MODULE 4

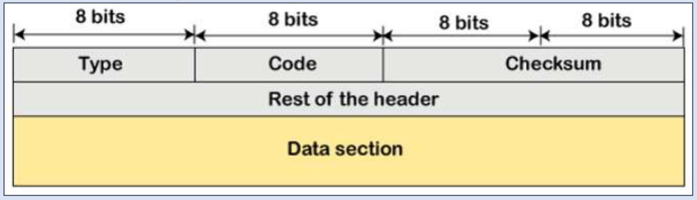
NETWORK LAYER IN THE INTERNET

Internet Control Message Protocol (ICMP)

- IP does not have an inbuilt mechanism for sending error and control messages.
- It depends on Internet Control Message Protocol(ICMP) to provide an error control.
- It is used for reporting errors and management queries.
- It is a supporting protocol and is used by networks devices like routers for sending error messages and operations information., e.g. the requested service is not available or that a host or router could not be reached.

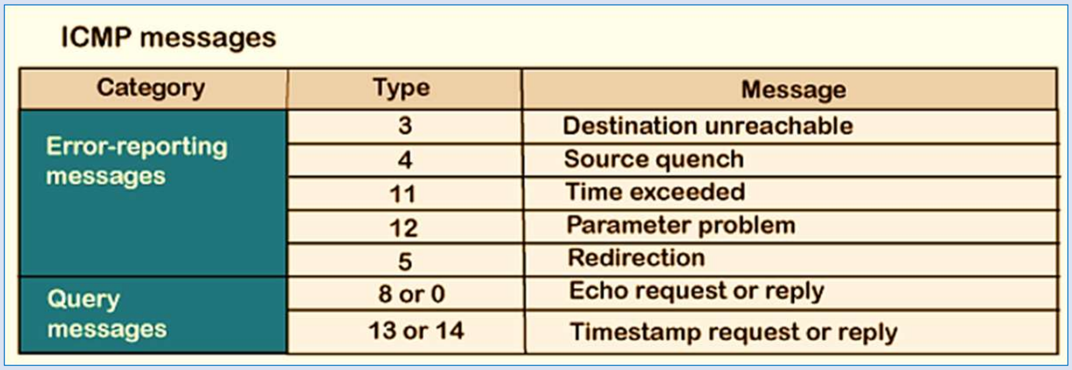
- The ICMP resides in the IP layer

❖ICMP Message Format



- **Type:** It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.
- **Code:** It is an 8-bit field that defines the subtype of the ICMP message
- **Checksum:** It is a 16-bit field to detect whether the error exists in the message or not.

- The ICMP protocol always reports the error messages to the original source. For example, when the sender sends the message, if any error occurs in the message then the router reports to the sender rather than the receiver as the sender is sending the message.

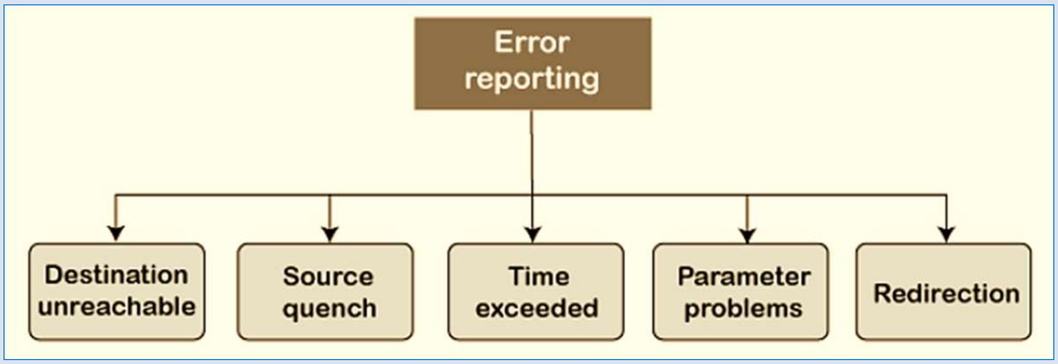


ICMP messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

❖Types of Error Reporting messages

- The error reporting messages are broadly classified into the following categories:



Error reporting

Destination unreachable

Source quench

Time exceeded

Parameter problems

Redirection

1. Destination unreachable

- The destination unreachable error occurs when the packet does not reach the destination. Suppose the sender sends the message, but the message does not reach the destination, then the intermediate router reports to the sender that the destination is unreachable.

2. Source quench message

- Source quench message is a request to decrease the traffic rate for messages sending to the host(destination). Or we can say when receiving host detects that the rate of sending packets (traffic rate) to it is too fast it sends the source quench message to the source to slow down so that no packet can be lost.

- ICMP will take the source IP from the discarded packet and informs the source by sending a source quench message. Then source will reduce the speed of transmission so that router will be free from congestion.
- When the congestion router is far away from the source the ICMP will send hop by hop source quench message so that every router will reduce the speed of transmission.

3. Parameter problem

- Whenever packets come to the router then the calculated header checksum should be equal to the received header checksum then the only the packet is accepted by the router.

- If there is a mismatch, packet will be dropped by the router. ICMP will take the source IP from the discarded packet and informs to the source by sending a parameter problem message.

4. Time exceeded

- Sometimes the situation arises when there are many routers that exist between the sender and the receiver. When the sender sends the packet, then it moves in a routing loop. The time exceeded is based on the time-to-live (TTL) value.
- When the packet traverses through the router, then each router decreases the value of TTL by one. Whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to the original source.

- Each of the MAC layers has different data units. For example, some layers can handle upto 1500 data units, and some can handle upto 300 units.
- When the packet is sent from a layer having 1500 units to the layer having 300 units, then the packet is divided into fragments; this process is known as fragmentation.
- These 1500 units are divided into 5 fragments, i.e., f1, f2, f3, f4, f5, and these fragments reach the destination in a sequence.
- If all the fragments are not reached to the destination in a set time, they discard all the received fragments and send a time-exceeded message to the original source.

5. Redirection

- When the packet is sent, then the routing table is gradually augmented and updated. The tool used to achieve this is the redirection message.
- For example, A wants to send the packet to B, and there are two routers exist between A and B. First, A sends the data to the router 1. The router 1 sends the IP packet to router 2 and redirection message to A so that A can update its routing table.

❖ICMP Query Messages

1. Echo-request and echo-reply message

- A router or a host can send an echo-request message. It is used to ping a message to another host that "Are you alive".
- If the other host is alive, then it sends the echo-reply message.
- An echo-reply message is sent by the router or the host that receives an echo-request message.

2. Timestamp-request and timestamp-reply message

- The timestamp-request and timestamp-reply messages are also a type of query messages.
- Suppose the computer A wants to know the time on computer B, so it sends the timestamp-request message to computer B.
- The computer B responds with a timestamp-reply message.

ADDRESS RESOLUTION PROTOCOL (ARP)

- Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address.
- This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.
- ARP relates an IP address with the physical address. On a typical physical network such as LAN, each device on a link is identified by a physical address, usually printed on the network interface card (NIC).
- A physical address can be changed easily when NIC on a particular machine fails.

- The IP Address cannot be changed. ARP can find the physical address of the node when its internet address is known. ARP provides a dynamic mapping from an IP address to the corresponding hardware address.
- When one host wants to communicate with another host on the network, it needs to resolve the IP address of each host to the host's hardware address.

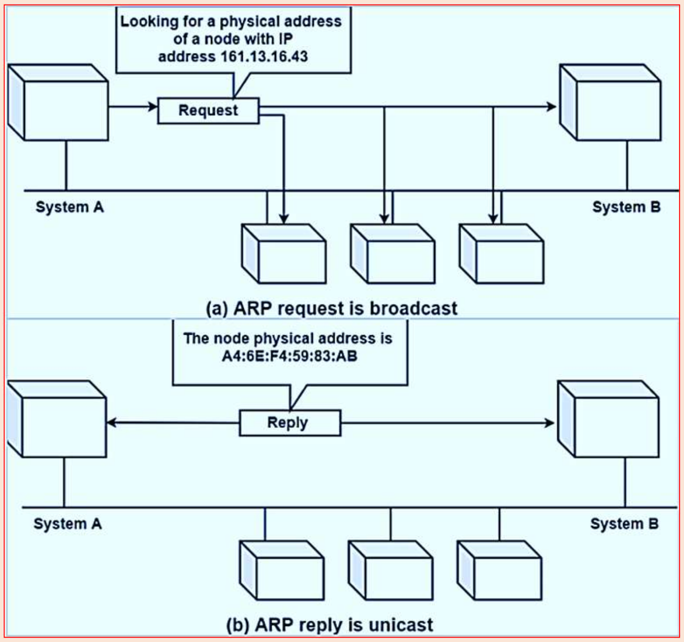
❖WORKING OF ARP

1. When a host tries to interact with another host, an ARP request is initiated. If the IP address is for the local network, the source host checks its ARP cache to find out the hardware address of the destination computer.

2. If the correspondence hardware address is not found, ARP broadcasts the request to all the local hosts.
3. All hosts receive the broadcast and check their own IP address. If no match is discovered, the request is ignored.
4. The destination host that finds the matching IP address sends an ARP reply to the source host along with its hardware address, thus establishing the communication.
5. The ARP cache is then updated with the hardware address of the destination host.

❖Important ARP terms

- **ARP Cache:** After resolving the MAC address, the ARP sends it to the cache stored in a table for future reference. The subsequent communications can use the MAC address from the table.
- **ARP Cache Timeout:** It is the time for which the MAC address in the ARP cache can reside.
- **ARP request:** Broadcasting a packet over the network to validate whether we came across the destination MAC address or not.
- **ARP response/reply:** The MAC address response that the source receives from the destination aids in further communication of the data.


Looking for a physical address of a node with IP address 161.13.16.43
Request
System A
System B
(a) ARP request is broadcast
The node physical address is A4:6E:F4:59:83:AB
Reply
System A
System B
(b) ARP reply is unicast

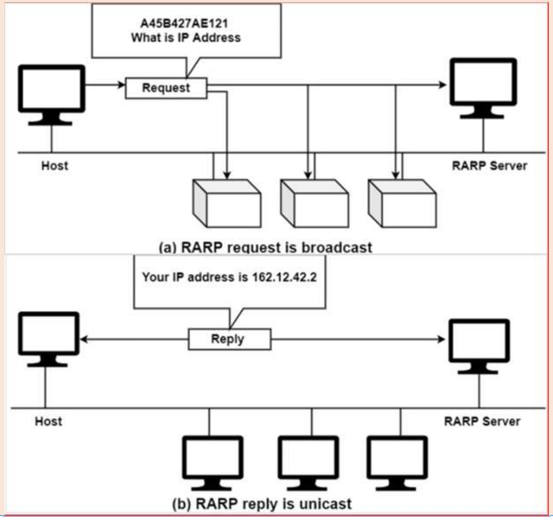
Reverse Address Resolution Protocol (RARP)

- Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol.
- Some network hosts, such as a diskless workstation, do not know their own IP address when they are booted.
- To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter, and the IP address is the queried parameter.
- The reverse address resolution is performed the same way as the ARP address resolution. The same packet format is used

❖**METHOD**

- **Source Device “Generates RARP Request Message”** – The source device generates a RARP Request message.
- **Source Device “Broadcasts RARP Request Message”** – The source broadcasts the RARP Request message on the local network.
- **Local Devices “Process RARP Request Message”** – The message is received by each device on the local network and processed. Devices that are not configured to act as RARP servers ignore the message.
- **RARP Server Generates RARP Reply Message -** Any device on the network that is a RARP server responds to the broadcast from the source device. It generates a RARP Reply
- **RARP Server Sends RARP Reply Message** - The RARP server sends the RARP Reply message unicast to the device looking to be configured.

- **Source Device Processes RARP Reply Message -** The source device processes the reply from the RARP server. It then configures itself using the IP address in the Target Protocol Address supplied by the RARP server.



(a) RARP request is broadcast

(b) RARP reply is unicast

BOOTSTRAP PROTOCOL (BOOTP)

- Bootstrap Protocol (BOOTP) is a networking protocol which is used by networking administration to give IP addresses to each member of that network for participating with other networking devices by the main server.
- BOOTP is used during the bootstrap process when the computer is initially starting up, hence the name.
- BOOTP was intended for diskless systems because they require such a protocol in order to contact a server to obtain a network address and some information on which operating system to use.

❖How does BOOTP Work

➢When a BOOTP client is started, it has no IP address, so it broadcasts a message containing its MAC address onto the network. This message is called a "**BOOTP request**," and it is picked up by the BOOTP server, which replies to the client with the following information that the client needs:

- The client's IP address, subnet mask, and default gateway address
- The IP address and host name of the BOOTP server
- The IP address of the server that has the boot image, which the client needs to load its operating system

- When the client receives this information from the BOOTP server, it configures and initializes its TCP/IP protocol stack, and then connects to the server on which the boot image is shared.
- The client loads the boot image and uses this information to load and start its operating system.

❖Important Features of Bootstrap Protocol

- Bootstrap Protocol (BOOTP) is a basic protocol that automatically provides each participant in a network connection with a unique IP address for identification and authentication as soon as it connects to the network. This helps the server to speed up data transfers and connection requests.

- BOOTP uses a unique IP address algorithm to provide each system on the network with a completely different IP address in a fraction of a second.
- This shortens the connection time between the server and the client. It starts the process of downloading and updating the source code even with very little information.
- BOOTP uses a combination of DHCP (Dynamic Host Configuration Protocol) and UDP (User Datagram Protocol) to request and receive requests from various network-connected participants and to handle their responses.

- In a BOOTP connection, the server and client just need an IP address and a gateway address to establish a successful connection.
- Typically, in a BOOTP network, the server and client share the same LAN, and the routers used in the network must support BOOTP bridging.
- A great example of a network with a TCP / IP configuration is the Bootstrap Protocol network.
- Whenever a computer on the network asks for a specific request to the server, BOOTP uses its unique IP address to quickly resolve them.

❖Uses of Bootstrap Protocol

- Bootstrap (BOOTP) is primarily required to check the system on a network the first time you start your computer. Records the BIOS cycle of each computer on the network to allow the computer's motherboard and network manager to efficiently organize the data transfer on the computer as soon as it boots up.
- BOOTP is mainly used in a diskless environment and requires no media as all data is stored in the network cloud for efficient use.
- BOOTP is the transfer of a data between a client and a server to send and receive requests and corresponding responses by the networking server.
- BOOTP supports the use of motherboards and network managers, so no external storage outside of the cloud network is required.

Dynamic Host Configuration Protocol (DHCP)

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so they can communicate using IP (Internet Protocol).
- DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.
- DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments).

❖DHCP does the following

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network.
- The server acknowledges by providing an IP address to the client/node/device.
- DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

- There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

❖How DHCP works

- DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.
- DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

❖Components of DHCP

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.

- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.

❖Advantages

- centralized management of IP addresses
- ease of adding new clients to a network
- reuse of IP addresses reducing the total number of IP addresses that are required
- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

Disadvantage - IP conflict can occur

Open Shortest Path First (OSPF) Protocol

- Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First.
- OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain.
- OSPF uses multicast address 224.0.0.5 for normal communication.
- It is an intradomain protocol, which means that it is used within an area or a network.

❖How does OSPF work

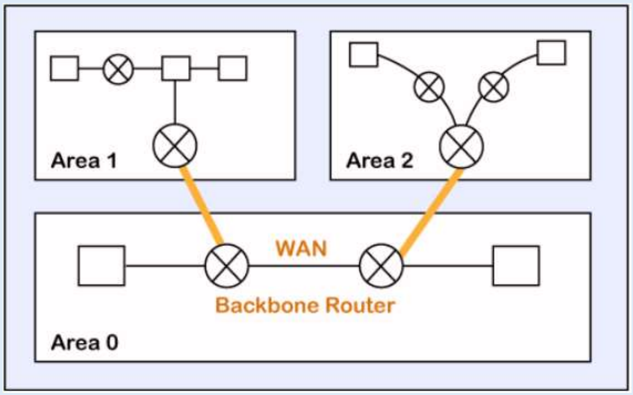
There are three steps that can explain the working of OSPF:

- **Step 1:** The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.
- **Step 2:** The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.
- **Step 3:** The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.

- OSPF divides the autonomous systems into areas where the area is a collection of networks, hosts, and routers.
- Routers that exist inside the area flood the area with routing information
- In Area, the special router also exists. The special routers are those that are present at the border of an area, and these special routers are known as **Area Border Routers.**
- This router summarizes the information about an area and shares the information with other areas.

- All the areas inside an autonomous system are connected to the backbone routers, and these backbone routers are part of a primary area.
- The role of a primary area is to provide communication between different areas.

OSPF Areas



- The OSPF relationship is a relationship formed between the routers so that they can know each other.
- The two routers can be neighbors if at least one of them is designated router or backup designated router in a network, or connected through a point-to-point link.

❖Types of links in OSPF

- A link is basically a connection, so the connection between two routers is known as a link.
- There are four types of links in OSPF
- **Point-to-point link:** The point-to-point link directly connects the two routers without any host or router in between.

- **Transient link:** When several routers are attached in a network, they are known as a transient link.
- The transient link has two different implementations:

Unrealistic topology: When all the routers are connected to each other, it is known as an unrealistic topology.

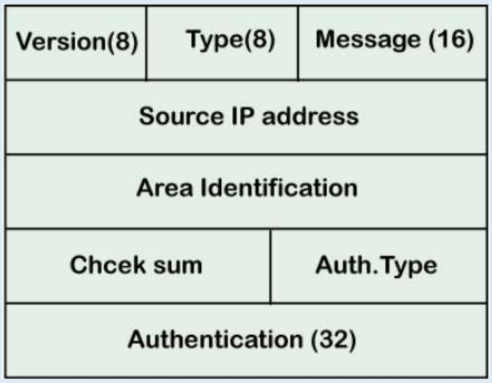
Realistic topology: When some designated router exists in a network then it is known as a realistic topology. Here designated router is a router to which all the routers are connected. All the packets sent by the routers will be passed through the designated router.

- **Stub link:** It is a network that is connected to the single router. Data enters to the network through the single router and leaves the network through the same router.

- **Virtual link:** If the link between the two routers is broken, the administration creates the virtual path between the routers, and that path could be a long one also.

OSPF Message Format

- The following are the fields in an OSPF message format:



Version(8)	Type(8)	Message (16)
Source IP address		
Area Identification		
Chcek sum		Auth.Type
Authentication (32)		

- **Version:** It is an 8-bit field that specifies the OSPF protocol version.
- **Type:** It is an 8-bit field. It specifies the type of the OSPF packet.
- **Message:** It is a 16-bit field that defines the total length of the message, including the header. Therefore, the total length is equal to the sum of the length of the message and header.
- **Source IP address:** It defines the address from which the packets are sent. It is a sending routing IP address.
- **Area identification:** It defines the area within which the routing takes place.
- **Checksum:** It is used for error correction and error detection.

- **Authentication type:** There are two types of authentication, i.e., 0 and 1. Here, 0 means for none that specifies no authentication is available and 1 means for pwd that specifies the password-based authentication.
- **Authentication:** It is a 32-bit field that contains the actual value of the authentication data.

IPv4 ADDRESSES

- An **IPv4** address is a 32-bit address that *uniquely* and *universally* defines the connection of a device (for example, a computer or a router) to the Internet
- Two devices on the Internet can never have the same address at the same time.
- IPv4 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.

- 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, more than 4 billion devices could be connected to the Internet.
- There are two prevalent notations to show an IPv4 address: binary notation and dotted decimal notation.

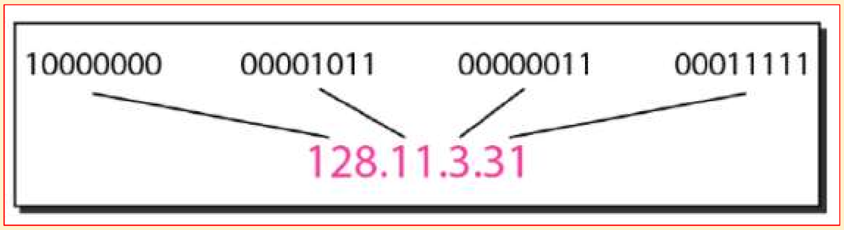
❖Binary Notation

- In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte.

Eg: **01110101 10010101 00011101 00000010**

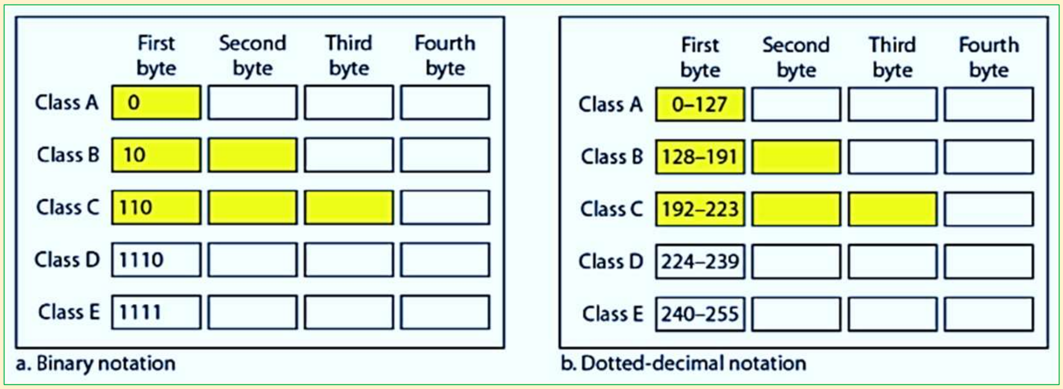
❖Dotted-Decimal Notation

- To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes.
- Eg: **117.149.29.2**
- Each number in dotted-decimal notation is a value ranging from 0 to 255



❖Classful Addressing

- IPv4 addressing used the concept of classes.
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.
- If the address is given in binary notation, the first few bits can immediately tell us the class of the address.
- If the address is given in decimal-dotted notation, the first byte defines the class



	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

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

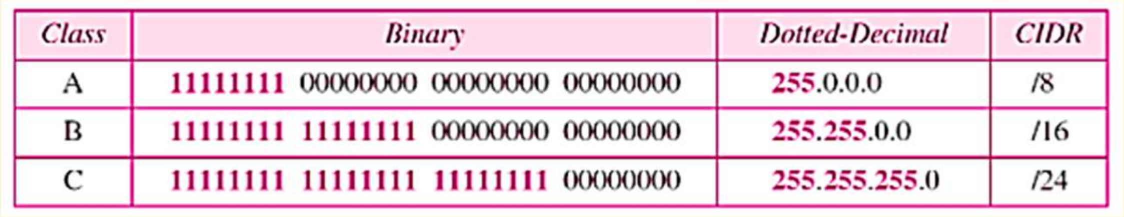
c. 14.23.120.8

d. 252.5.15.111

- In classful addressing, a large part of the available addresses were wasted.
- In classful addressing, an IP address in class A, B, or C is divided into **netid** and **hostid.** These parts are of varying lengths, depending on the class of the address.
- The above figure shows some netid and hostid bytes. The netid is in color, the hostid is in white.
- Note that the concept does not apply to classes D and E.
- In class A, one byte defines the netid and three bytes define the hostid. In class B, two bytes define the netid and two bytes define the hostid. In class C, three bytes definethe netid and one byte defines the hostid.

❖*Mask*

- The mask can help us to find the netid and the hostid.
- For example, the mask for a class A address has eight 1s, which means the first 8 bits of any address in class A define the netid; the next 24 bits define the hostid.
- A 32-bit number made of contiguous 1s followed by contiguous 0
- The concept does not apply to classes D and E



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