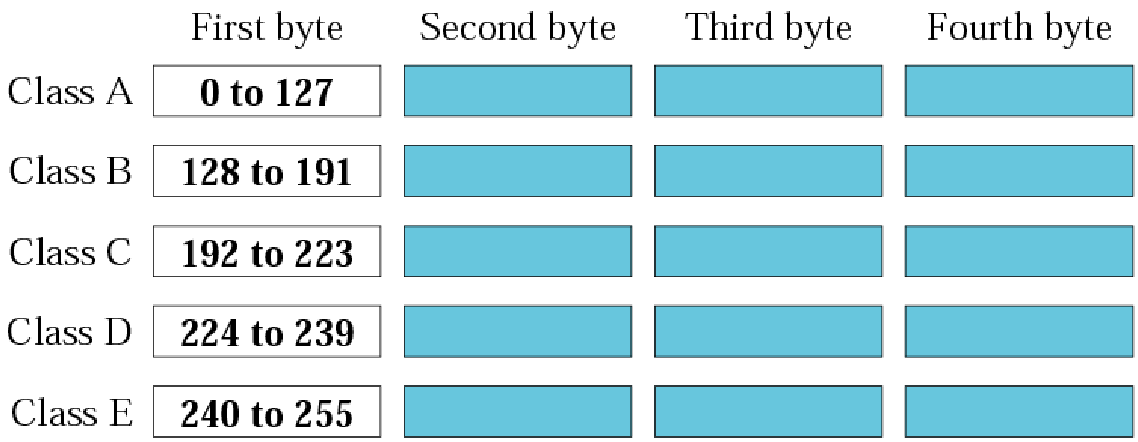
CLASSFUL ADDRESSING:

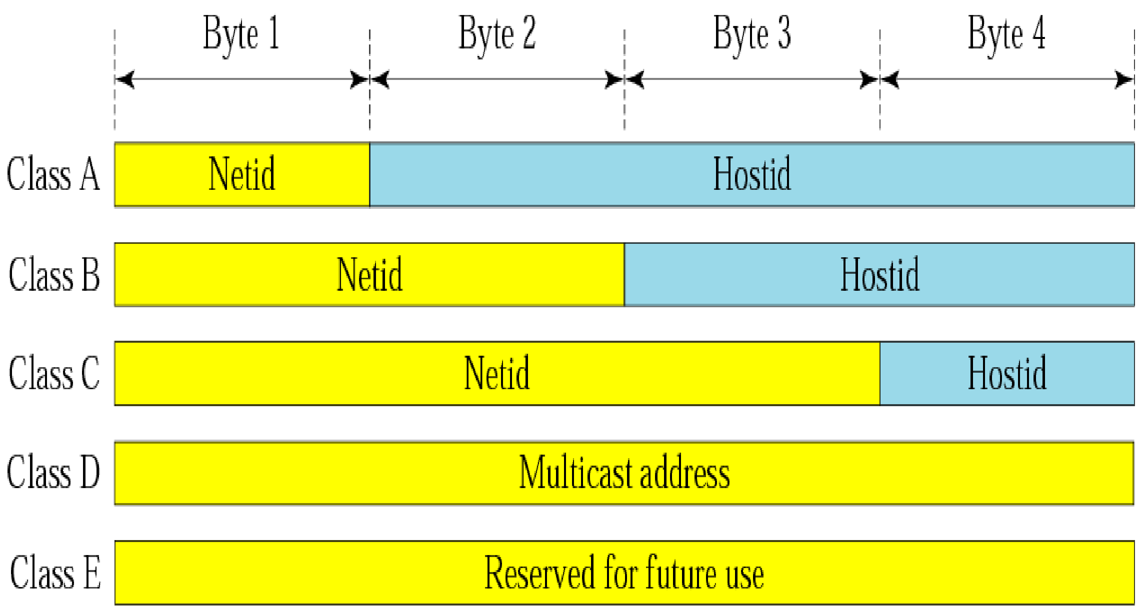


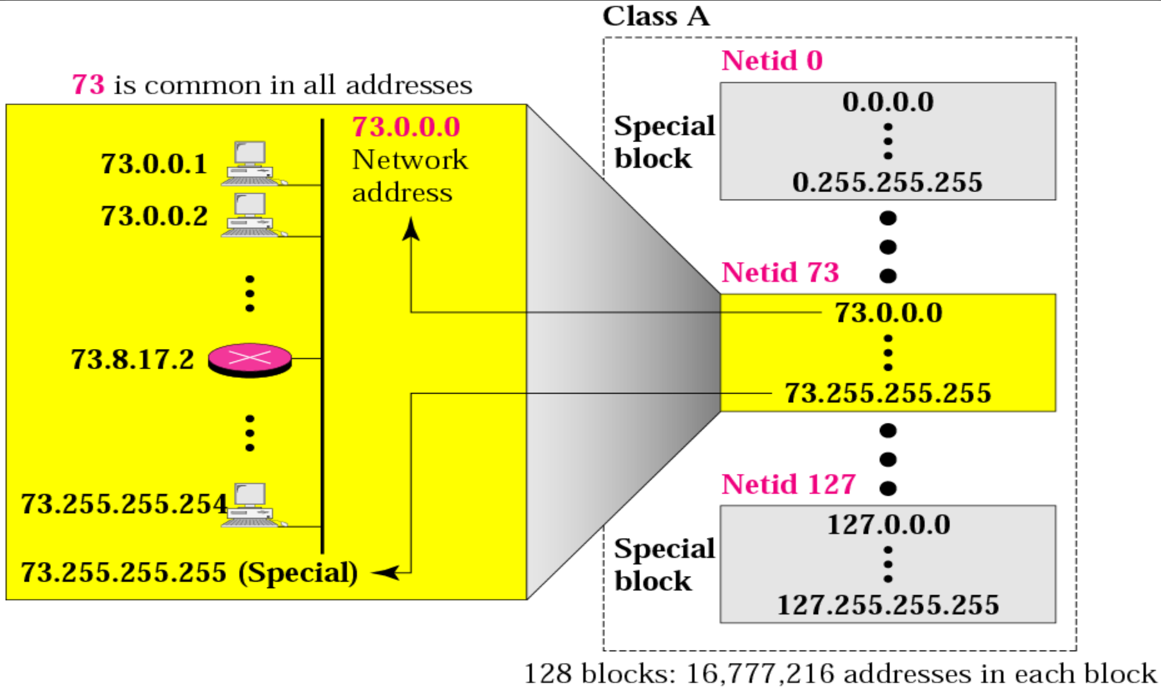
In Classful Addressing, the address space is divided into five classes: ***A, B, C, D, and E.***



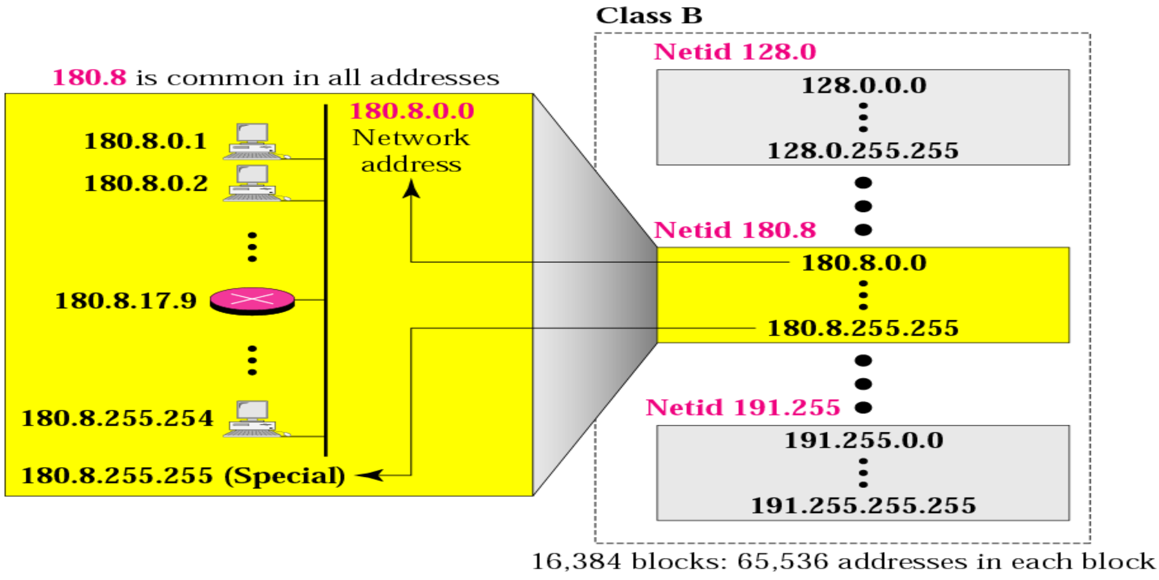

Start
1st Bit?
2nd Bit?
3rd Bit?
4th Bit?
1
0
Class: A
Class: B
Class: C
Class: D
Class: E


First byte
Second byte
Third byte
Fourth byte
Class A
0 to 127
Class B
128 to 191
Class C
192 to 223
Class D
224 to 239
Class E
240 to 255

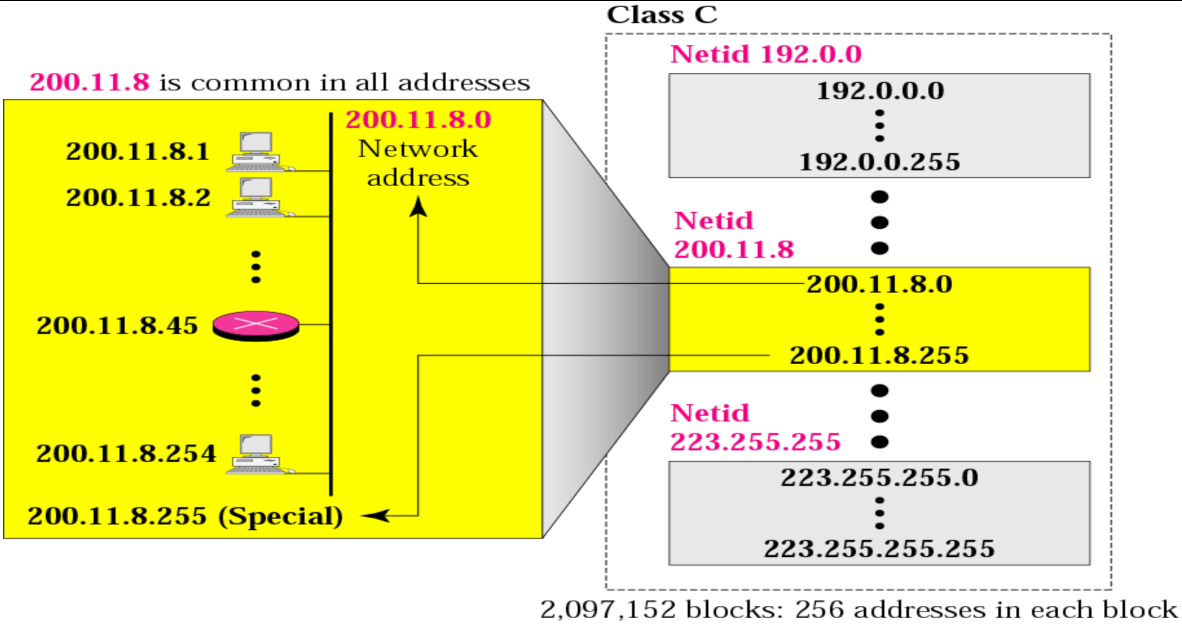

Byte 1
Byte 2
Byte 3
Byte 4
Class A
Netid
Hostid
Class B
Netid
Hostid
Class C
Netid
Hostid
Class D
Multicast address
Class E
Reserved for future use



NOTE: Millions of class A addresses are wasted.



NOTE: Many class B addresses are wasted.



The number of addresses in a class C block is smaller than the needs of most organizations. Class D addresses are used for multicasting; there is only one block in this class. Class E addresses are reserved for special purposes; most of the block is wasted.

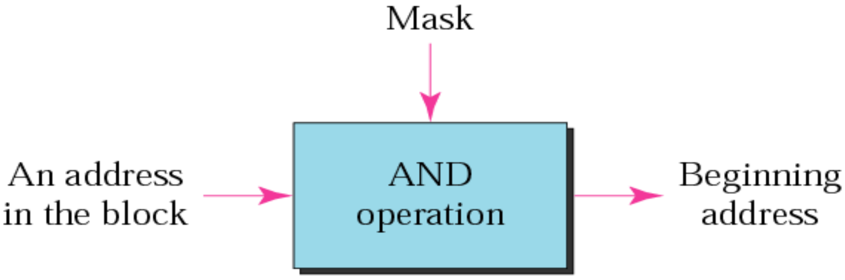
The network address is the first address. The network address defines the network to the rest of the Internet. Given the network address, we can find the class of the address, the block, and the range of the addresses in the block.

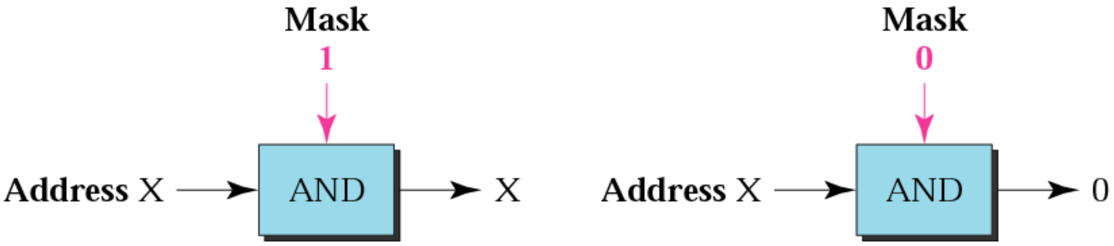
In Classful addressing, the network address (the first address in the block) is the one that is assigned to the organization.

EX: Given the network address 17.0.0.0, find the class, the block, and the range of the addresses.

The class is A because the first byte is between 0 and 127. The block has a netid of 17. The addresses range from 17.0.0.0 to 17.255.255.255.

Mask: A mask is a 32-bit binary number that gives the first address in the block (the network address) when bitwise ANDed with an address in the block.



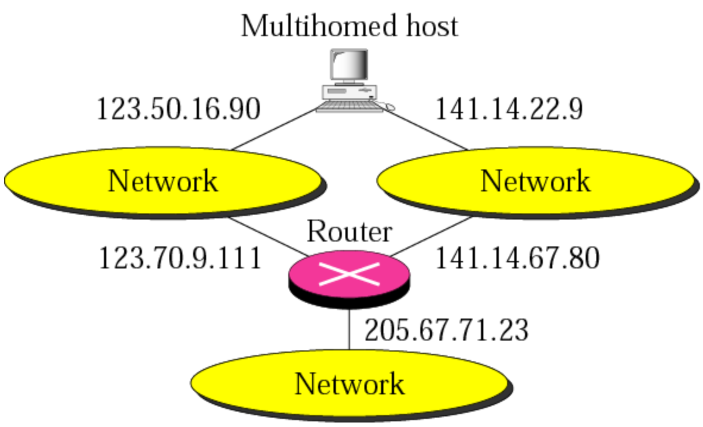


The network address is the beginning address of each block. It can be found by applying the default mask to any of the addresses in the block (including itself). It retains the netid of the block and sets the hostid to zero.

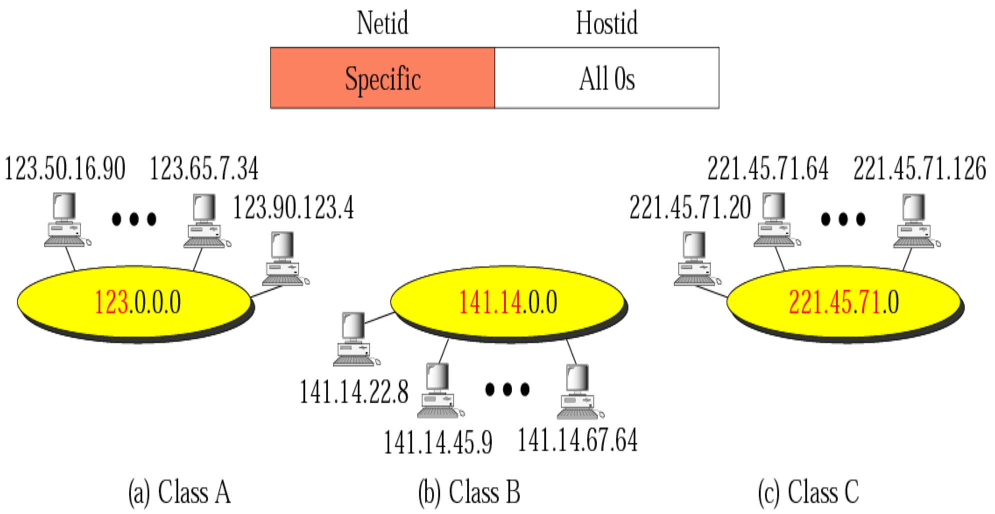
EX: Given the address 23.56.7.91 and the default class A mask, find the beginning address (network address).

The default mask is 255.0.0.0, which means that only the first byte is preserved and the other 3 bytes are set to 0s. The network address is 23.0.0.0.

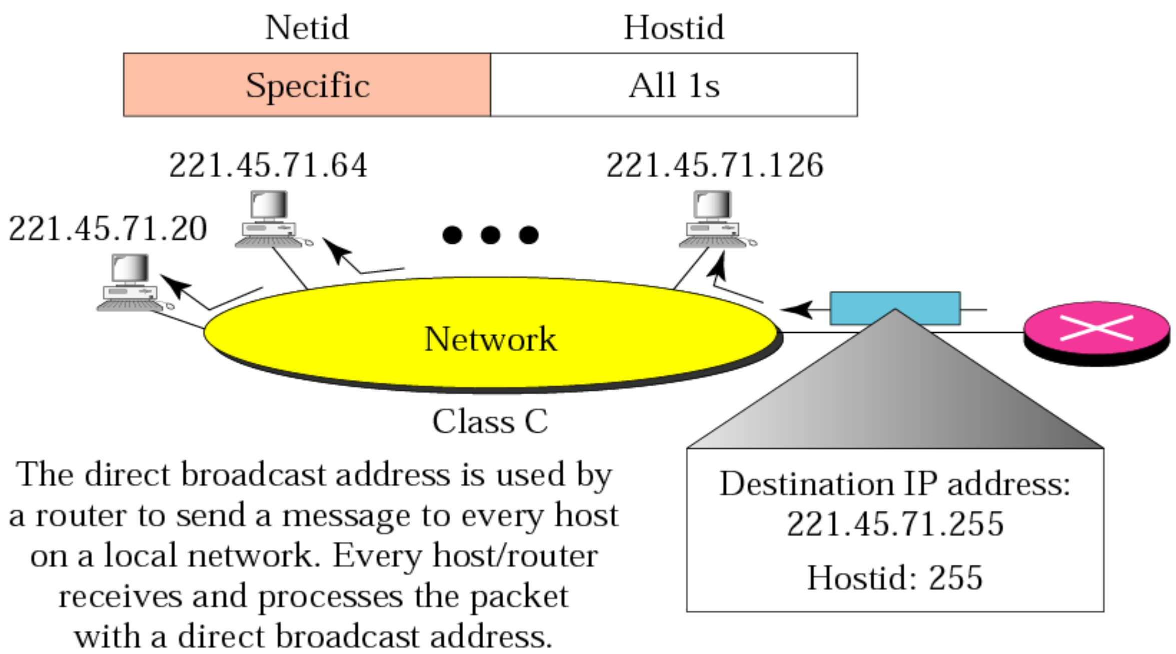
We must not apply the default mask of one class to an address belonging to another class.



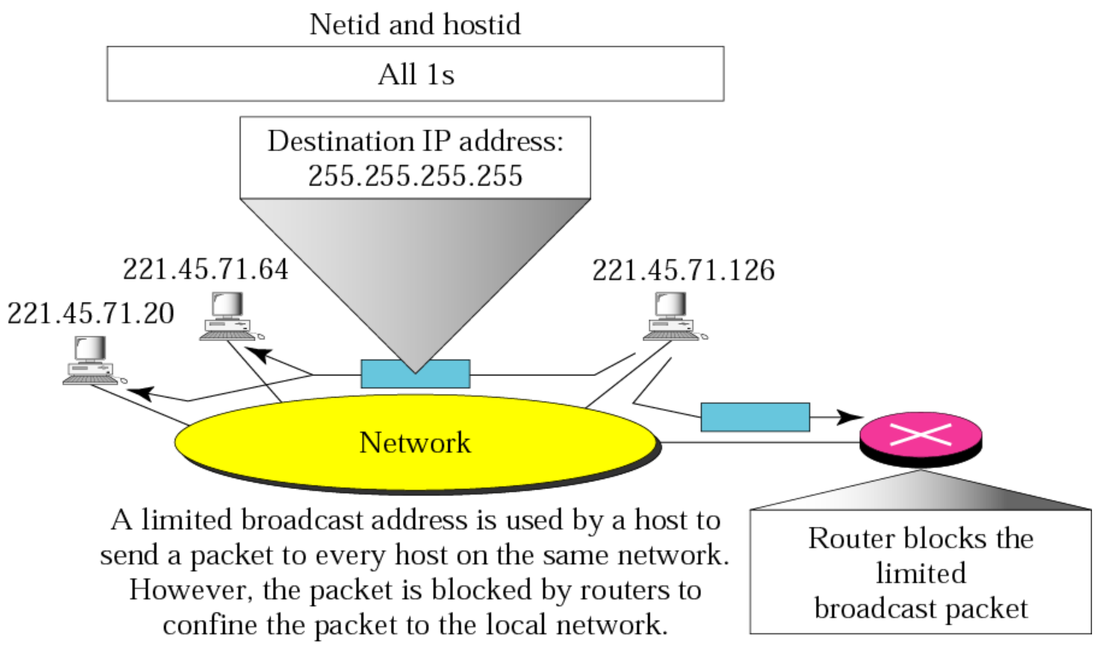
Network addresses:



Example of direct broadcast address:



Example of limited broadcast address:



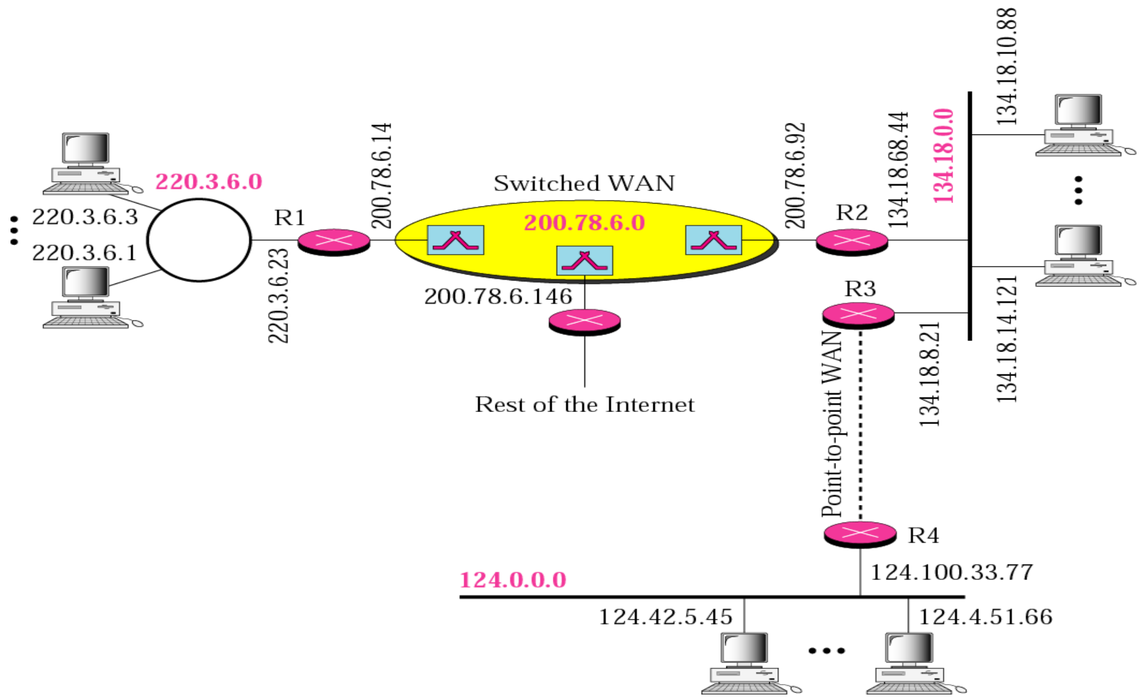
Unicast, Multicast, and Broadcast Addresses:

Unicast communication is *one-to-one*.

Multicast communication is *one-to-many*.

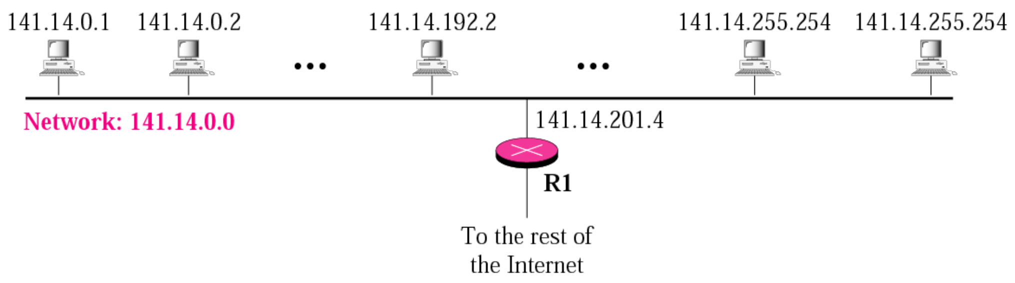
Broadcast communication is *one-to-all*.

Sample internet:

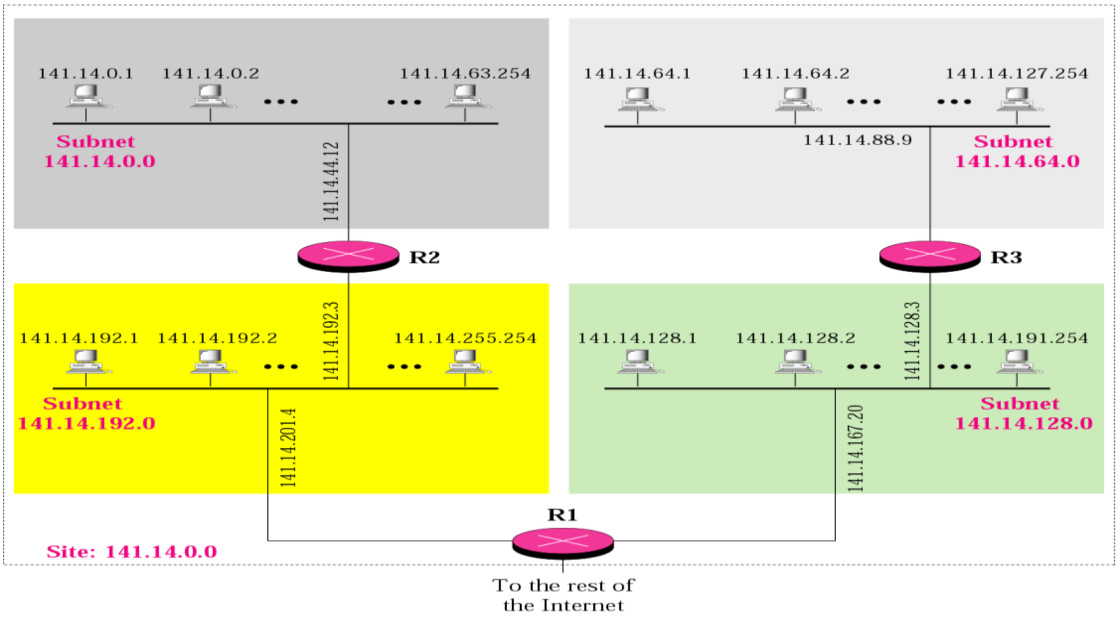


Subnetting/Supernetting:

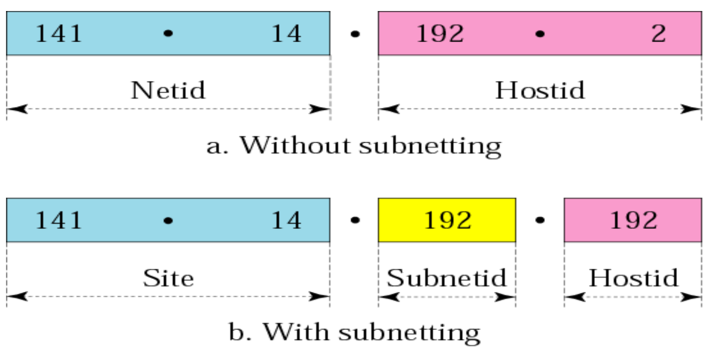
Subnetting: IP addresses are designed with two levels of hierarchy.



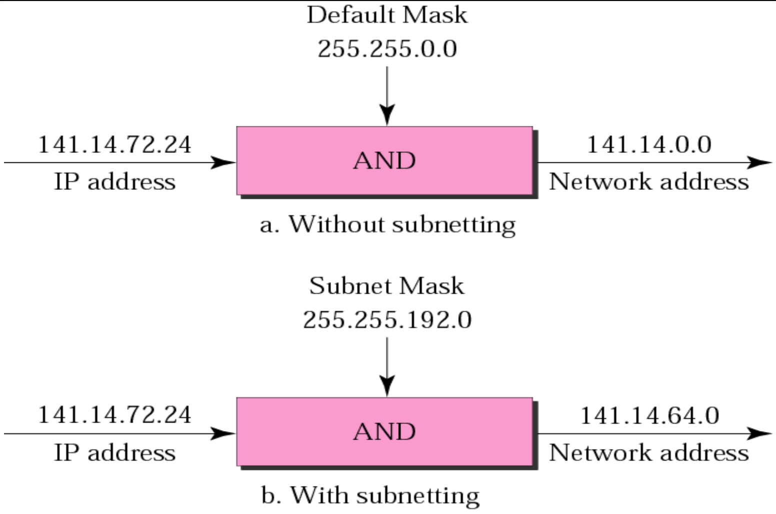
A network with three levels of hierarchy (subnetted)



Addresses in a network with and without subnetting:



Default mask and subnet mask:



Finding the Subnet Address:

We can do this in two ways: straight or short-cut.

EX: What is the subnetwork address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0?

11001000 00101101 00100010 00111000

11111111 11111111 1111**0000** **00000000**

11001000 00101101 0010**0000** **00000000**