# Chapter Four

# Internet Protocol (IP) and IP Addressing

## Data Communication and Computer Networks

(SEng2051)

haleluyaluya@yahoo.com

# Internet Protocol (IP)

- The **Internet Protocol** (**IP**) is a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.
- IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose the Internet Protocol defines addressing methods and structures for datagram encapsulation.
- The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4) is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide (128 bits).

# Contd.

- Communication at the network layer is host-to-host (computer-to-computer); a computer communicate with any computer anywhere else in the world.
- Usually, computers communicate through the Internet.
- The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer.
- For this level of communication, we need a global addressing scheme; we use the term IP address to mean a logical address in the network layer of the TCP/IP protocol suite. (What is phisical address?)

# IPv4 Addresses

- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (a computer or a router) to the Internet.
- IPv4 addresses are unique and universal.
- They are unique in the sense that each address defines one, and only one, connection to the Internet.
- Two devices on the Internet can never have the same address at the same time.

# Address Space

- A protocol such as IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses N bits to define an address, the address space is $2^N$ because each bit can have two different values (0 or 1) and N bits can have $2^N$ values.
- IPv4 uses 32-bit addresses, which means that the address space is $2^{32}$ or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.
- The actual number is much less because of the restrictions imposed on the addresses.

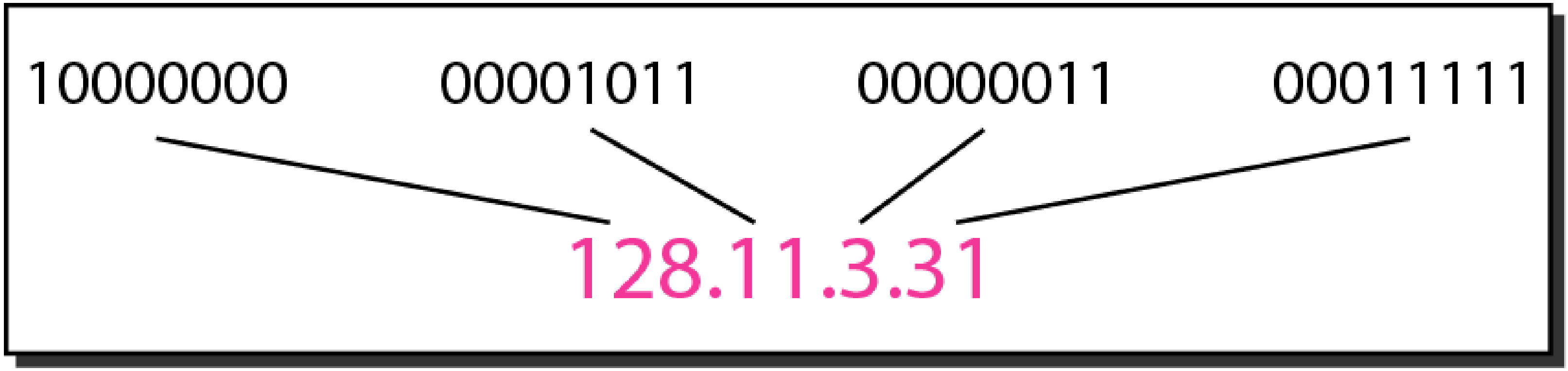
# Notations

- There are two prevalent notations to show an 1Pv4 address: binary notation and dotted-decimal notation.
- Binary Notation
  - In binary notation, the IPv4 address is displayed as 32 bits, 4 Octets, Each octet is often referred to as a byte (4-byte address). Eg.:

    01110101 10010101 00011101 00000010
- Dotted-Decimal Notation
  - Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Eg:

    117.149.29.2

# Example: *Dotted-decimal notation and binary notation for an IPv4 address*



# *Example 1*

*Change the following IPv4 addresses from binary notation to dotted-decimal notation.*

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

## *Solution*

*We replace each group of 8 bits with its equivalent decimal number and add dots for separation.*

a. 129.11.11.239

b. 193.131.27.255

# *Example 2*

*Change the following IPv4 addresses from dotted-decimal notation to binary notation.*

a. 111.56.45.78

b. 221.34.7.82

## *Solution*

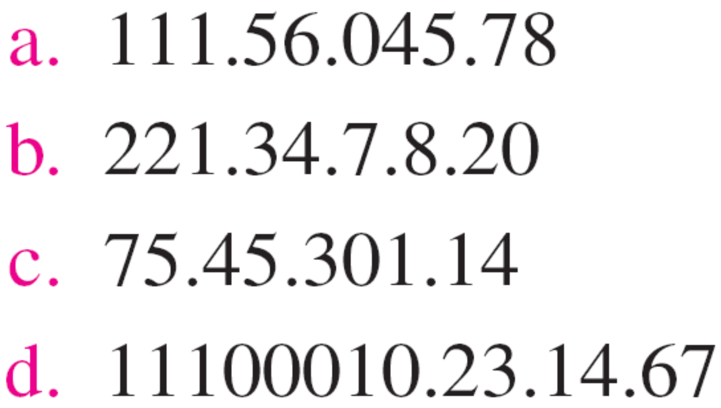
*We replace each decimal number with its binary equivalent.*

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

# *Example 3*

*Find the error, if any, in the following IPv4 addresses.*



a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

## *Solution*

*a. There must be no leading zero (045).*

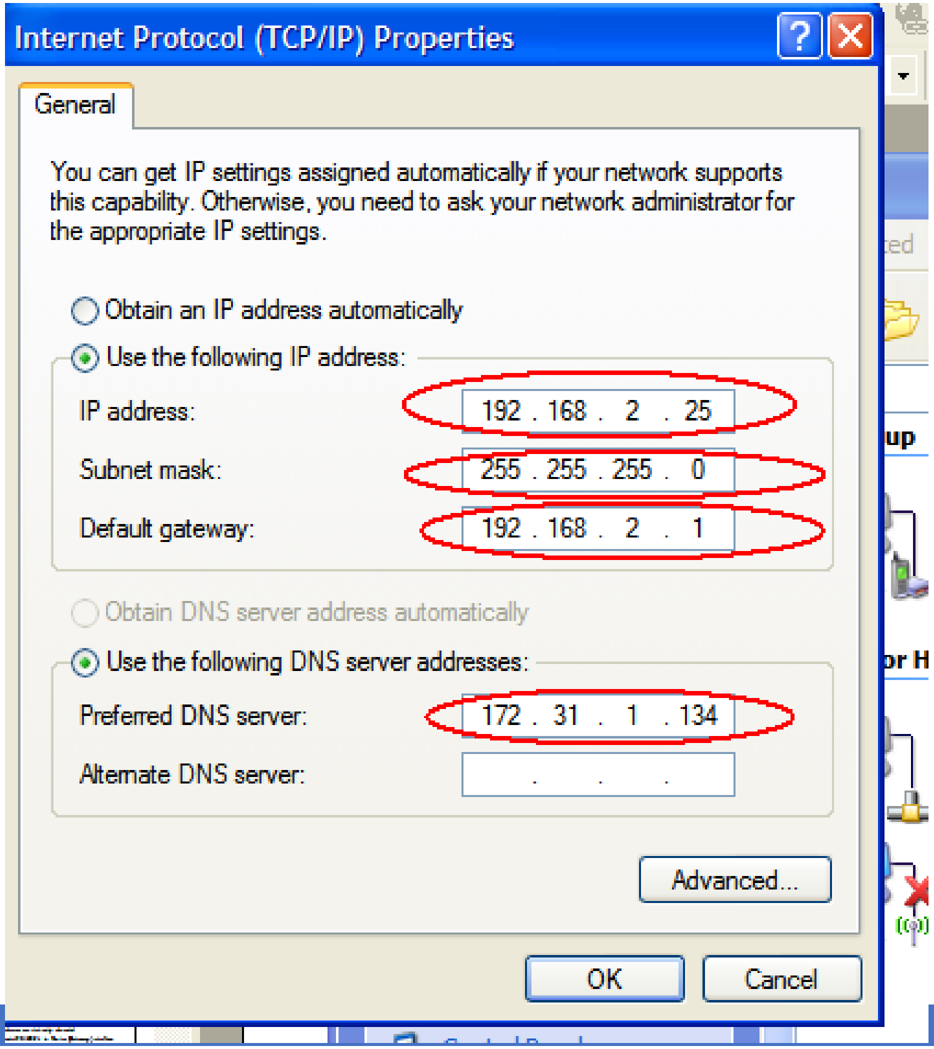
*b. There can be no more than four numbers.*

*c. Each number needs to be less than or equal to 255.*

*d. A mixture of binary notation and dotted-decimal notation is not allowed.*

# IP Configuration of an Interface

## Static



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

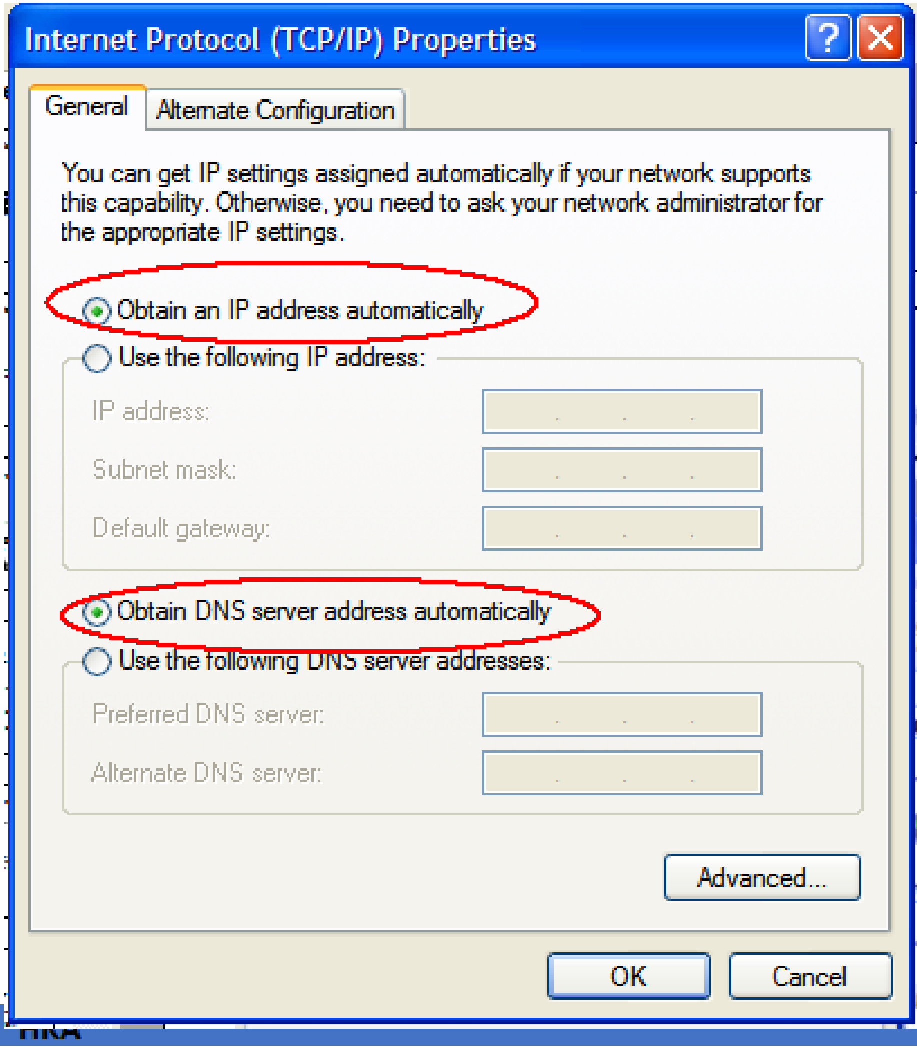
| | |
|---|---|
| IP address: | 192 . 168 . 2 . 25 |
| Subnet mask: | 255 . 255 . 255 . 0 |
| Default gateway: | 192 . 168 . 2 . 1 |

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

| | |
|---|---|
| Preferred DNS server: | 172 . 31 . 1 . 134 |
| Alternate DNS server: | . . . |

## DHCP



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

| | |
|---|---|
| IP address: | . . . |
| Subnet mask: | . . . |
| Default gateway: | . . . |

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

| | |
|---|---|
| Preferred DNS server: | . . . |
| Alternate DNS server: | . . . |

# Classful Addressing

- IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing.
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.

| | First byte | Second byte | Third byte | Fourth byte |
|---|---|---|---|---|
| Class A | 0 | | | |
| Class B | 10 | 🟨 | | |
| Class C | 110 | 🟨 | 🟨 | |
| Class D | 1110 | | | |
| Class E | 1111 | | | |

a. Binary notation

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

b. Dotted-decimal notation

# *Example 4*

*Find the class of each address.*

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

*Solution*

a. *The first bit is 0. This is a class A address.*

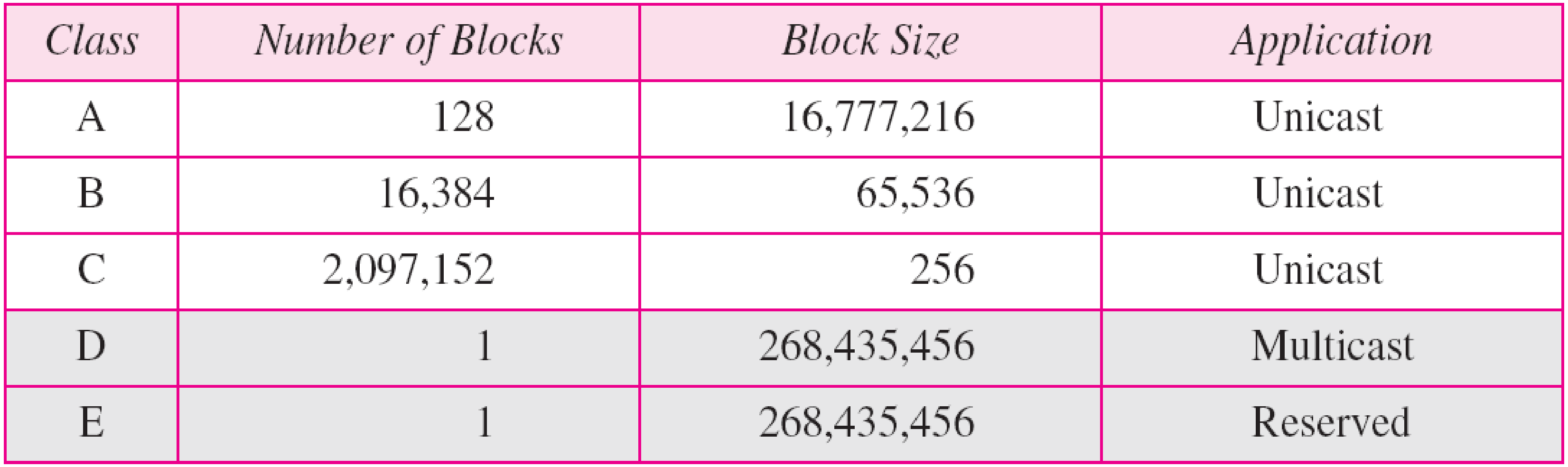
b. *The first 2 bits are 1; the third bit is 0. This is a class C address.*

c. *The first byte is 14; the class is A.*

d. *The first byte is 252; the class is E.*

# Classes and Blocks

- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size



| *Class* | *Number of Blocks* | *Block Size* | *Application* |
|---|---|---|---|
| A | 128 | 16,777,216 | Unicast |
| B | 16,384 | 65,536 | Unicast |
| C | 2,097,152 | 256 | Unicast |
| D | 1 | 268,435,456 | Multicast |
| E | 1 | 268,435,456 | Reserved |

Number of Blocks for class A = $2^7$
Number of Blocks for class B = $2^{14}$
Number of Blocks for class C = $2^{21}$

Block size for class A = $2^{24}$
Block size for class B = $2^{16}$
Block size for class C = $2^8$

# Class A

- If the first bit of an IP address is 0, it is the address of a class A network.
- The first bit of a class a address identifies the address class.
- The next seven bits identify the network, and
- The last 24 bits identify the host.
- There are fewer than 128 class a network numbers, but in each class a network can have millions of hosts.

# Class A

- |_| first one bit is used to determine the class to which an address belongs to for Class A address.
- |________| 7 bits are used for Network address.Therefore, the number of class A networks can be 2 $^{7}$ = 128. Number 0 is not used, and number 127 is used for testing loopback for each host. There are 126 potential Class A network numbers, which have a first dotted decimal number in the range 1 to 126.
- |___________________________| 24 bits are used for host address. Therefore, each Class A network can have 2 $^{24}$ = 16,777,216 hosts.
- Class A is not available to the general public, and it is restricted to special uses.
- ***Class A final format:***
- |_|________| |___________________________|
- *7 bits                    24 bits*<br>*Network          Host*<br>*Part                        Part*

# Class A

***Summary:***

- If the the first decimal number in IP address is 1 to  126, then it is a class A address.
- The first byte is for the network number, and the next three bytes are for the host addresses.

# Class B

- If the fir**st two** bits of the address are **1** and **0**, it is a class B network address.
- The first **two** bits identify class; the next **fourteen** bits  identify the network, and the last **sixteen** bits identify the host.
- There are thousands of class B network numbers.
- Each class B network can have thousands of hosts.

# Class B

- |__|  first two bits are used to determine the class to which an address belongs to for class B address.
- |________________| 14 (6 + 8) bits are used for network address. Therefore, the number of class B networks can be $2^{14}$ =  16,384. There are 16,384 potential Class B network numbers, which have a first dotted decimal number in the range 128 to 191.
- |__________________| 16 bits  are used for host address. Therefore, each Class B network can have $2^{16}$ = 65,536 hosts.

# Class B

- ***Class B final format***

- |__|_______|__________| |____________________|
  14 bits Network part 16 bits Host part

***Summary:***

- If the the first decimal number in IP address is 128 to 191, then it is a class B address.
- The first two bytes identify the network.
- The last two bytes identify the host.

# Class C

- If the **first three** bits of the address are **1 1 0**, it is a class C network address.
- The first three bits are class identifiers.
- The next 21 bits are for the network address.
- The last eight bits  identify the host.
- There are millions of class C network numbers.
- However, each class C network can have 254 hosts.

# Class C

- |___| first three bits are used to determine the class to which an address belongs to for class C address.
- |_____|________|________| 21 (5 + 16) bits are used for network address. Therefore, the number of class C networks can be $2^{21}$ = 2, 097,152. There are 2,097,152 potential Class C network numbers, which have a first dotted decimal number in the range 192 to 223.
- |________| 8 bits are used for host address. Therefore, each Class C network can have $2^{8}$ = 256 hosts.

# Class C

***Class C final format***

|____|_______| |__________| |__________| |_________|

21 bits Network part                                8 bits host part

***Summary:***

- If the the first decimal number in IP address is 192 to 223, then it is a class C address.
- The first three bytes are for the network address.
- The last byte is for the host number.

# Summary

- **Class A**:Few networks, each with many hosts.
- **Class B**: Medium number of networks, each with a medium number of hosts
- **Class C**: Many networks, each with a few hosts.

# Summary.

- Previously, when an organization requested a block of addresses, it was granted one in class A, B, or C.
- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
- Class C addresses were designed for small organizations with a small number of attached hosts or routers.
- A block in class A address is too large for almost any organization. This means most of the addresses in class A were **wasted & were not used**.
- A block in class B is also very large, probably too large for many of the organizations that received a class B block.
- A block in class C is probably too small for many organizations.

# Summary

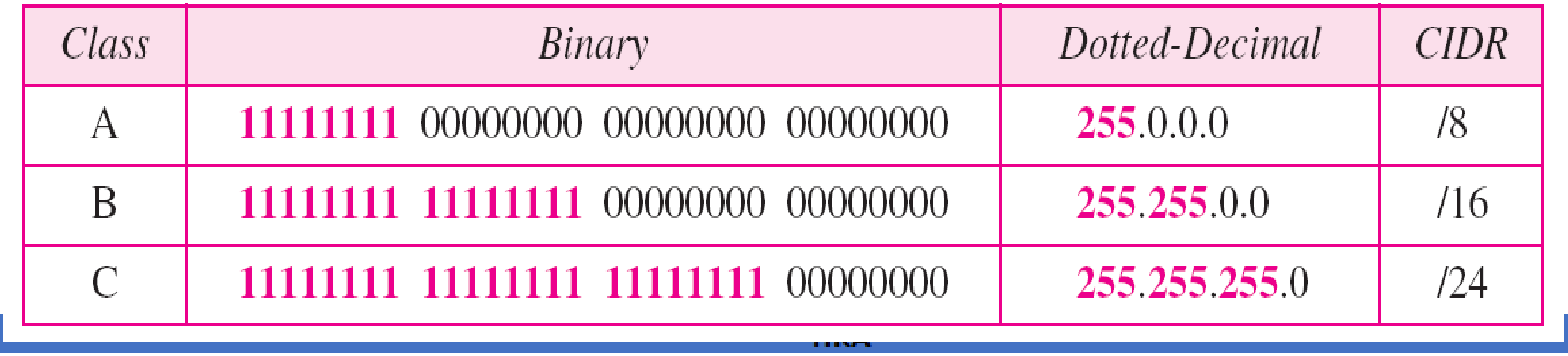
- In classful addressing, an IP address in class A, B, or C is divided into network ID and host ID.
- These parts are of varying lengths, depending on the class of the address.
- In class A, one byte defines the network ID and three bytes define the host ID.
- In class B, two bytes define the network ID and two bytes define the host ID.
- In class C, three bytes define the network ID and one byte defines the host ID.

# Loopback Address

- IP defines a loopback address used to test network applications.
- Programmers often use loopback testing for preliminary debugging after a network application has been created.
- To perform a loopback test, a programmer must have two application programs that are intended to communicate across a network.
- Each application includes the code needed to interact with TCP/IP protocol software.
- Instead of executing each program on a separate computer, the programmer runs both programs on a single computer and instructs them to use a loopback IP address when communicating.

# Default subnet Mask

- ❖ Although the length of the network ID and host ID (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask), a 32-bit number made of contiguous 1s followed by contiguous 0s. The masks for classes A, B, and C are shown below
- ❖ The mask can help us to find the network ID and the host ID. For example, the mask for a class A address has eight 1 s, which means the first 8 bits of any address in class A define the network ID; the next 24 bits define the host ID.



| *Class* | *Binary* | *Dotted-Decimal* | *CIDR* |
|---|---|---|---|
| A | 11111111 00000000 00000000 00000000 | 255.0.0.0 | /8 |
| B | 11111111 11111111 00000000 00000000 | 255.255.0.0 | /16 |
| C | 11111111 11111111 11111111 00000000 | 255.255.255.0 | /24 |

# SPECIAL IP ADDRESSES

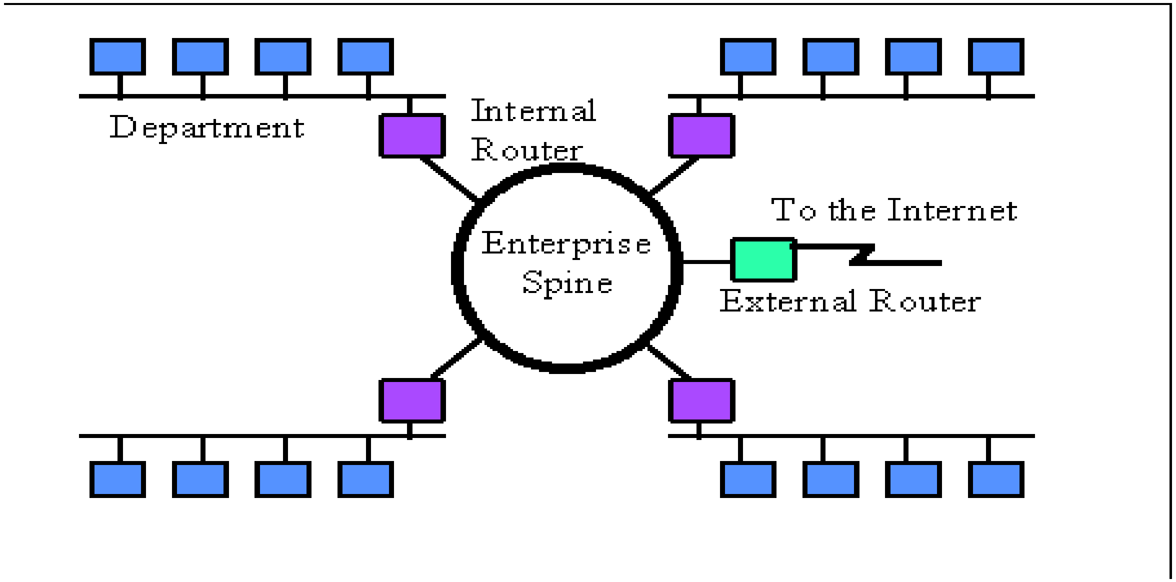
| IP addresses | also called | Description |
|---|---|---|
| **0.0.0.0 /0** | Default route | |
| **0.0.0.0/32** | This host | |
| **10.0.0.0-10.255.255.255** | Private IP address | Used for LAN in a private network |
| **127.0.0.0-127.255.255.255** | Loopback address | Used for loopback addresses |
| **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 |
| **172.16.0.0-172.31.255.255** | Private IP Address | Used for LAN in a private network |
| **192.168.0.0-192.168.255.255** | Private IP Address | Used for LAN in 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** | | |

# Subnetting

- During the era of classful addressing, subnetting was introduced.
- Classful IP addressing **does not provide any flexibility** of having less number of Hosts per Network or more Networks per IP Class.
- If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.
- Subnetting increases the number of 1s in the mask.
- Allocating a part of the host address space to network addresses, which will let you have more networks

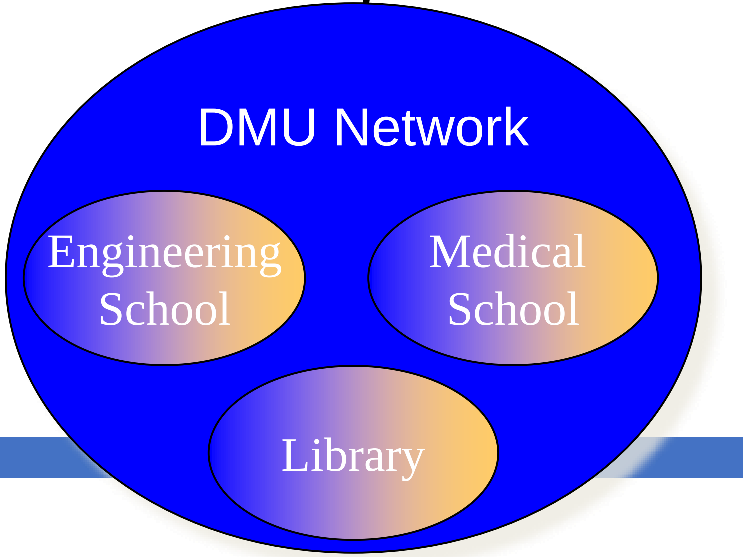
# Why subnetting?

- Preservation of address space
- Control network traffic, avoid collisions
- Reduce the routing complexity
- Improve network performance
- Security



# Subnet Design Considerations

1. How many total subnets does the organization need today?
2. How many total subnets will the organization need in the future?
3. How many hosts are there on the organization's largest subnet today?
4. How many hosts will there be on the organization's largest subnet in the future?



# Subnetting

- The subnet mask is used to determine the bits of the network identifier.
- All **hosts on the same network** should have the **same subnet mask**.
- **Steps:**
  - Determine the number of networks required and convert it into binary.
  - Reserve bits in the mask and find the increment
  - Find the network ranges based on the increment
- 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.

# Subnetting - soln

- **Solution**
  - 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.
  - 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.**111*1***0000
    - New subnet mask:  255.255.255.240 or /28
    - Increment=lowest bit in the network portion (Italic one) i.e. **16.**
  - Find the network ranges based on the increment

# VLSM (Variable Length Subnet Masks)

- VLSMs allow you to use different masks for each subnet, 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

# VLSM (Variable Length Subnet Masks)

- 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

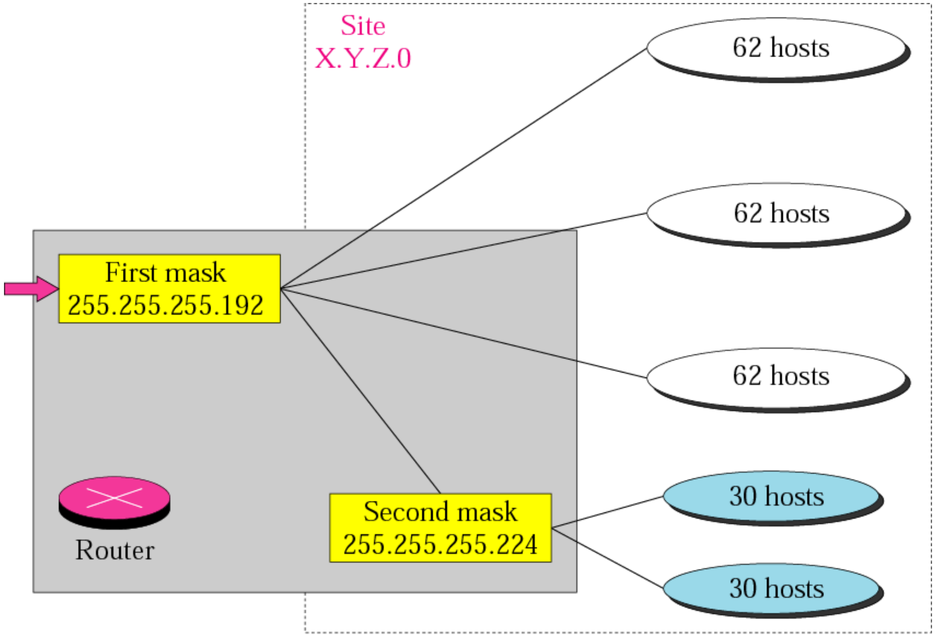
# VLSM (Variable Length Subnet Masks)

- A company is granted the site address 181.56.0.0 (class B). The company needs 1000 subnets. Design the subnets.
- But, what if it has two departments with 30 computers.

The number of 1s in the default mask is 16 (class B).

Number of bits borrowed 1024 ($2^{10}$).

The total number of 1s in the subnet mask is 26 (16 + 10).

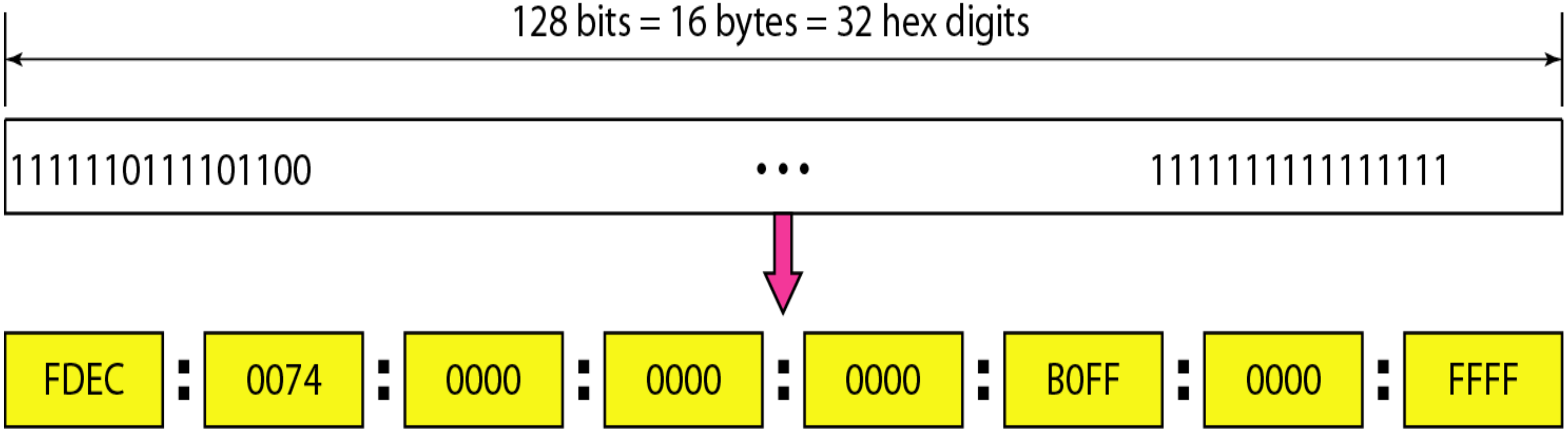


# IPv6 ADDRESSES

- 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.
    - Future Internet addresses
  - 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.

# IPv6 ADDRESSES

- An IPv6 address is 128 bits or 32 hexadecimal digits long.



128 bits = 16 bytes = 32 hex digits

1111110111101100 • • • 1111111111111111

FDEC : 0074 : 0000 : 0000 : 0000 : B0FF : 0000 : FFFF

# IPv6 ADDRESSES

- 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.

# IPv6 Provider-Based Addresses

- The first IPv6 addresses will be allocated to a provider-based plan

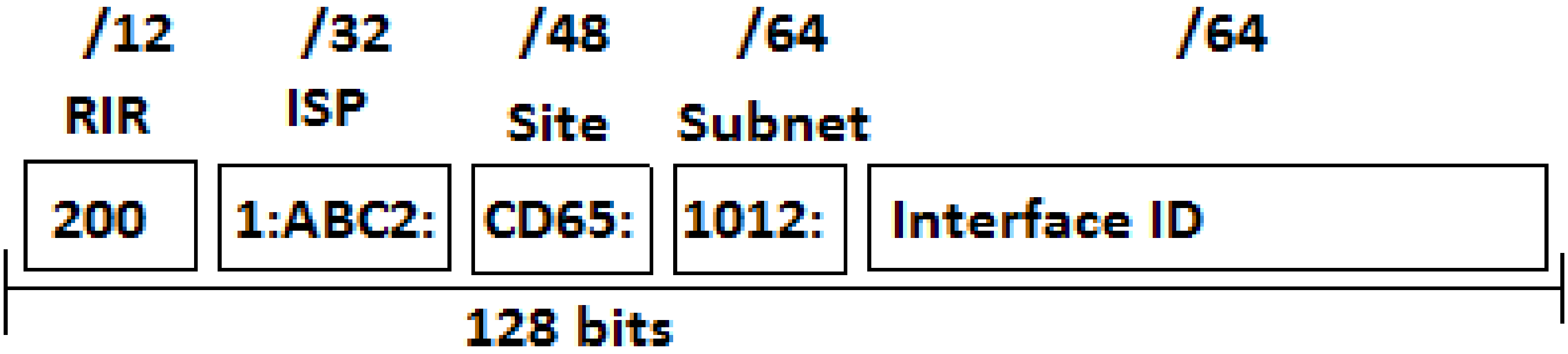
| | | | | | |
|---|---|---|---|---|---|
| 010 | Registry ID | Provider ID | Subscriber ID | Subnetwork ID | Interface ID |

- Type: Set to “010” for provider-based addresses
- Registry: identifies the agency that registered the address

*The following fields have a variable length (recommeded length in “() ”)*

- Provider: Id of Internet access provider *(16 bits)*
- Subscriber: Id of the organization at provider *(24 bits)*
- Subnetwork: Id of subnet within organization *(32 bits)*
- Interface: identifies an interface at a node *(48 bits)*

# IPv6 ADDRESSES



**0010000000000001** 0000000000000000 **0011001000111000** 1101111111100001 **0000000001100011** 0000000000000000 **0000000000000000** 1111111011111011

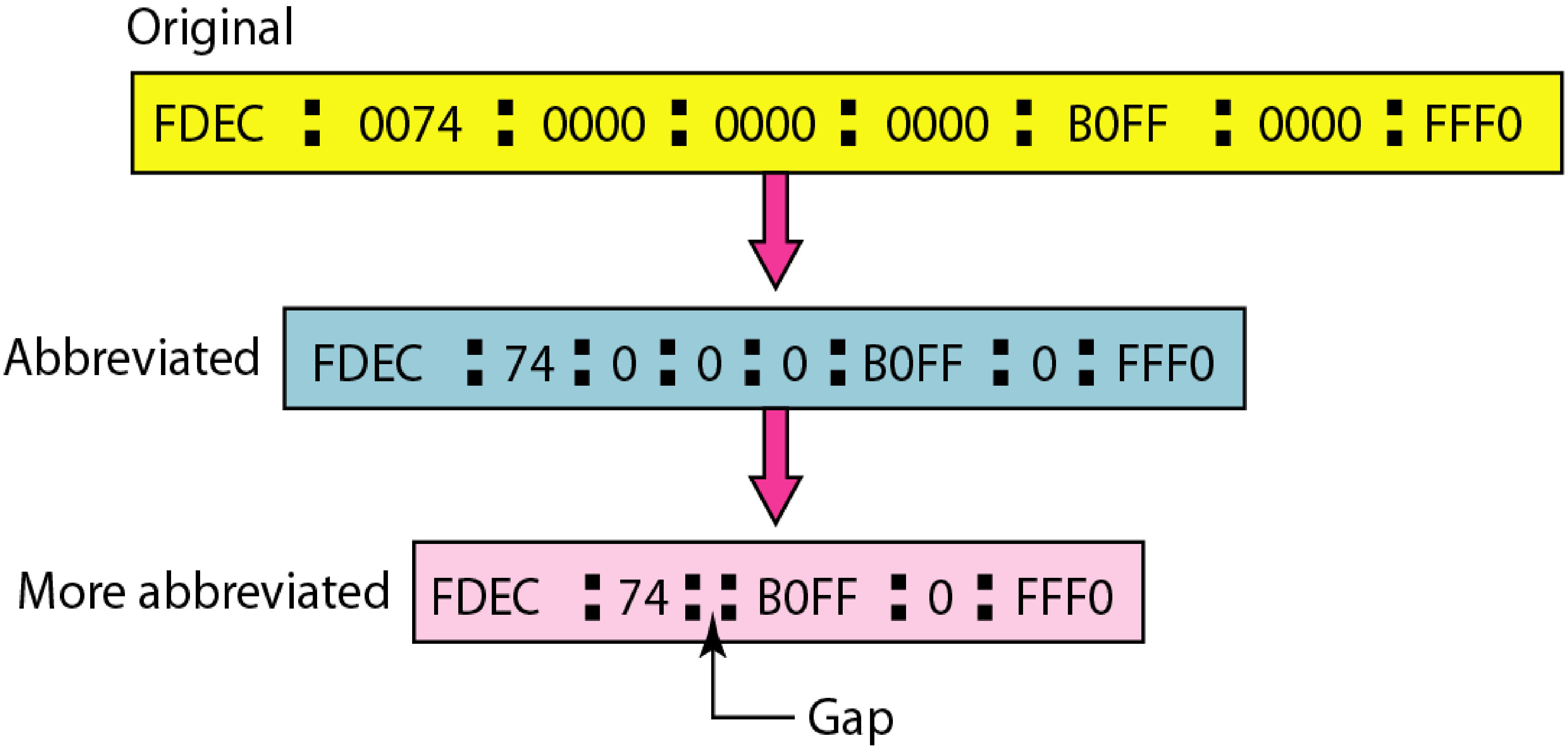
**Each block is then converted into Hexadecimal and separated by ‘:’ symbol:**

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

# IPv6 ADDRESSES

- Even after converting into Hexadecimal format, IPv6 address remains long. 2001:0000:3238:DFE1:0063:0000:0000:FEFB
- Some rules to shorten the address.
- **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
- **Rule 3:** 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

# Abbreviated IPv6 addresses



Original

FDEC : 0074 : 0000 : 0000 : 0000 : B0FF : 0000 : FFF0

Abbreviated

FDEC : 74 : 0 : 0 : 0 : B0FF : 0 : FFF0

More abbreviated

FDEC : 74 :: B0FF : 0 : FFF0

Gap

# More on IPv6 Addresses

- The provider-based addresses have a similar flavor as CIDR addresses
- IPv6 provides address formats for:
  - Unicast – identifies a single interface
  - Multicast – identifies a group. Datagrams sent to a multicast address are sent to all members of the group
  - Anycast – identifies a group. Datagrams sent to an anycast address are sent to one of the members in the group.

# IPv6 Address types

- In IPv6, a destination address can belong to one of three categories:
- ***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.
- ***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.
- ***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. It is interesting that IPv6 does not define broadcasting, even in a limited version. IPv6 considers broadcasting as a special case of multicasting.

# Special IPv6 Addresses

| 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 |

# TRANSITION FROM IPv4 TO IPv6

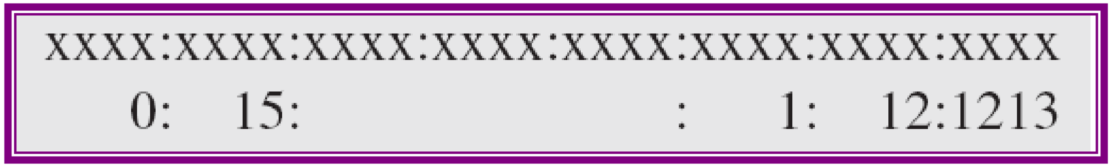
- Three strategies have been devised for transition:
  - ***Dual Stack***
    - It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols during the transition. In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.
  - ***Tunneling***
    - 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.
  - ***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. 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.

# Example 9

*Expand the address 0:15::1:12:1213 to its original.*

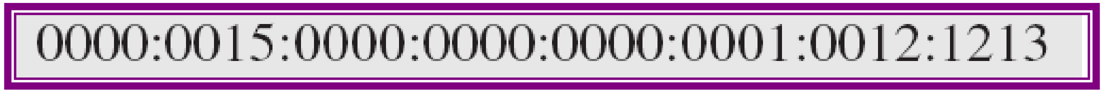
## Solution

*We first need to align the left side of the double colon to the left of the original pattern and the right side of the double colon to the right of the original pattern to find how many 0s we need to replace the double colon.*



```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
   0:   15:                 :   1:   12:1213
```

*This means that the original address is.*



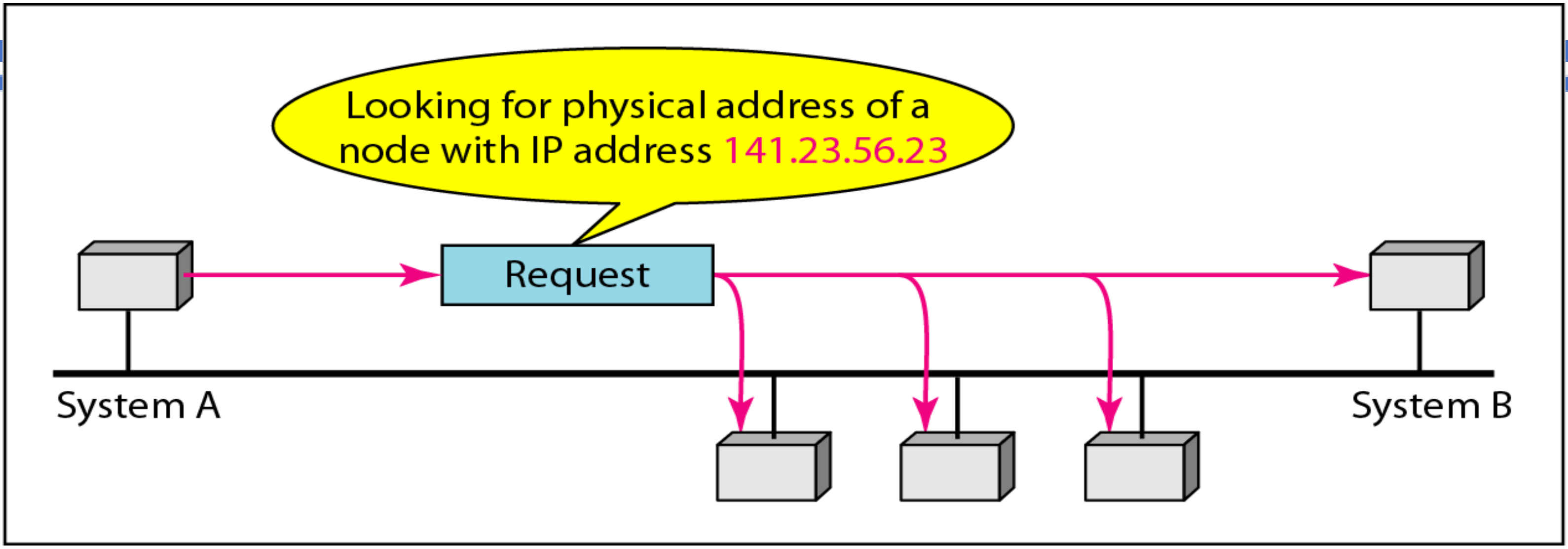
```
0000:0015:0000:0000:0000:0001:0012:1213
```

# ADDRESS MAPPING

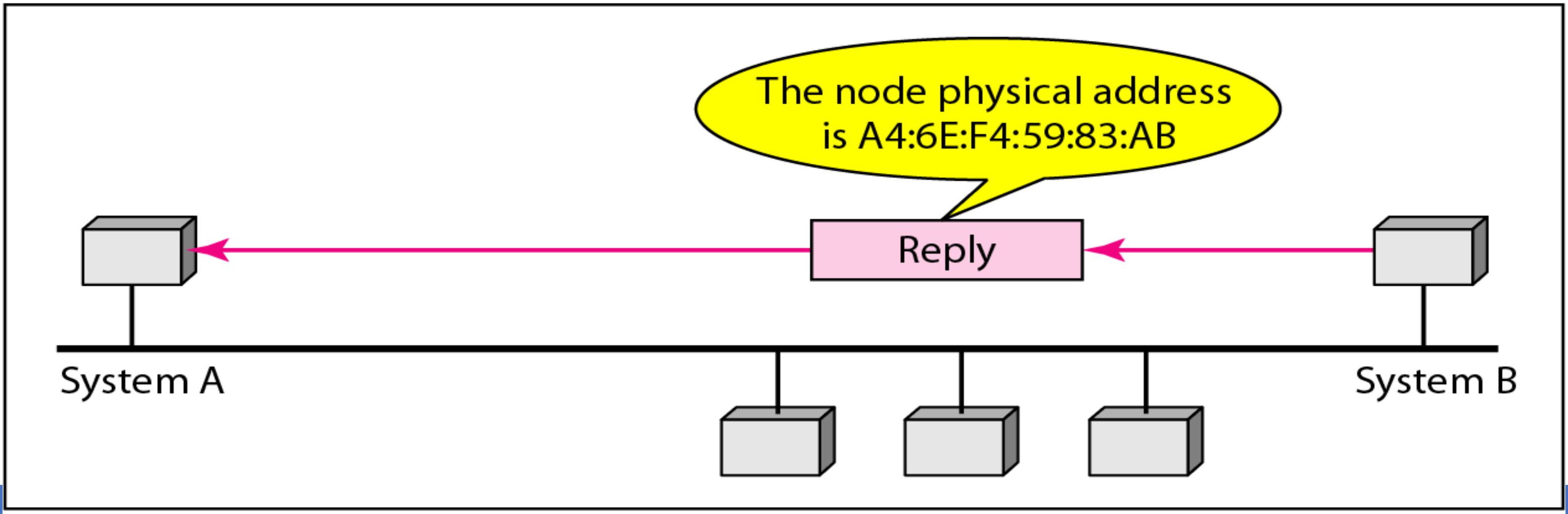
- The delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa. This can be done by using either static or dynamic mapping.
- IP is used for logical addressing
- MAC is used for physical addressing in a local network such as Ethernet

# Mapping Logical to Physical Address: ARP

- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
- The logical (IP) address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router.
- But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver. The host or the router sends an ARP query packet.
- The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network


Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B

a. ARP request is broadcast



b. ARP reply is unicast

# Mapping Physical to Logical Address: RARP

- There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.
2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.

- Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.
- The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol. A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply.

# ICMP

- The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.
- PING and TRACEROUTE are two tools for ICMP