INTRODUCTION TO INTERNET AND WEB TECHNOLOGY

Prepared by
Smt Reetanjali Panda
Lecturer(CA),UCPES

Introduction to Internetworking

- **The Motivation For Internetworking:** The technology, called internetworking, accommodates multiple, diverse underlying hardware technologies by providing a way to interconnect heterogeneous networks and a set of communication conventions that makes them interoperate. The internet technology hides the details of network hardware, and permits computers to communicate independent of their physical network connections. It is called open because anyone can build the software needed to communicate across an internet. The entire technology has been designed to foster communication among machines with diverse hardware architectures, to use almost any packet switched network hardware, to accommodate a wide variety of applications, and to accommodate multiple computer operating systems.

Introduction to Internetworking(Cont.)

- **Internet Evoloution**
- The concept of Internet was originated in 1969 and has undergone several technological &Infrastructural changes as discussed below:
- The origin of Internet devised from the concept of **Advanced Research Project Agency Network *ARPANET*.**
- **ARPANET** was developed by United States Department of Defence.
- Basic purpose of ARPANET was to provide communication among the various bodies of government.
- Initially, there were only four nodes, formally called **Hosts.**
- In 1972, the **ARPANET** spread over the globe with 23 nodes located at different countries and thus became known as **Internet.**

Introduction to Internetworking(Cont.)

- **The Internet Architecture Board(IAB):** The ARPA technology includes a set of network standards that specify the details of how computers communicate, as well as a set of conventions for interconnecting networks and routing traffic,referred to as TCP/IP , can be used to communicate across any set of interconnected networks. The IAB provides the focus and coordination for much of the research and development underlying the TCP/IP protocols, and guides the evolution of the Internet. It decides which protocols are a required part of the TCP/IP suite and sets official policies.
- **Internet Protocols And Standardization:**
- *Use existing protocol standards whenever such standards apply; invent new protocols only when existing standards are insufficient, and be prepared to use new standards when they become available and provide equivalent functionalities.*

Introduction to Internetworking(Cont.)

- **Properties Of The Internet:** Internet must enable us to send data across intermediate networks even though they are not directly connected to the source or destination computers. All the computers in the internet must share a universal set of machine identifiers. Our notion of a unified internet also includes the idea of network independence in the user interface. That is, the set of operations used to establish communication or to transfer data must remain independent of the underlying network technologies and the destination computer. Certainly, a user should not have to understand the network interconnection topology when creating or using application programs to communicate.

Introduction to Internetworking(Cont.)

- **Internet Architecture**: To have a viable internet, we need special computers that can transfer packets from one network to another. Computers that interconnect two networks and pass packets from one to the other are called internet gateways or internet routers.
- **Interconnection Through IP Router:** In a TCP/IP internet, special computers called IP routers or IP gateways provide interconnections among physical networks.
- Routers use the **destination network**, not the destination computer, when forwarding a packet.

Internet Advantages

- **Internet Advantages**
- Internet covers almost every aspect of life, one can think of.

Advantages of Internet:

- **Communication tool:** Data, voice, video can be instantly exchanged thanks to high-speed networks.
- **Teaching aid:** Many complex concepts were easily explained using graphics. Wealth of knowledge. Business tool: E-commerce has totally changed the way we were doing business
- **Information tool:** Ocean full of information on any particular topic thanks to the powerful search engines. E-governance: Many government organisations already started using for collection of revenue, tax and so on; Imagine earlier- even to pay electricity bill it was total one day's job sometimes!

Disadvantages of Internet

- **Travel:** Internet is useful for advance reservation, tour planning and so on.
- **Medical & health**: A specialist doctor's services can be availed over net

Disadvantages of Internet:

- Threat to personal information
- Virus attack
- Spamming
- Cybercrime

Safeguards

- **Protect yourself from security issues:** Keep your computer's operating system updated. For example, if you are using Microsoft Windows, visit windowsupdate.microsoft.com and follow the instructions. You can also keep the automatic update feature of your computer turned on so that security updates are downloaded automatically.
- **Install or use Spam protection:** Visit the Web site of your Internet Service Provider (the one who gives you Internet connection) and look for information they have about preventing spam and viruses from reaching your email.

Safeguards(Cont.)

- **Enable popup blocking features of your Web browser** (see the Help section of your Web browser) or install popup blocking software: Pop ups can be annoying and can also lure you into scams or other problems. Your Internet Service provider may also have special assistance or software for you to use to block popup windows.
- **Enable cookie protection in your Web browser**: (Cookie is a piece of information that is automatically conversed with webserver whenever someone visits a web site. Some times it may carry very sensitive information about your system!) You shouldn't be afraid of cookies—they are useful for many ways but consider accepting cookies from only known, trusted Web sites.

Safeguards(Cont.)

- **Protect yourself from potential loss of data** and create backup copies of your data regularly: If your computer crashes or if there is a fire or flood in your home, you don't want to lose important personal information. Copy information you don't want to lose onto a disk and store the disk in a secure place away from your computer. Be sure to password protect the disk if it contains sensitive information or keep the disk in a safe place.

Extranet

- **Extranet**
- Extranet refers to network within an organization, using internet to connect to the outsiders in a controlled manner. It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner.

Intranet

- An **intranet** is a private computer network within an enterprise that is used to securely share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and teleconferences.
- Intranets increase communication within an organization by allowing employees to easily access important information, links, applications and forms as well as databases that can provide company records.

Uses of the intranet

- Centralizing and managing important information and company data in a single database.
- Making collaboration easier since information can be shared across the entire network.
- Providing personalized content to employees based on their role within the company.
- Improving internal communication by making employee directories, company news and organization charts readily available.
- Providing fast and easy access to information about company policies, benefits and updates.

How the intranet works

- A secure and reliable intranet requires a web server that is responsible for managing all requests for the files hosted on the server, finding the requested file and delivering it to the appropriate computer. A content management system (CMS) should also be set up to control the creation, publication and management of content on the intranet.
- An intranet may also consist of many interlinked local area networks (LANs) as well as Wide Area Network (WAN). It uses TCP/IP, HTTP and other Internet protocols . Typically, an intranet includes connections through one or more gateway computers to the outside .
- An employee who wants to access the intranet must have a special network password and be connected to the LAN. However, an employee working remotely can gain access to the intranet through a virtual private network (VPN). The VPN allows users who are not actually connected to the required LAN to sign into the intranet and access all the informations and functions that would be available had they been connected to the LAN.

How the intranet works (CONT.)

- Firewall software is essential to the security of an organization's intranet; it stands between the outside Internet and the private intranet. The firewall will monitor all incoming and outgoing data packets to confirm they do not contain unauthorized or suspicious requests, ensuring malware and other malicious attacks do not leak into the intranet. When a segment of an intranet is made accessible to the customers, partners, suppliers, or others outside the company, that segment becomes part of an Extranet. The firewall is especially important for intranet networks that include Extranet extensions.
- The intranet generally looks like a private version of the Internet. With tunneling, companies can send private messages through the public network while using special encryption/decryption and other security safeguards to connect one part of their intranet to another.

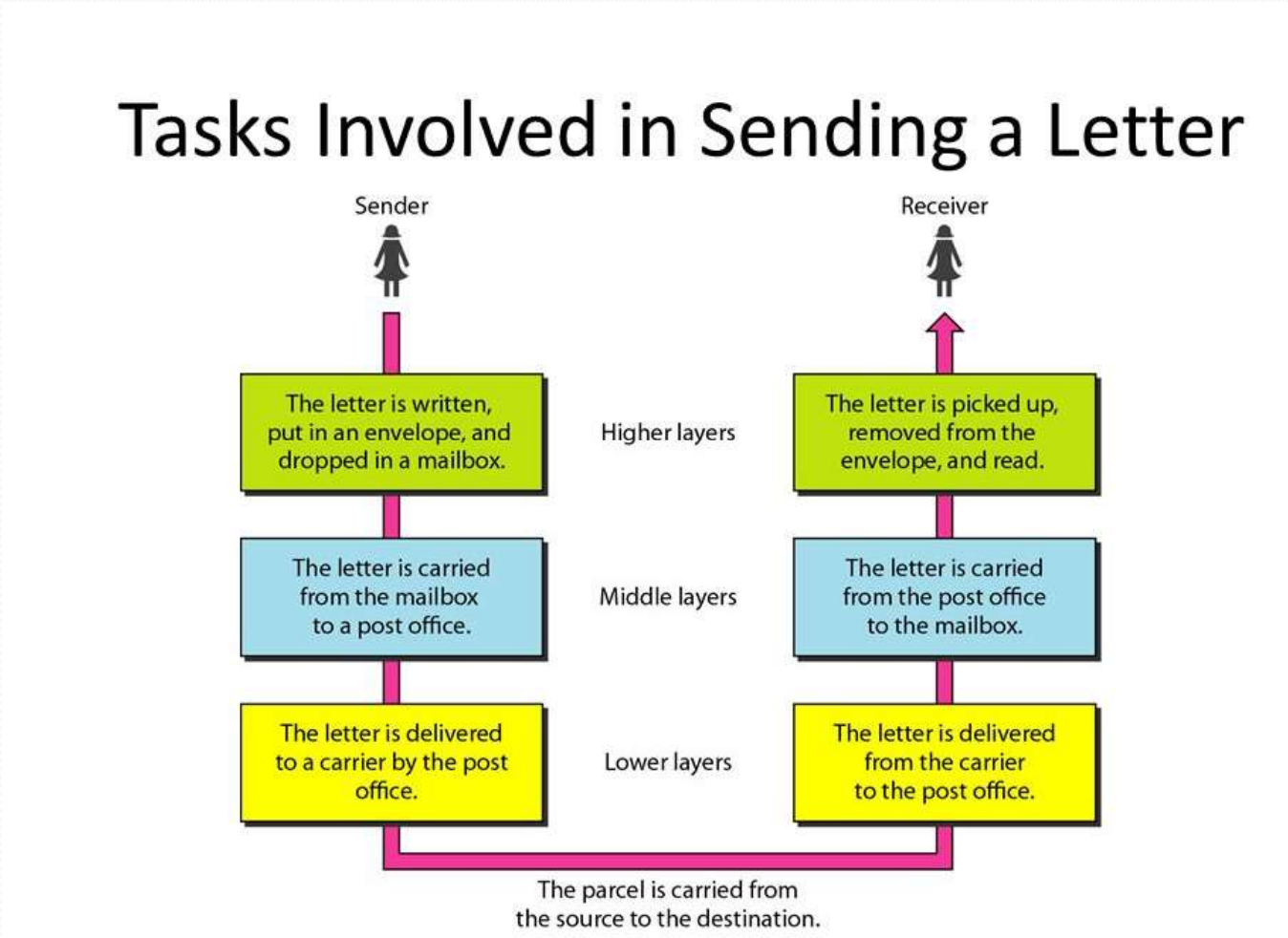
Difference between Extranet and Intranet

Extranet	Intranet
Internal network that can be accessed externally.	Internal network that can not be accessed externally.
Extranet is extension of company's Intranet.	Only limited users of a company.
For limited external communication between customers, suppliers and business partners.	Only for communication within a company.

TCP/IP

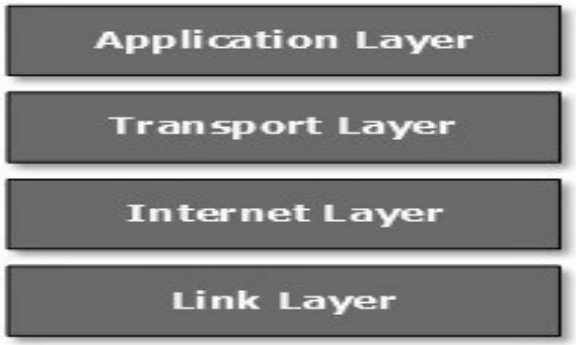
- **TCP/IP**
- Network engineering is a complicated task, which involves software, firmware, chip level engineering, hardware, and electric pulses. To ease network engineering, the whole networking concept is divided into multiple layers. Each layer is involved in some particular task and is independent of all other layers. But as a whole, almost all networking tasks depend on all of these layers. Layers share data between them and they depend on each other only to take input and send output.
- **Layered Tasks**
- The total task is divided in to small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.
- In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the topmost layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to layer below it.

Layered Tasks

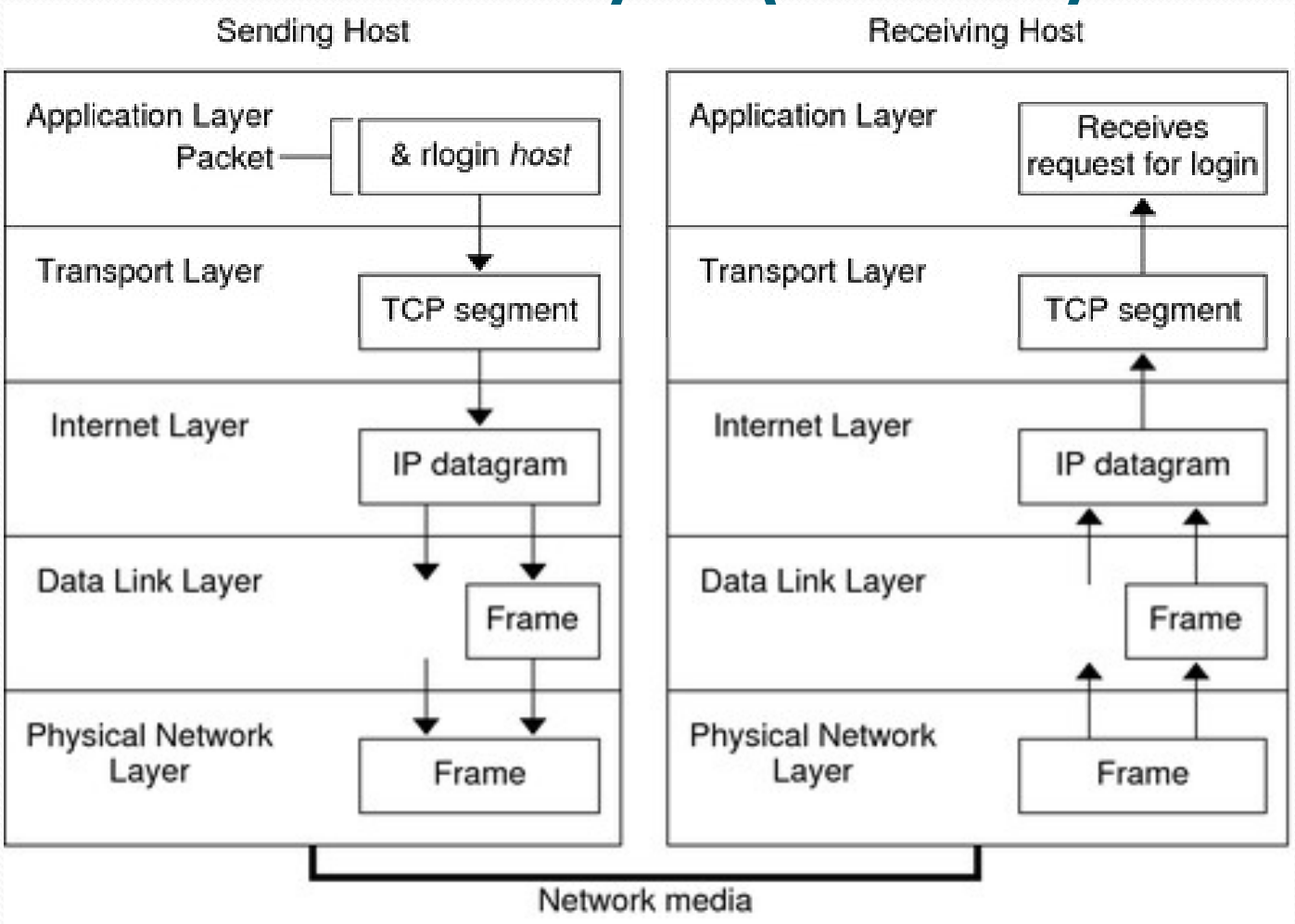


TCP/IP(Cont.)

- Every layer clubs together all procedures, protocols, and methods which it requires to execute its piece of task. All layers identify their counterparts by means of encapsulation header and trailor. Each layer gets service from the layer below it and provides services to the layer above it through interfaces.
- **Internet Model:** Internet uses TCP/IP protocol suite, also known as Internet suite. This defines Internet Model which contains four layered architecture. OSI Model is general communication model but Internet Model is what the internet uses for all its communication. The internet is independent of its underlying network architecture so is its Model. This model has the following layers:



TCP/IP(Cont.)


Sending Host
Receiving Host
Application Layer
Packet
& rlogin host
Application Layer
Receives request for login
Transport Layer
TCP segment
Transport Layer
TCP segment
Internet Layer
IP datagram
Internet Layer
IP datagram
Data Link Layer
Frame
Data Link Layer
Frame
Physical Network Layer
Frame
Physical Network Layer
Frame
Network media

TCP/IP(Cont.)

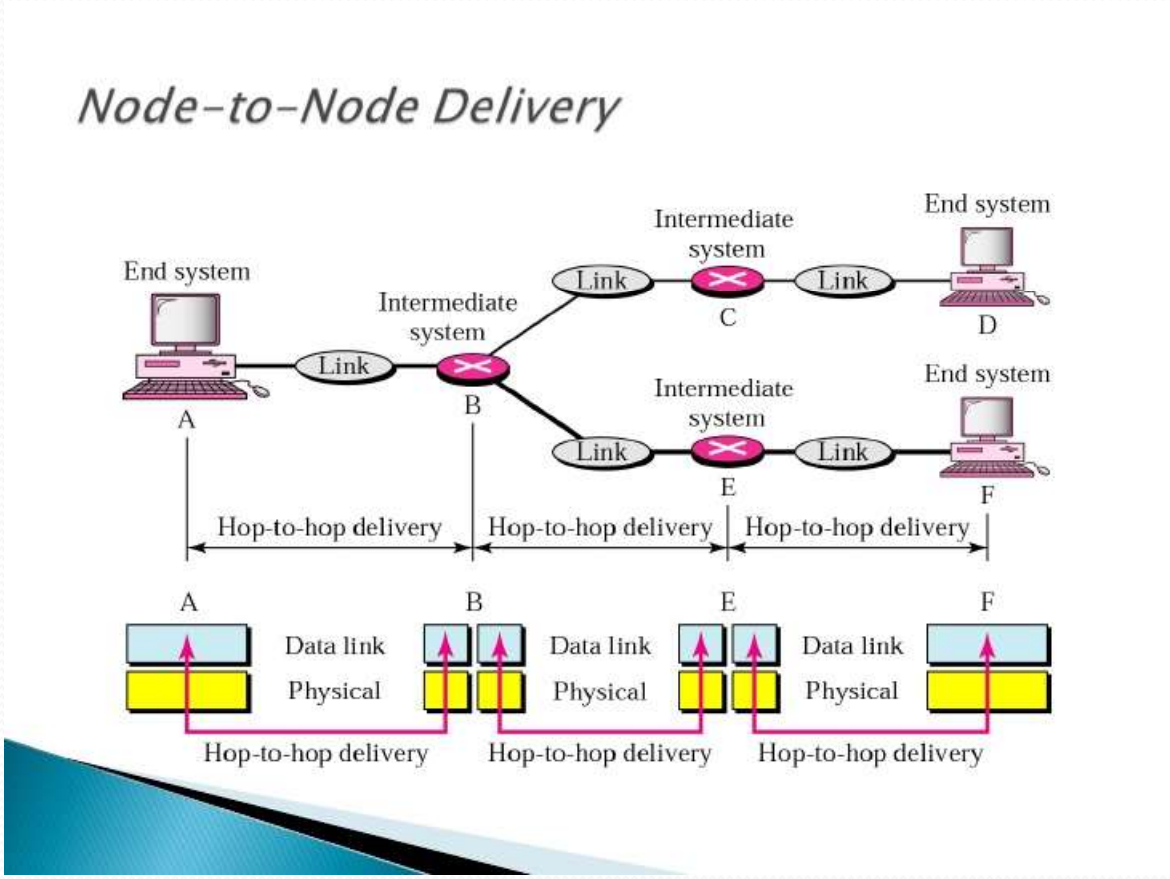
- **Application Layer:** This layer defines the protocol which enables user to interact with the network. The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services. It is responsible for providing various services to the users like : Mail services, File transfer and access, Remote log in and accessing the World Wide Web.

- **Transport Layer:** This layer defines how data should flow between hosts. Major protocol at this layer is Transmission Control Protocol (TCP) and User Datagram Protocol(UDP). The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. The various responsibilities of transport layer are port addressing, segmentation and reassembly, connection control, flow control and error control .

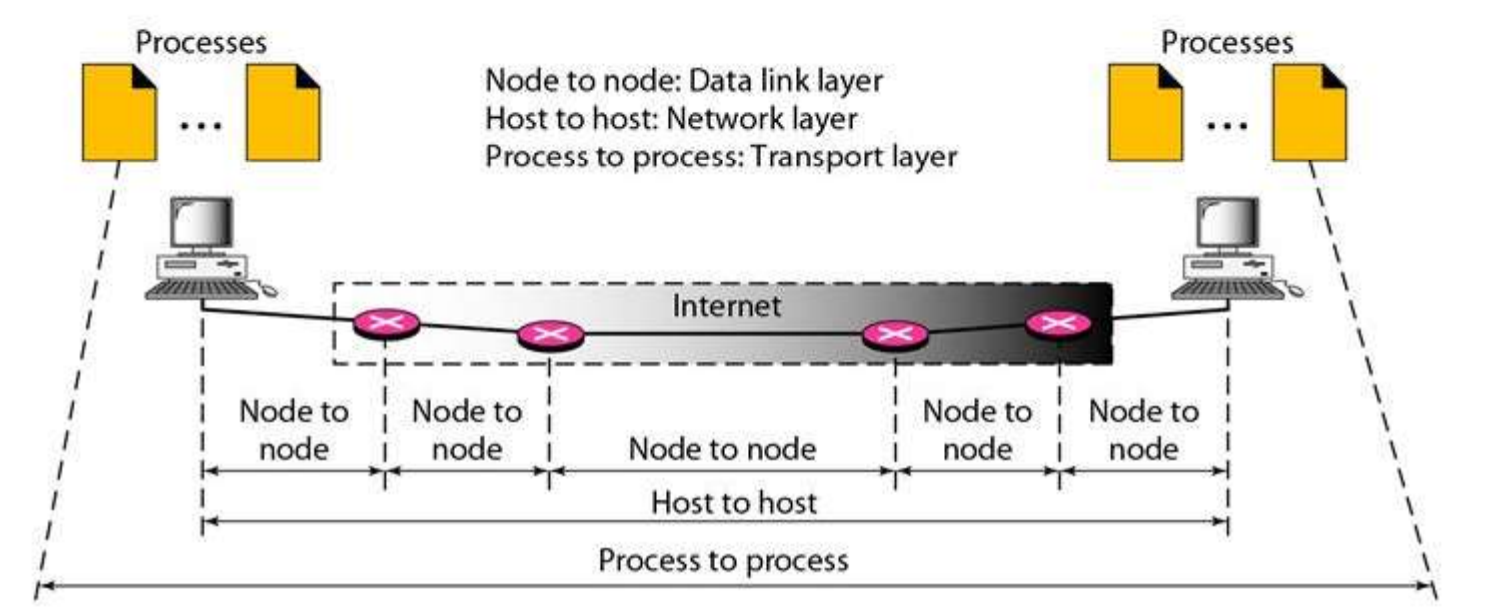
TCP/IP(Cont.)

- **Internet Layer:** Internet Protocol (IP) works on this layer. This layer facilitates host addressing and recognition. This layer defines routing and is responsible for end- to-end delivery. The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. The various responsibilities of Internet layer are Logical Addressing and Routing.
- **Link Layer:** This layer provides mechanism of sending and receiving actual data. Unlike its OSI Model counterpart, this layer is independent of underlying network architecture and hardware. At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols.The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium

TCP/IP(Cont.)


Node-to-Node Delivery
End system
Intermediate system
End system
Link
Link
Link
Intermediate system
C
D
End system
Intermediate system
Link
B
A
Link
Link
E
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
A
B
E
F
Data link
Data link
Data link
Physical
Physical
Physical
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery

TCP/IP(Cont.)


Processes
Processes
Node to node: Data link layer
Host to host: Network layer
Process to process: Transport layer
Internet
Node to node
Node to node
Node to node
Node to node
Node to node
Host to host
Process to process

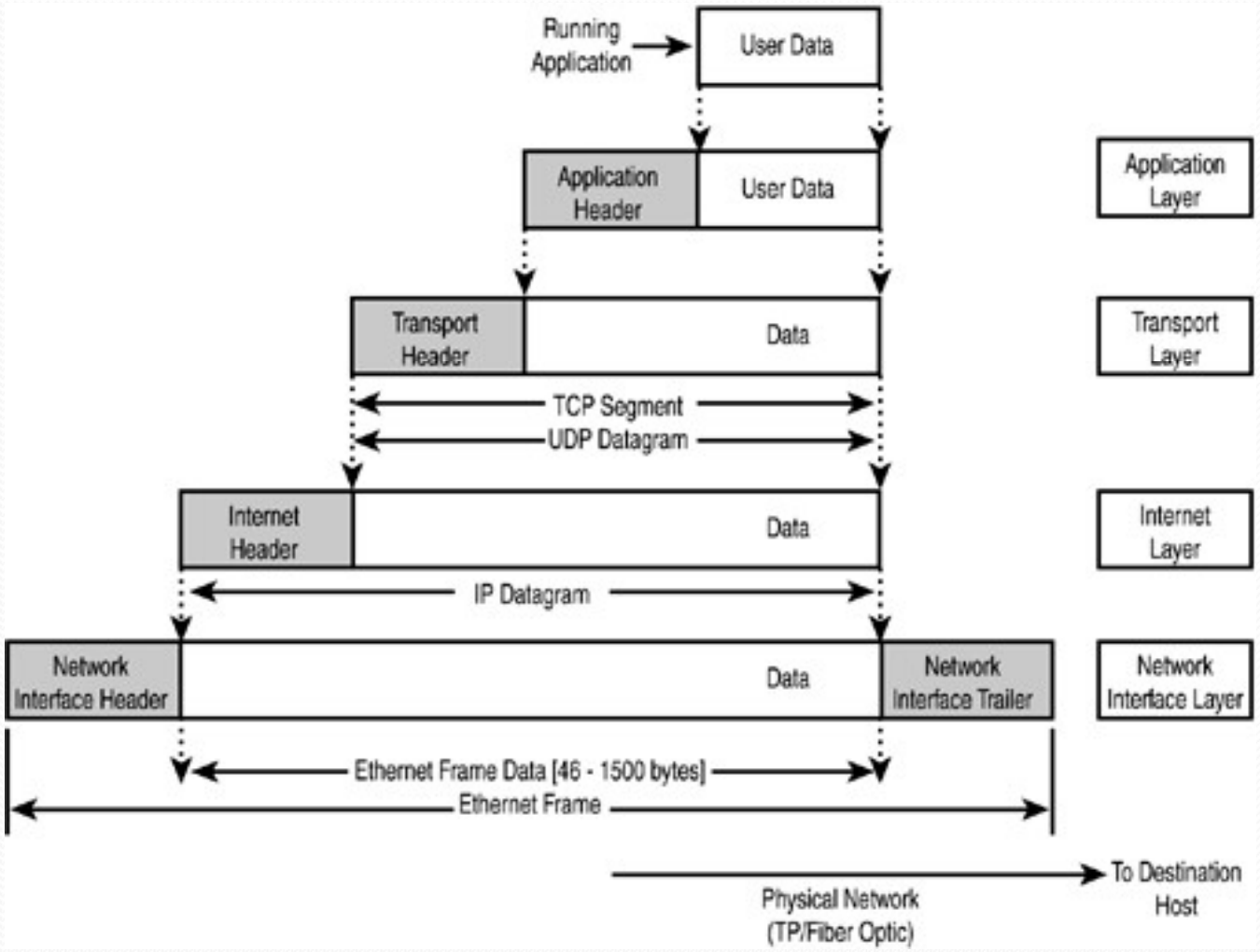
TCP/IP(Cont.)

- It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. The physical layer is responsible for movements of individual bits from one hop (node) to the next. The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). The datalink layer is responsible for moving frames from one hop (node) to the next. The various responsibilities of Datalink layer are : Framing, Physical addressing, Flow control, Error control and access control. The various responsibilities of physical layer are : Defining the physical characteristics of interfaces and media, Representation of bits, Data rate and Synchronization of bits.

Peer-to-Peer Communication

- Each layer actually communicates with its peer layer on another host, so the Application layer on a host sends a message to the Application layer on another host; the fact that the message passes through the Transport, Internet, and Network Interface layers on the local host (and the same layers on the other host) is transparent to the user . The Internet layer, for example, where the IP addresses are added, talks to only the Internet layer on another host.
- **Encapsulation**
- Each layer in the TCP/IP model communicates with its peer layer on another host. To do this, each layer must add some control information that will be understood by the receiving host, so that the message is dealt with correctly. This process of adding header information at each layer is known as *encapsulation* .

THE ENCAPSULATION PROCESS IN THE TCP/IP MODEL.



THE ENCAPSULATION PROCESS IN THE TCP/IP MODEL.

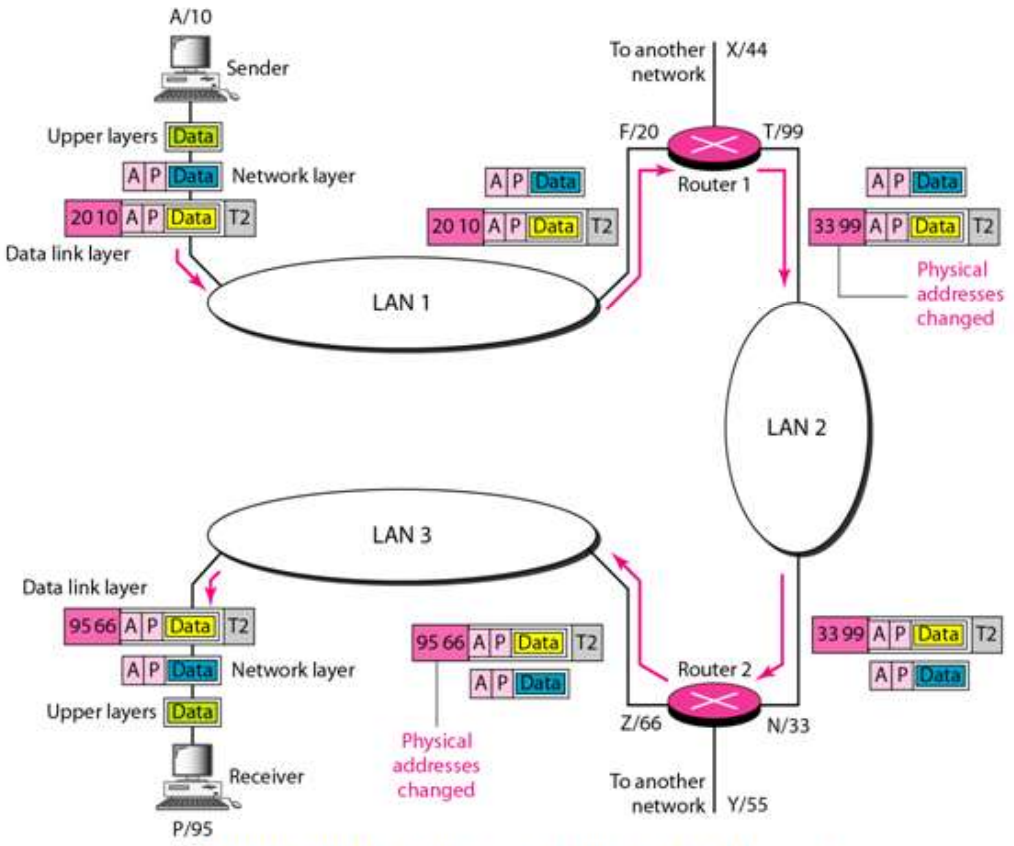
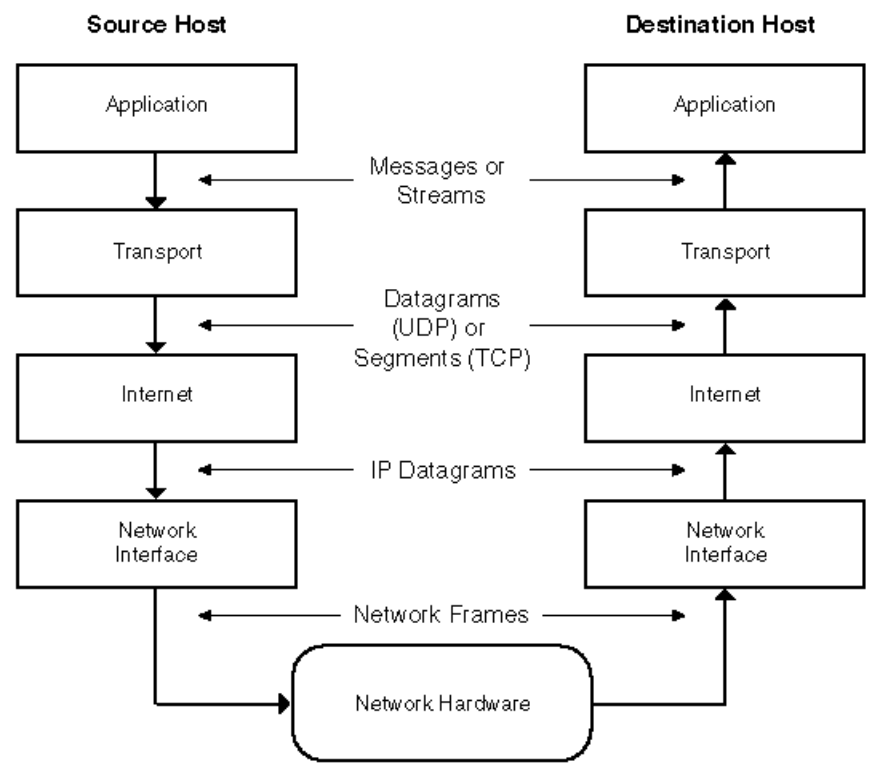


Figure 30: IP Addresses & Physical Addresses

Peer-to-Peer Communication(Cont.)

- Each protocol layer within the TCP/IP suite has various functions; these functions are independent of the other layers. Each layer, however, expects to receive specific services from the layer beneath it, and each layer provides specific services to the layer above it.
- The layers at the same level on the source and destination computers are *peers*. For example, the application on the source computer and the application on the destination computer are peers. Each layer of the protocol stack on the source computer communicates with its peer layer on the destination computer. From the perspective of the software developer or user, the transfer takes place as if the peer layers sent their packets directly to one another.

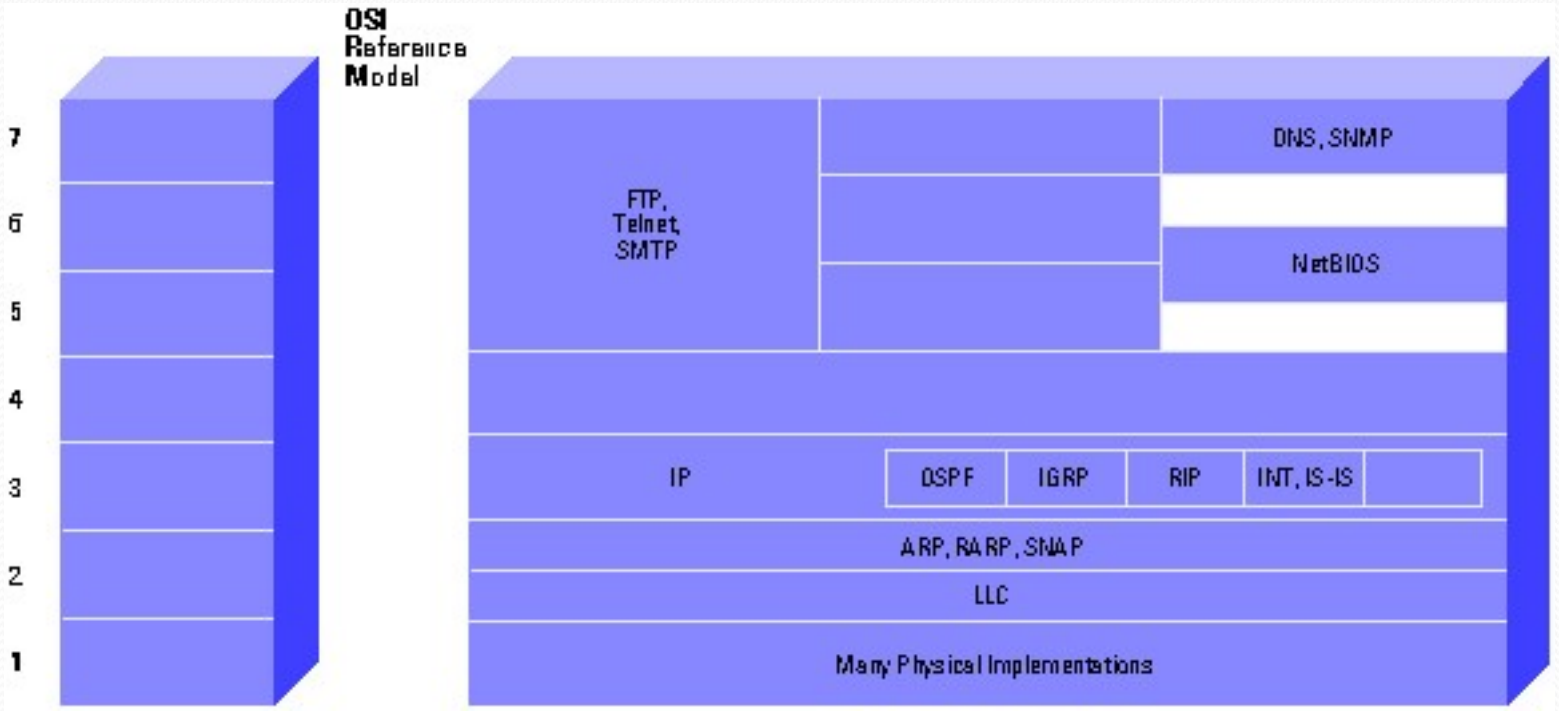
Peer-to-Peer Communication(Cont.)



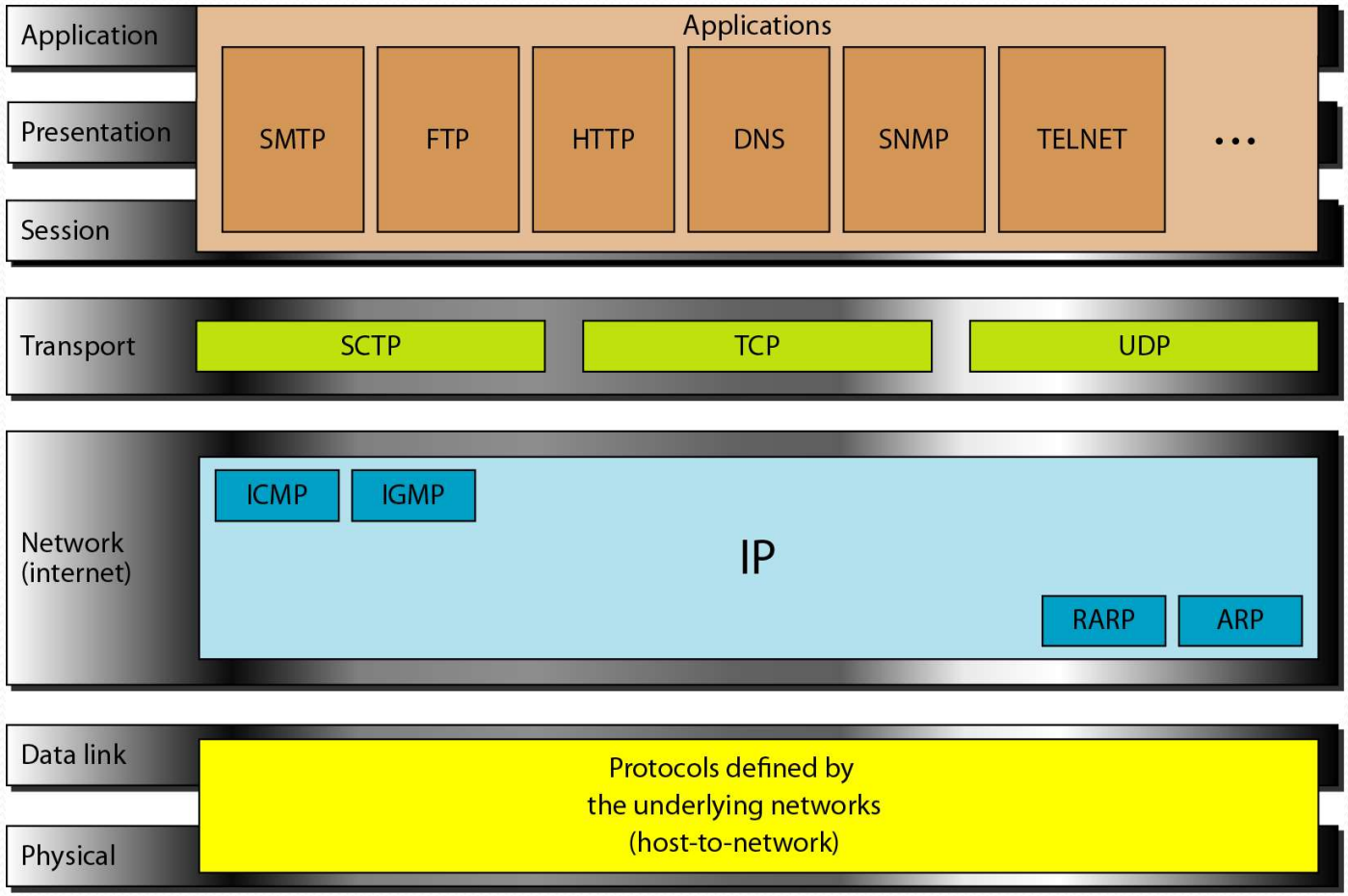
Advantages of using Layers

- **Networking technologies** are **separated** or compartmentalised into **layers**, **each one** containing specific *hardware* and *software* protocols.
- Each layer **performs specific tasks** and interacts with **adjacent layers** in the network model.
- **The advantages of this approach are:**
- It simplifies the overall model by dividing it into four parts.
- Each layer is specialised to perform a particular function.
- The different layers can be combined in different ways as required.
- One layer can be developed or changed without affecting the other layers.
- It makes it easier to identify and correct networking errors and problems.
- It provides a universal standard for hardware and software manufacturers to follow, so that they will be able to communicate with each other.

TCP/IP versus OSI



TCP/IP versus OSI(Cont.)



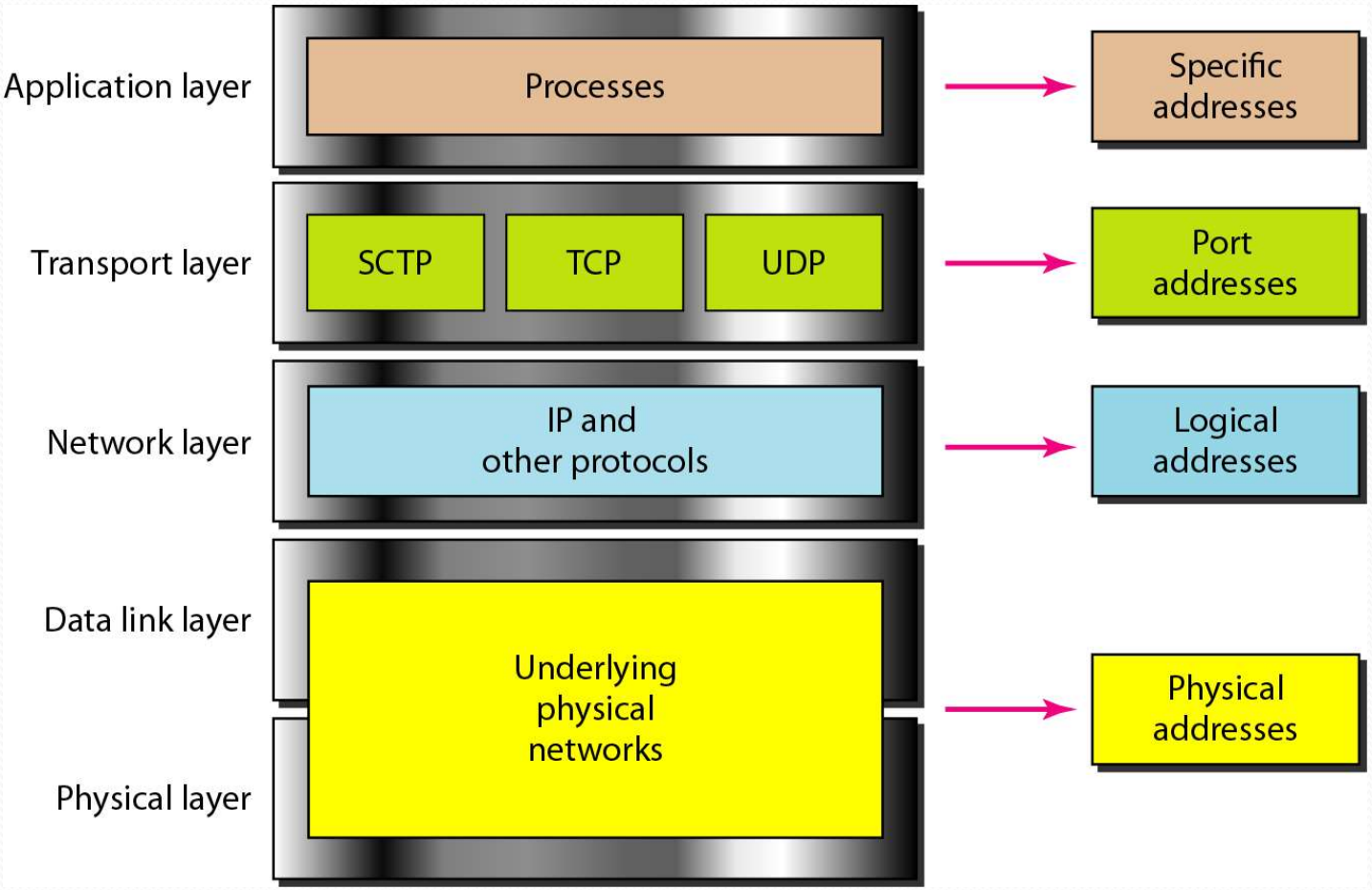
RELATIONSHIP OF LAYERS AND ADDRESSES IN TCP/IP

- **Physical Addresses**
- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. It is the lowest-level address. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal
- **Logical Addresses**
- Logical addresses are necessary for universal communications that are independent of underlying physical networks. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address. The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network).

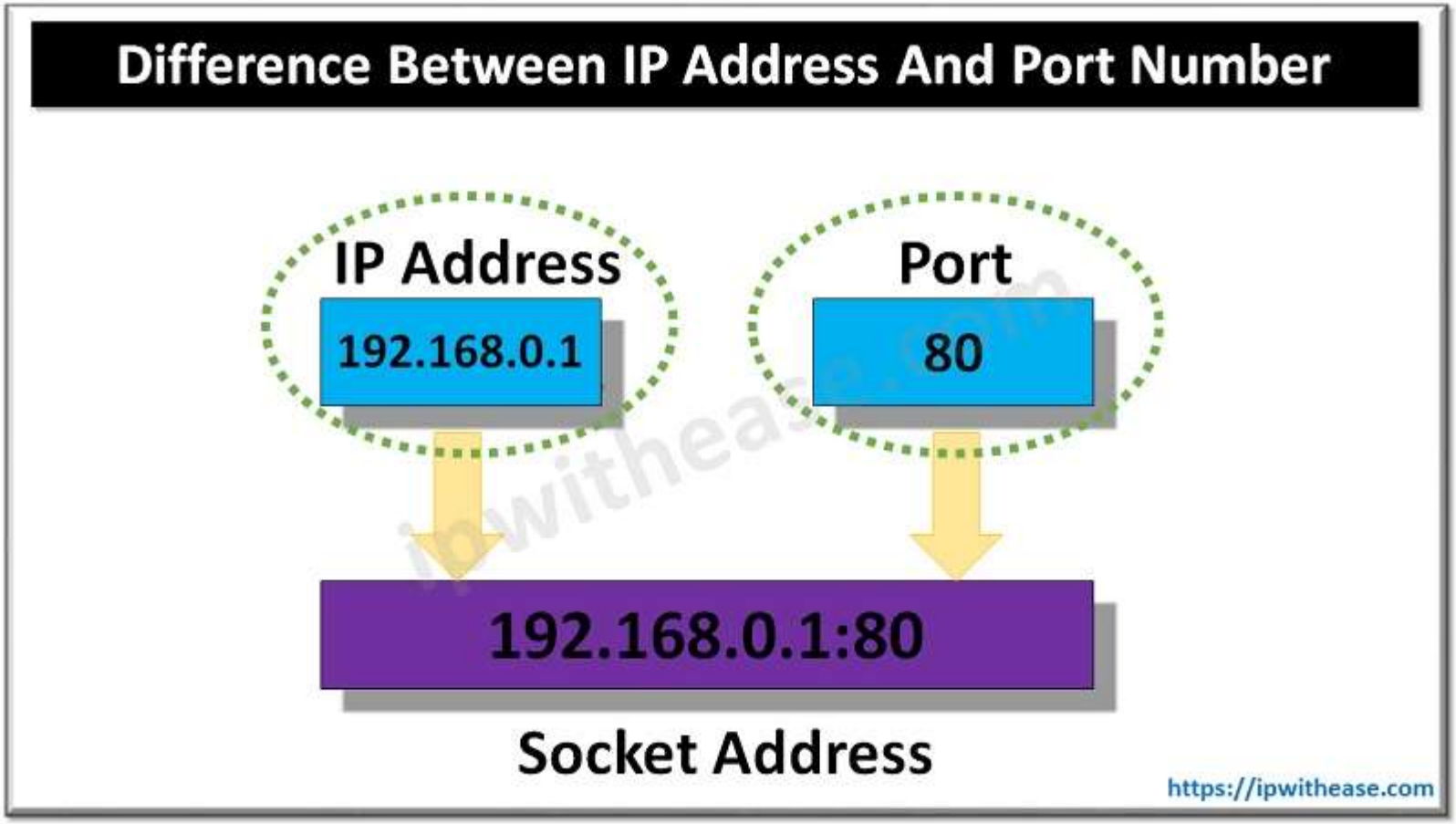
RELATIONSHIP OF LAYERS AND ADDRESSES IN TCP/IP(Cont.)

- **Port Addresses**
- computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process which is made possible using port addresses. Process-to-process delivery needs two identifiers, IP address and the port number, at each end to make a connection. The combination of an IP address and a port number is called a socket address. The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely.
- **Specific Addresses**
- Some applications have user-friendly addresses that are designed for that specific address. Examples include the e-mail address and the Universal Resource Locator (URL).

RELATIONSHIP OF LAYERS AND ADDRESSES IN TCP/IP(Cont.)



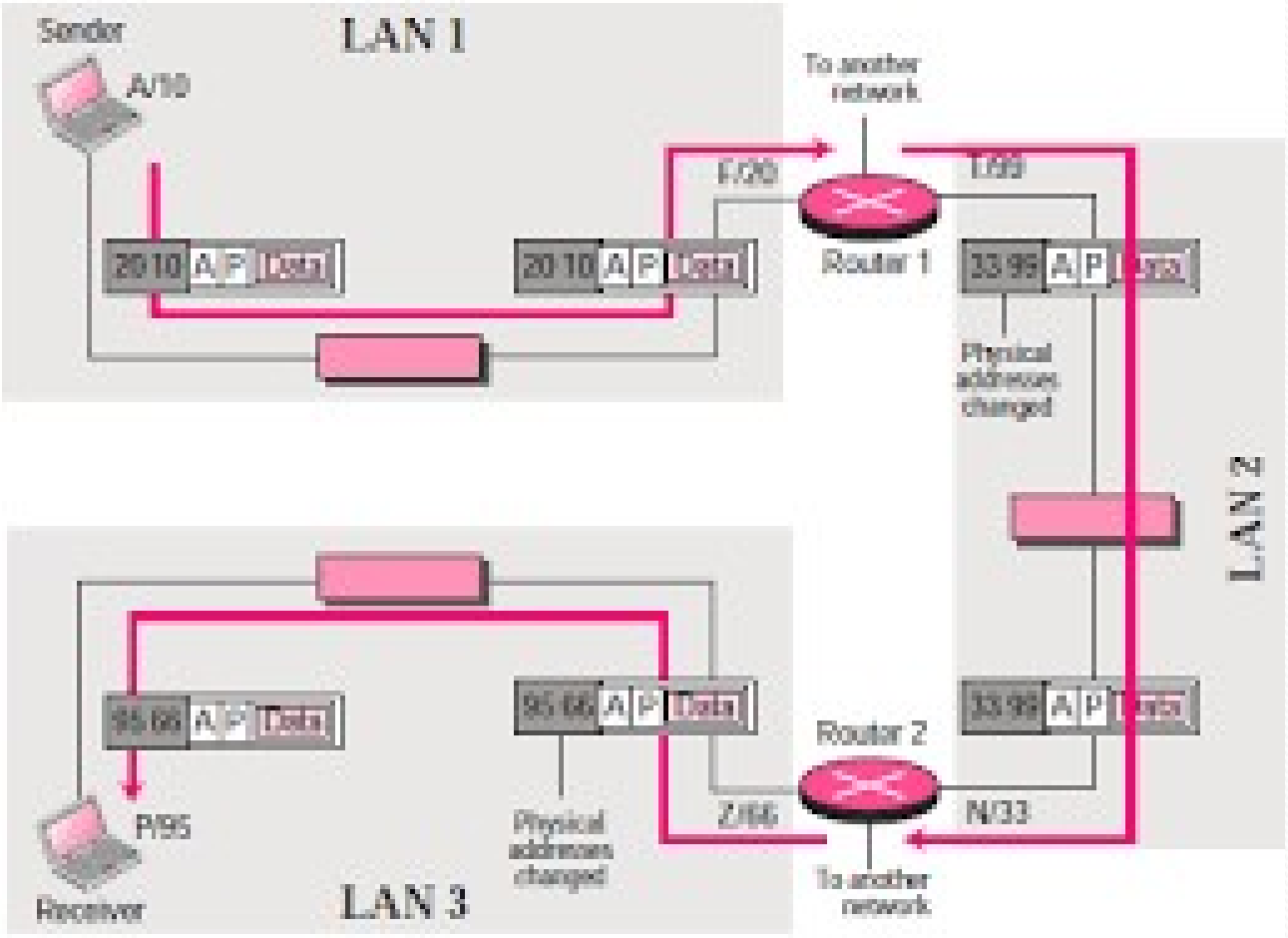
RELATIONSHIP OF LAYERS AND ADDRESSES IN TCP/IP(Cont.)



TCP/IP(Cont.)

Layer Name	Protocols in this Layer Cover	Protocol Examples
Layer 4 – Application Layer	This is where applications such as web browsers & email clients operate. It is also where requests are made to web servers or emails are originated by the applications. Requests are then passed on to the Transport Layer.	HTTP, HTTPS, FTP, SMTP, POP, SSH, IMAP
Layer 3 – Transport Layer	This is where the TCP protocol is active and is concerned with host-to-host communications. Language settings and packet size is agreed. Packets are also checked to confirm safe delivery via an acknowledgement. UDP is an alternative to TCP where packets are just sent without acknowledgement.	TCP, UDP
Layer 2 – Network Layer (also called Internet Layer)	This is where the IP protocol is active and adds the source & destination IP addresses to the packets & routes them to the recipient computer.	IP
Layer 1 – Data Link Layer (also called Network access layer)	This layer is concerned with the transmission of data through the local network using protocols of the specific network, for example Ethernet. This is where the network interface card (NIC) & the device drivers of the OS are located.	Ethernet, NIC, Wi-Fi

Logical address vs physical address



Logical address vs physical address(CONT.)

- The Figure shows a part of an internet with two routers connecting three LANs. The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95. The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). , the logical source address comes before the logical destination address (contrary to the order of physical addresses). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered.

Logical address vs physical address(CONT.)

- The network layer consults its routing table and finds the logical address of the next hop (router 1) to be F. Another protocol, Address Resolution Protocol (ARP) finds the physical address of router 1 that corresponds to its logical address (20). Now the network layer passes this address to the data link layer, which in turn, encapsulates the packet with physical destination address 20 and physical source address 10. The router 1 decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded. The router consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2. Note the physical addresses in the frame. The source physical address changes from 10

Logical address vs physical address(CONT.)

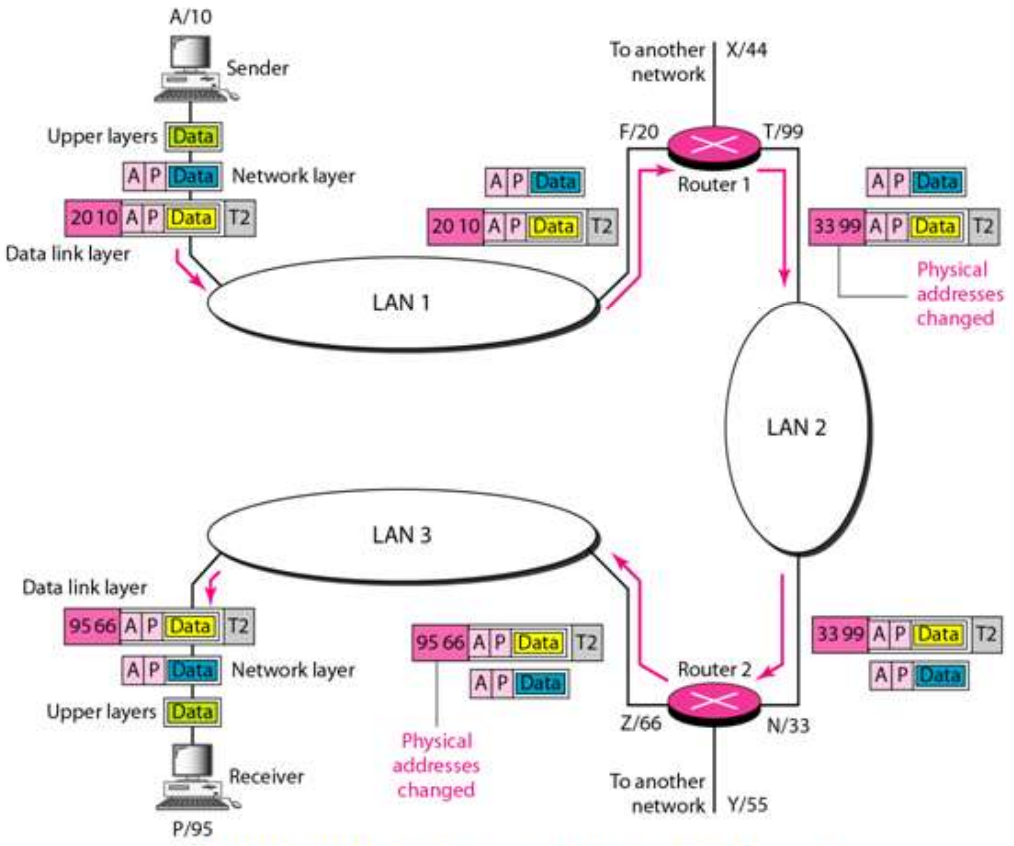
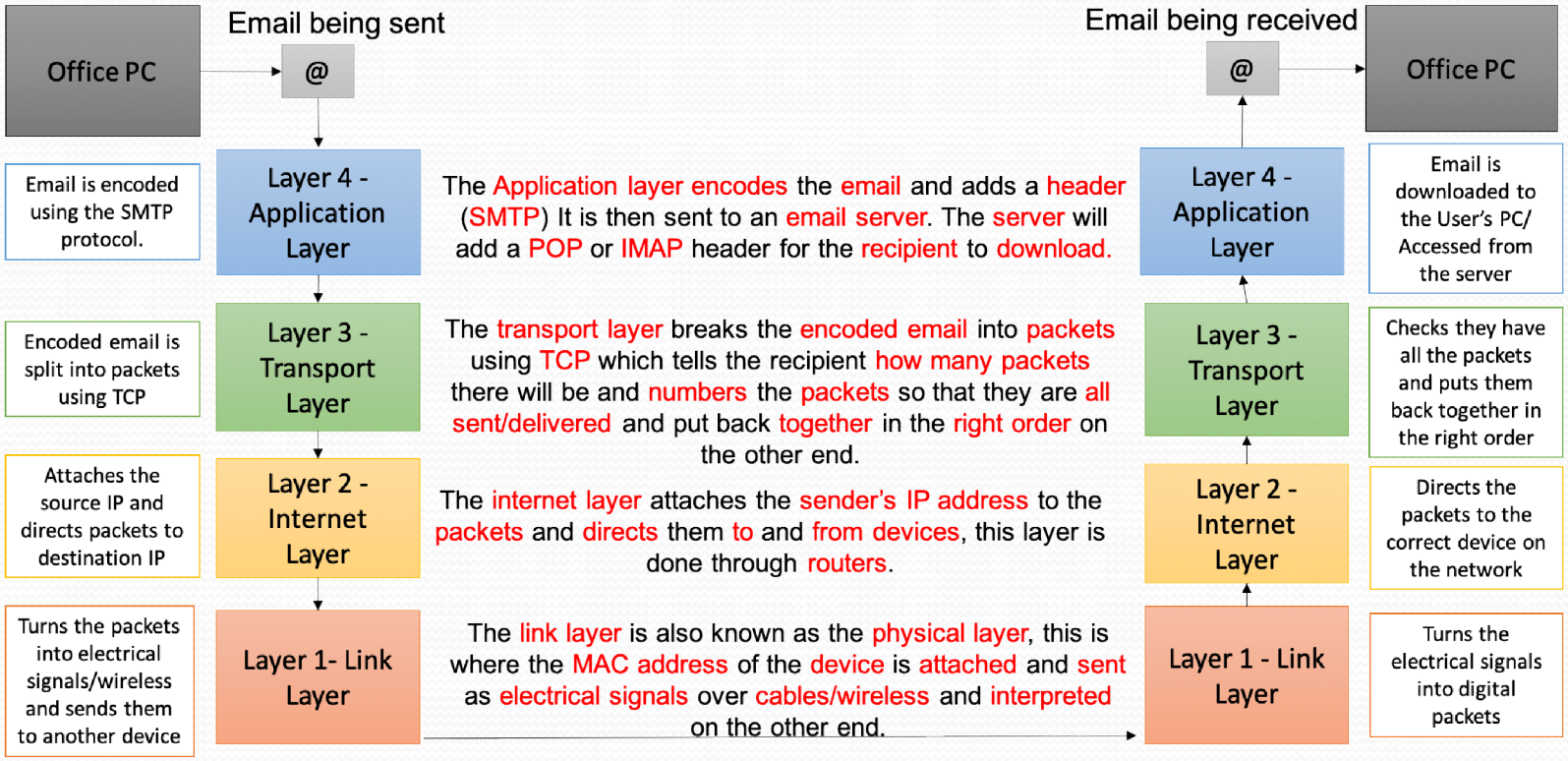


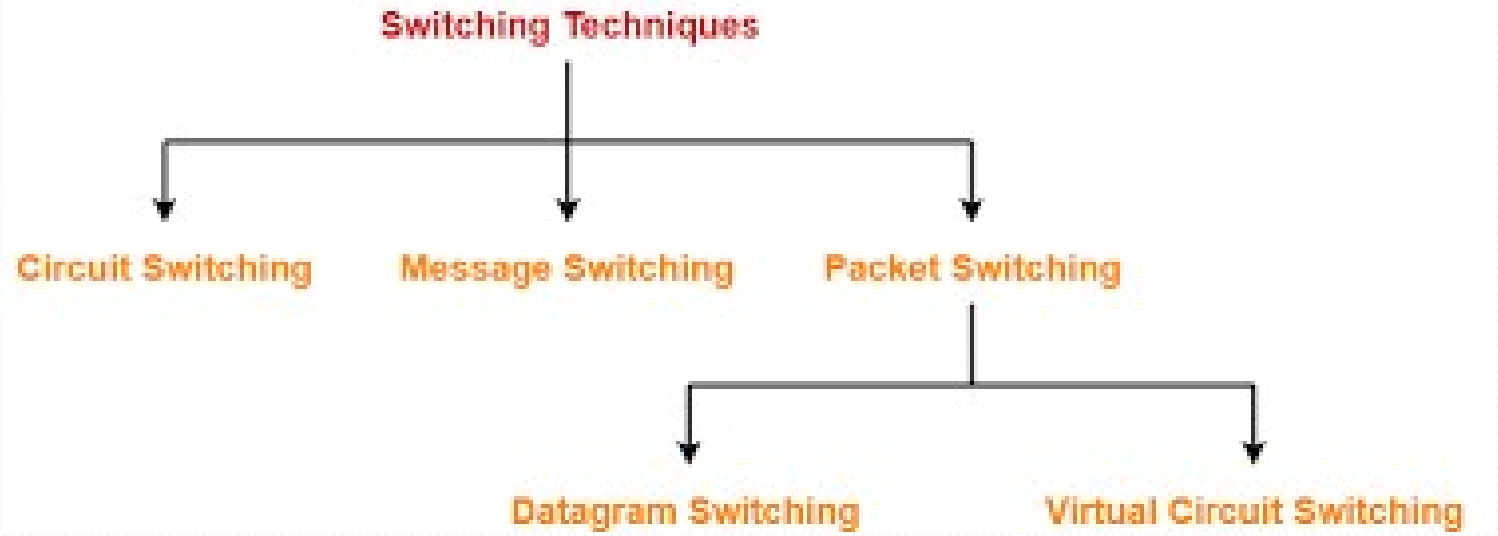
Figure 30: IP Addresses & Physical Addresses

TCP/IP LAYERING MODEL IN NUT SHELL



Switching techniques

- In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.
- Switching technique is used to connect the systems for making one-to-one communication.
- **Classification Of Switching Techniques**



Switching techniques(CONT.)

1. *Circuit switching* is a switching technique that establishes a dedicated path between sender and receiver. In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
2. *Message Switching* is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded. In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.

Switching techniques(CONT.)

3. *Packet switching* is a switching technique in which the message is splitted into smaller pieces known as packets and they are sent individually. The packets are given a unique number to identify their order at the receiving end.Every packet contains some information in its headers such as source address, destination address and sequence number.Packets will travel across the network, taking the shortest path as possible.All the packets are reassembled at the receiving end in correct order.If any packet is missing or corrupted, then a message will be sent to the source to resend the message.

Switching Techniques(cont.)

Circuit Switching Vs Packet Switching

Circuit Switching	Packet Switching
Physical path between source and destination	No physical path
All packets use same path	Packets travel independently
Reserve the entire bandwidth in advance	Does not reserve
Bandwidth Wastage	No Bandwidth wastage
No store and forward transmission	Supports store and forward transmission

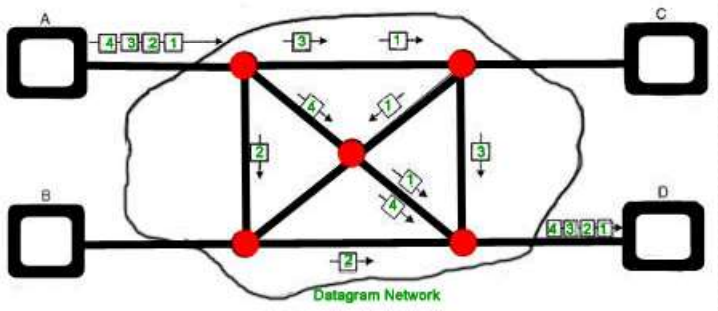
Approaches Of Packet Switching

- There are two approaches to Packet Switching:
- **Datagram Packet switching:**

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.The packets are reassembled at the receiving end in correct order. In Datagram Packet Switching technique, the path is not fixed. Intermediate nodes take the routing decisions to forward the packets. Datagram Packet Switching is also known as connectionless switching. Packet Switching uses Store and Forward technique.
- **Virtual Circuit Switching:**

- Virtual Circuit Switching is also known as connection-oriented switching.In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.Call request and call accept packets are used to establish the connection between sender and receiver.In this case, the path is fixed for the duration of a logical connection.

Datagram packet switching



Datagram Packet Switching

INTERNET PROTOCOL(IP)

- Network layer manages options pertaining to host and network addressing,managing sub-networks, and internetworking,connecting networks together to make an internetwork or an internet.

- Network layer takes the responsibility for routing packets from source to destination within or outside a subnet. Two different subnet may have different addressing schemes or non-compatible addressing types. Same with protocols, two different subnet may be operating on different protocols which are not compatible with each other. Network layer has the responsibility to route the packets from source to destination, mapping different addressing schemes and protocols.

INTERNET PROTOCOL(IP)(Cont.)

- **Network Layer Functionalities**
- Devices which work on Network Layer mainly focus on routing. Routing may include various tasks aimed to achieve a single goal. These can be:
- Addressing devices and networks.
- Populating routing tables or static routes.
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets.
- Internetworking between two different subnets.
- Delivering packets to destination with best efforts.
- Provides connection less transfer mechanism.

INTERNET PROTOCOL(IP)(Cont.)

- Switching at the network layer in the Internet uses the datagram approach to packet switching.
- Communication at the network layer in the Internet is connectionless. Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.
- 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.
- The IPv4 addresses are unique and universal. The address space of IPV4 is 2^{32} or 4,294,967,296. In IPv4 addressing, a block of addresses can be defined as x.y.z.t /*n* in which x.y.z.t defines one of the addresses and the /*n* defines the mask. The first address in the block can be found by setting the rightmost 32 – *n* bits to 0s , called as Network Address that identifies a particular network.
- The last address in the block can be found by setting the rightmost 32 – n bits to 1s , which is the broadcast address.

INTERNET PROTOCOL(IP)(Cont.)

- IP Addresses are always logical i.e. these are software based addresses which can be changed by appropriate configurations.

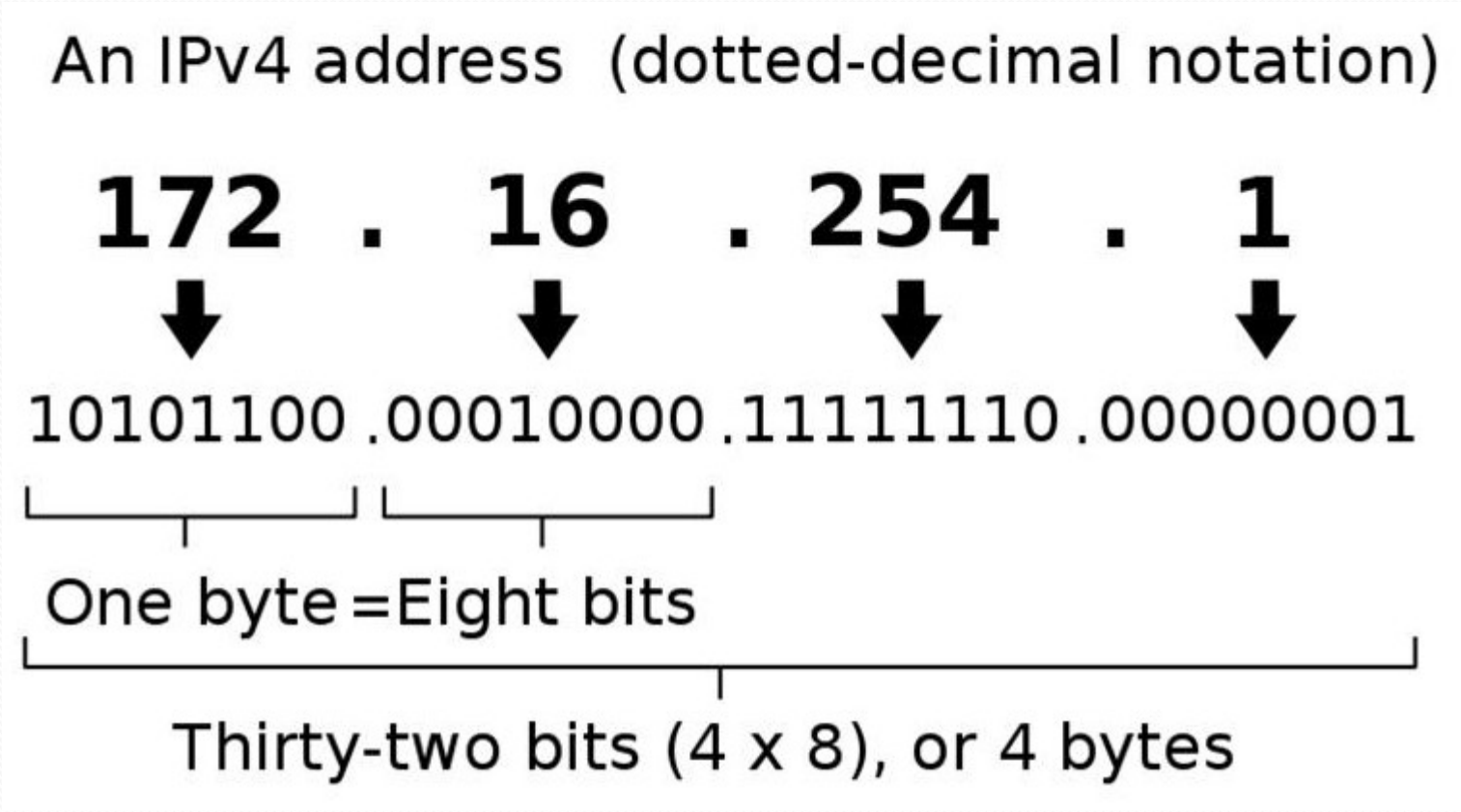
- A network address always points to host / node / server or it can represent a whole network. Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.

- IP addressing provides mechanism to differentiate between hosts and network. Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network. The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent.

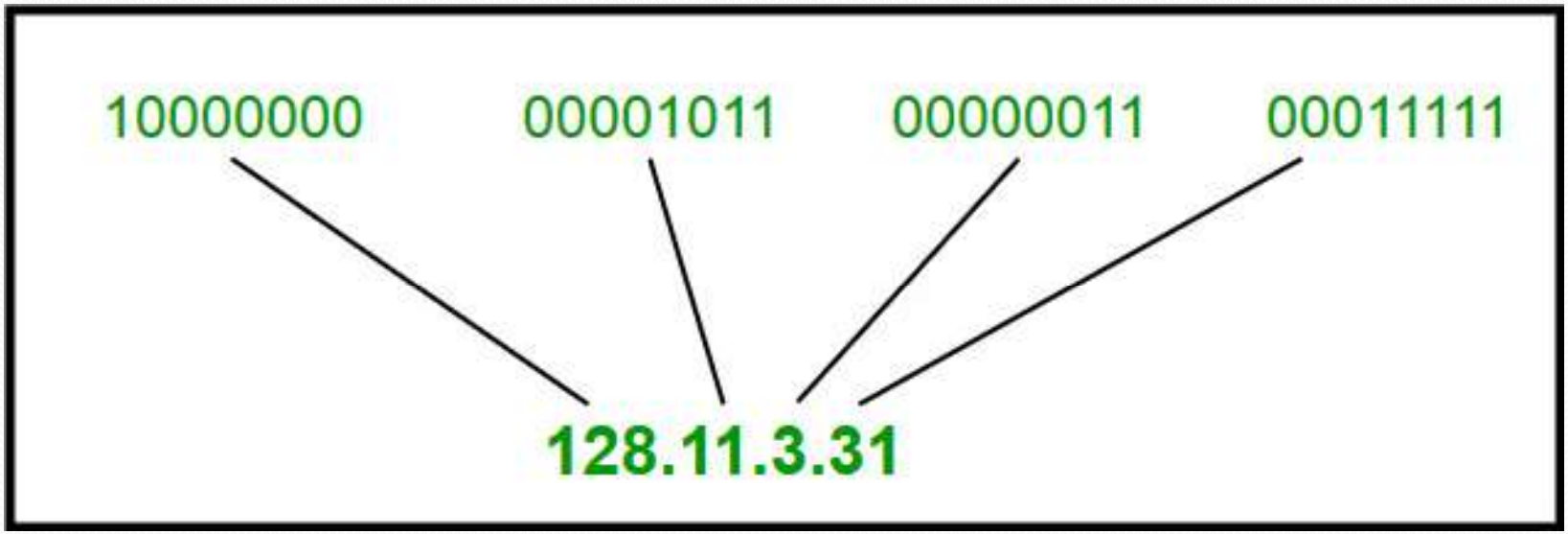
INTERNET PROTOCOL(IP)(Cont.)

- IP address is a logical numeric address assigned to every single computer, printer, Gigabit Ethernet switch, router or any other device in a TCP/IP-based network, with each of them possessing a unique IP address. IP addresses are either configured manually (static IP address) or configured by a DHCP server. An IP address consists of 4-bytes of data. A byte consists of 8 bits (a bit is a single digit and it could only be either a 1 or 0), therefore we have a total of 32 bits for each IP address. This is an IP address example in binary: 10101100. 00010000. 11111110.00000001. To simplify things, the dotted decimal representation is usually used to make IP address as: 172. 16. 254. 1

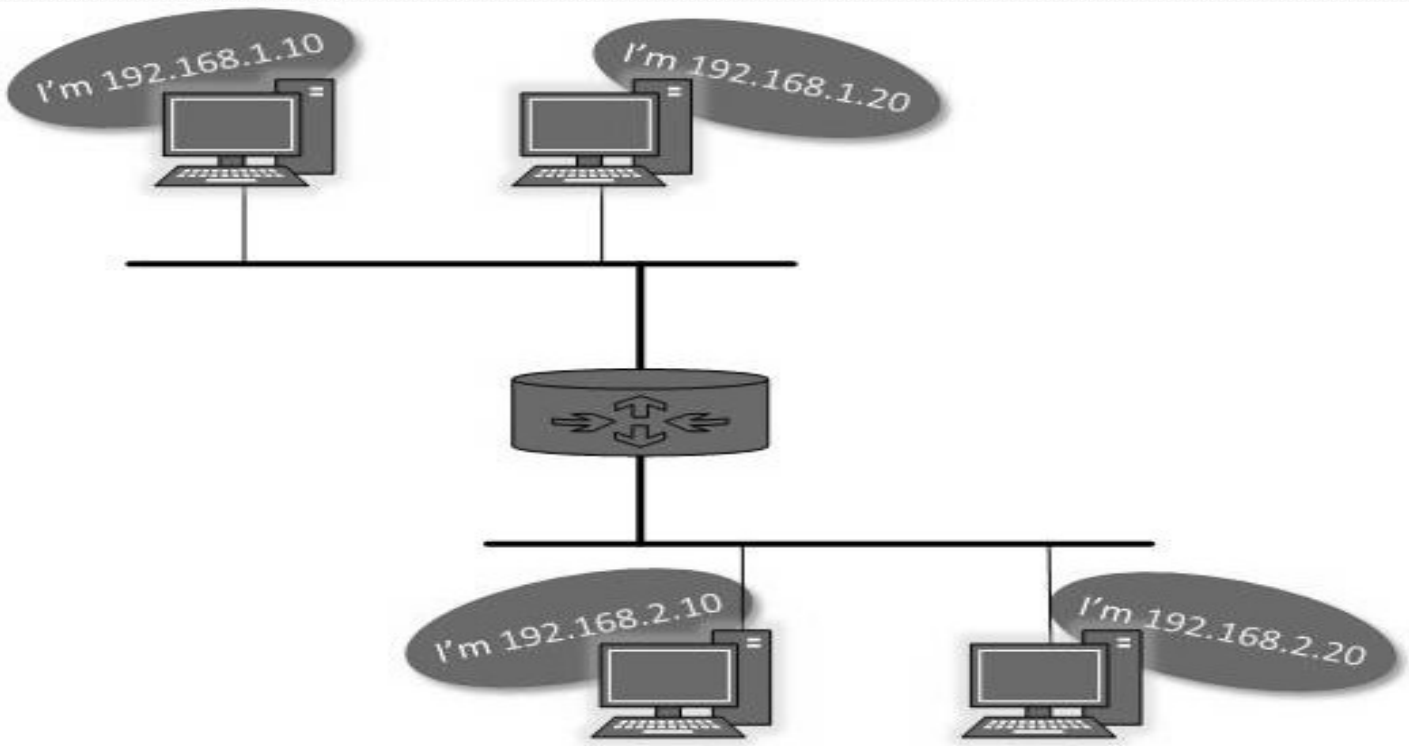
INTERNET PROTOCOL(IP)(Cont.)



INTERNET PROTOCOL(IP)(Cont.)



INTERNET PROTOCOL(IP)(Cont.)



INTERNET PROTOCOL(IP)(Cont.)

- Hosts in different subnet need a mechanism to locate each other. This task can be done by DNS. DNS is a server which provides Layer-3 address of remote host mapped with its domain name or FQDN. When a host acquires the Layer-3 Address (IP Address) of the remote host, it forwards all its packet to its gateway. A gateway is a router equipped with all the information which leads to route packets to the destination host.
- Routers take help of routing tables, which has the following information:
- Address of destination network
- Method to reach the network
- Routers upon receiving a forwarding request, forwards packet to its next hop (adjacent router) towards the destination.
- The next router on the path follows the same thing and eventually the data packet reaches its destination.

INTERNET PROTOCOL(IP)(Cont.)

- Network address can be of one of the following:
- Unicast (destined to one host)
- Multicast (destined to group)
- Broadcast (destined to all)
- Anycast (destined to nearest one)

- A router never forwards broadcast traffic by default. Multicast traffic uses special treatment as it is most a video stream or audio with highest priority. Anycast is just similar to unicast, except that the packets are delivered to the nearest destination when multiple destinations are available

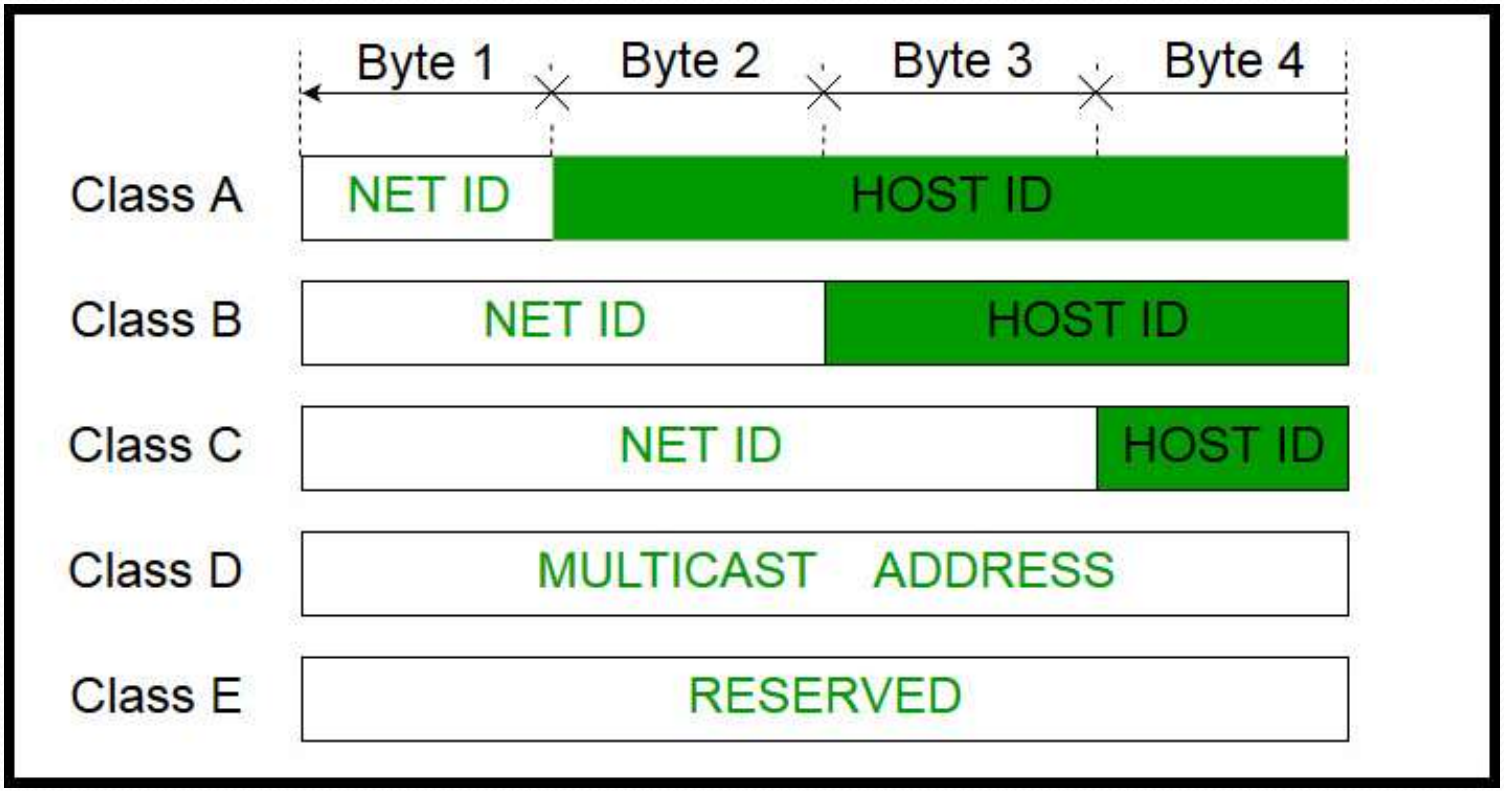
Classful Addressing

- The 32 bit IP address is divided into five sub-classes. These are:
- Class A
- Class B
- Class C
- Class D
- Class E
- Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address. IPv4 address is divided into two parts:

Classful Addressing(cont.)

- **Network ID**
- **Host ID**
- The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.

Classful Addressing(cont.)



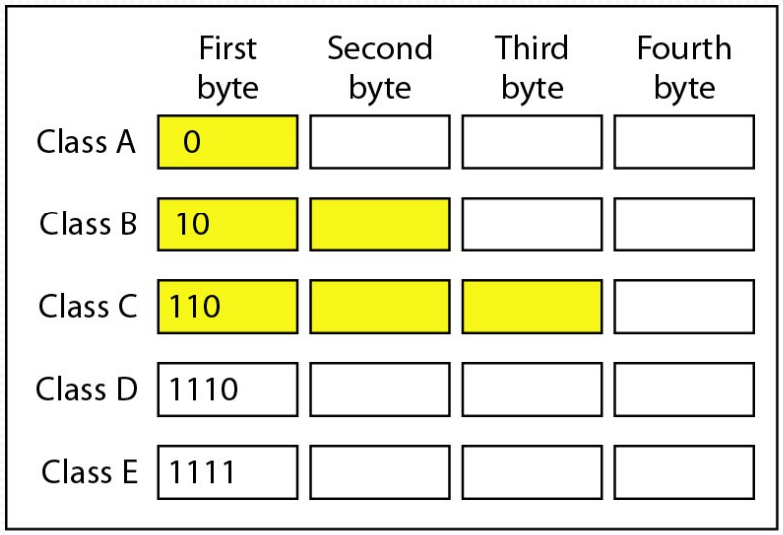
Classful Addressing(cont.)

- **Internet Protocol Version 4 (IPv4)**
- addressing enables every host on the TCP/IP network to be uniquely identifiable.
- IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:
- **Class A:** It uses first octet for network addresses and last three octets for host addressing.
- **Class B:** It uses first two octets for network addresses and last two for host addressing.
- **Class C:** It uses first three octets for network addresses and last one for host
- addressing.
- **Class D:** It provides flat IP addressing scheme in contrast to hierarchical structure for above three.

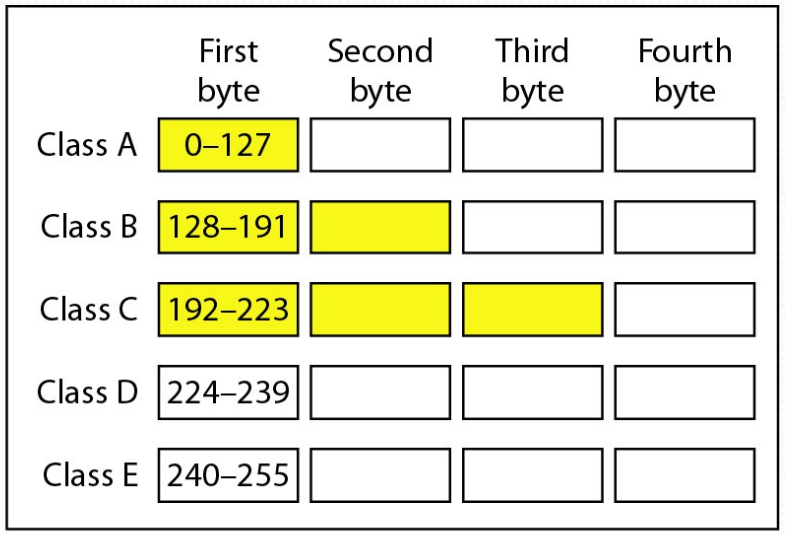
Classful Addressing(cont.)

- **Class E:** It is used as experimental.
- IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).
- Though IP is not reliable one; it provides 'Best-Effort-Delivery' mechanism.

FINDING THE CLASSES IN BINARY AND DOTTED-DECIMAL NOTATION



a. Binary notation



b. Dotted-decimal notation

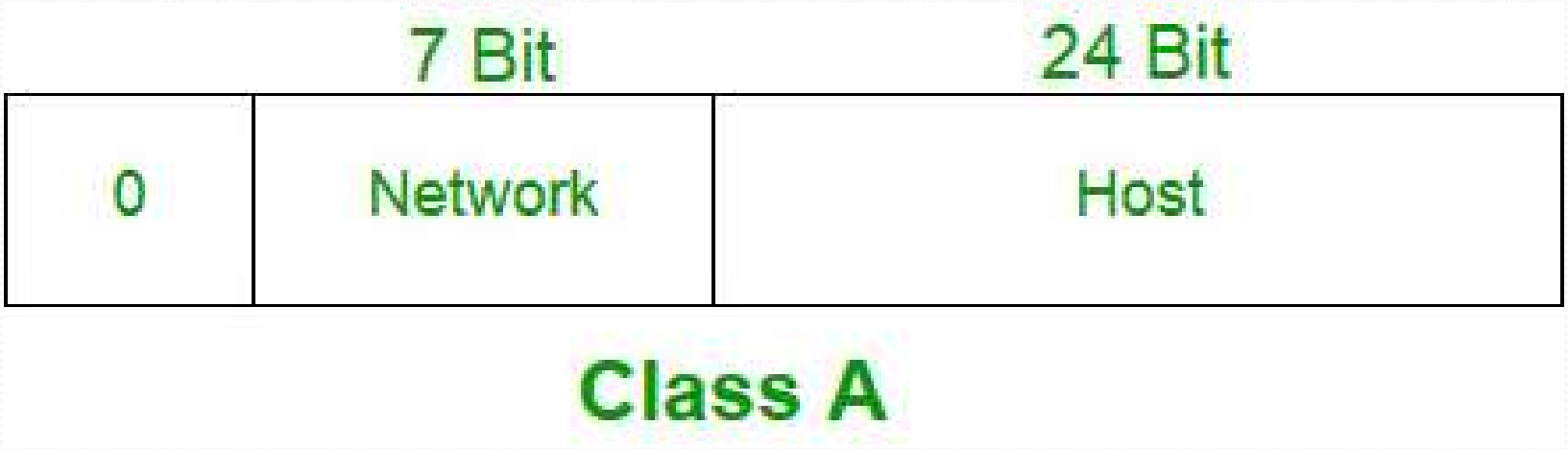
Classful Addressing(cont.)

- While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network address which identifies a network and whereas the last IP address is reserved for broadcast IP.

Class A

- IP address belonging to class A are assigned to the networks that contain a large number of hosts.
- The network ID is 8 bits long.
- The host ID is 24 bits long.
- The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:
- 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 – 2 = 16,777,214 host ID
- IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x

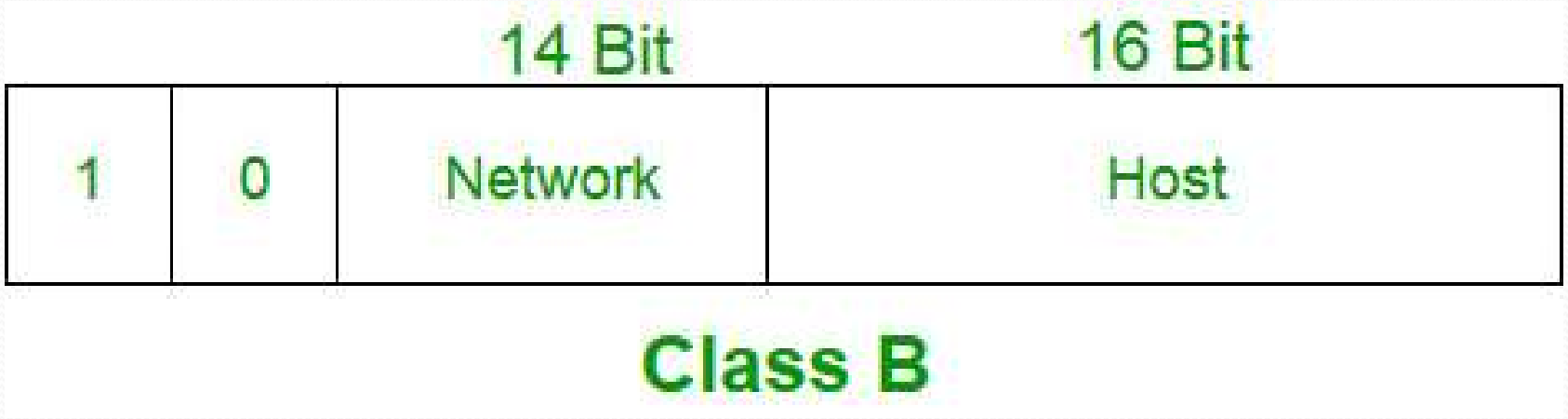
Class A



Class B

- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.
- The network ID is 16 bits long.
- The host ID is 16 bits long.
- The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:
- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address
- IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.

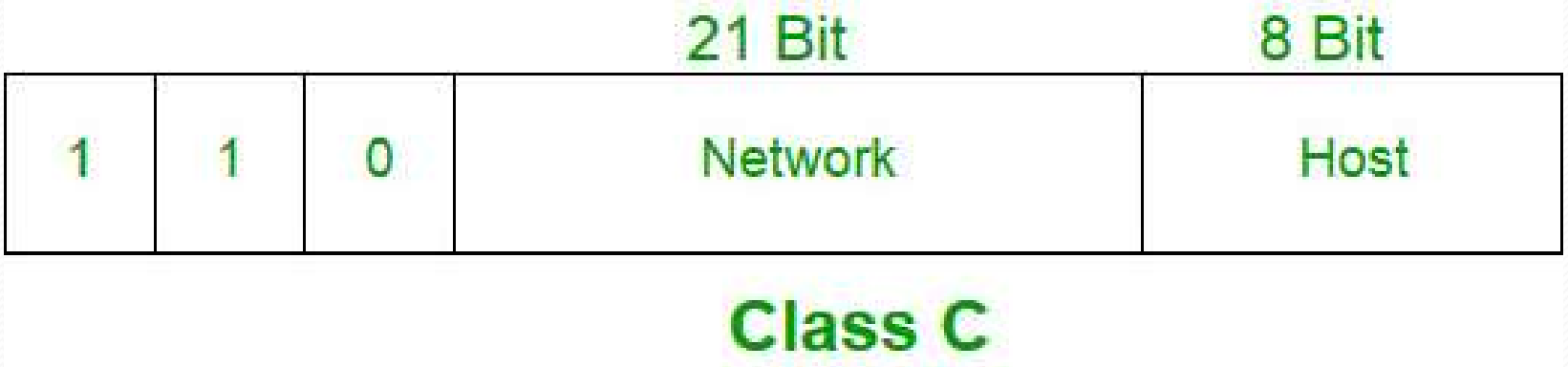
Class B



Class C

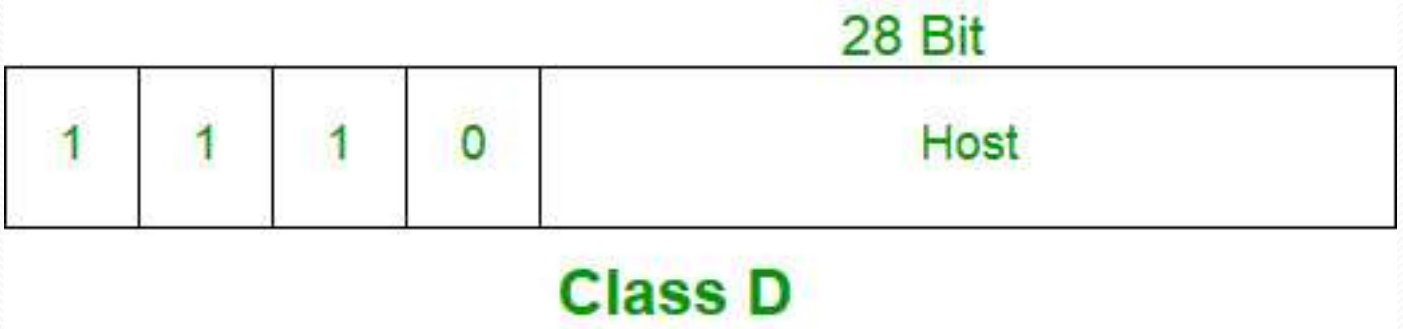
- IP address belonging to class C are assigned to small-sized networks.
  - The network ID is 24 bits long.
  - The host ID is 8 bits long.
- The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:
  - 2^21 = 2097152 network address
  - 2^8 – 2 = 254 host address
- IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

Class C



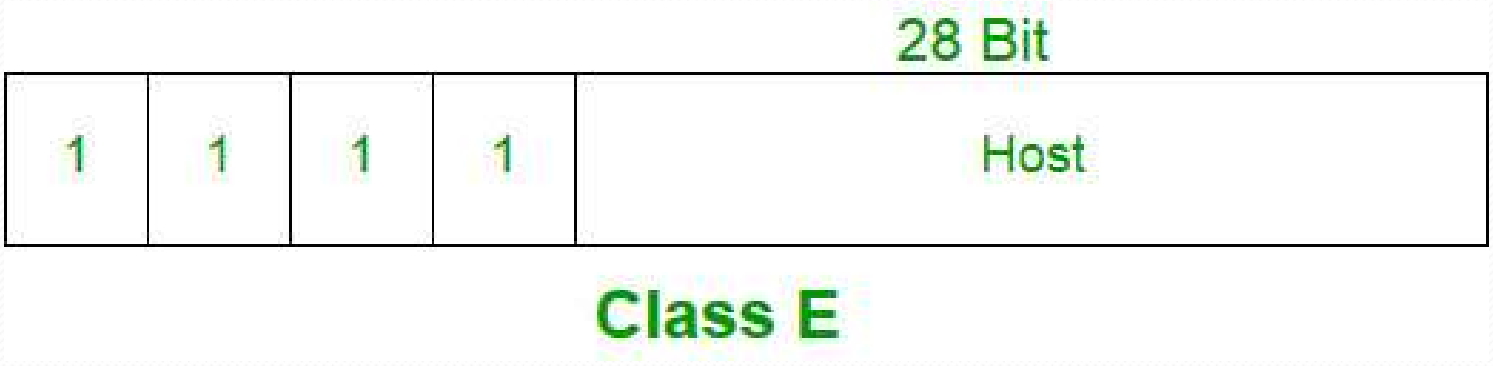
Class D

- IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.
- Class D does not posess any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class E

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.255. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



NUMBER OF BLOCKS AND BLOCK SIZE IN CLASSFUL IPV4 ADDRESSING

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

Default Subnet Masks or default masks

- There are default standard subnet masks for **IP Address Classes** (Class A, B and C addresses):
- Subnet masks apply only to Class A, B or C IP addresses. The subnet mask is like a filter that is applied to a message's destination IP address. Its objective is to determine if the local network is the destination network.
- The subnet mask goes like this: If a destination IP address is 206.175.162.21, we know that it is a Class C address & that its binary equivalent is: 11001110.10101111.10100010.00010101
- We also know that the default standard Class C subnet mask is: 255.255.255.0 and that its binary equivalent is: 11111111.11111111.11111111.00000000
- When these two binary numbers (the IP address & the subnet mask) are combined using Boolean Algebra, the Network ID of the destination network is the result:
- 11001110.10101111.10100010.00000000
- The result is the IP address of the network which in this case is the same as the local network; means that the message is for a node on the local network.

Default Subnet Masks or default masks

Class A
Subnet Mask

Netwok	Host	Host	Host
255	0	0	0

Class B
Subnet Mask

Netwok	Network	Host	Host
255	255	0	0

Class C
Subnet Mask

Netwok	Network	Network	Host
255	255	255	0

IP addresses classes and Default subnet mask

Class	IP address ranges	Default subnet mask
A	0.0.0.0 to 127.255.255.255	255.0.0.0
B	128.0.0.0 to 191.155.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Not applicable
E	240.0.0.0 to 255.255.255.255	Not applicable

Default Subnet Masks or default masks

- In classful addressing, a large part of the available addresses were wasted.
- **Default masks for classful addressing**

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

- Classful addressing, which is almost obsolete, is replaced with classless addressing.

Default Subnet Masks or default masks

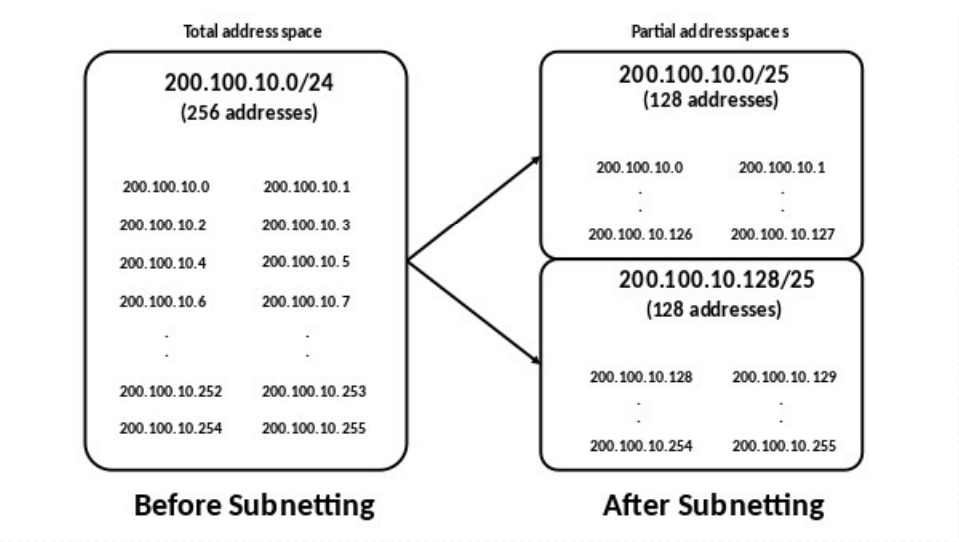
IP: 211. 139. 157. 9

Subnet Mask: 255. 255. 255. 0

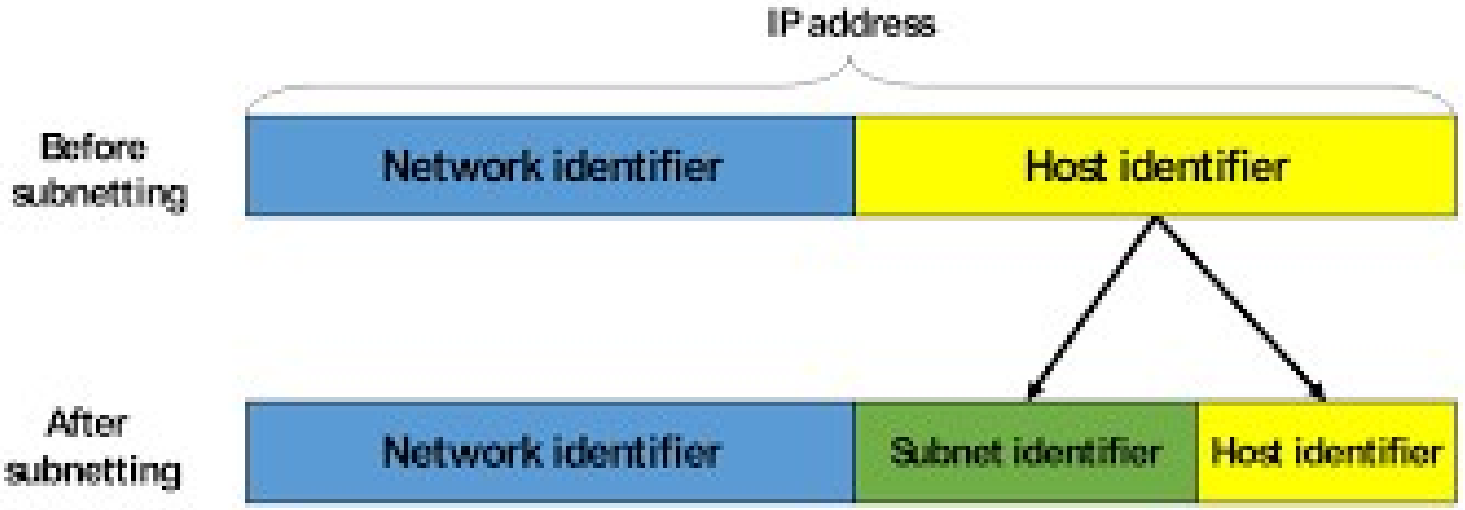
Subnet (subnetwork)

- A subnet, or subnetwork, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments. The Internet Protocol (IP) is the method for sending data from one computer to another over the internet. Each computer, or host, on the internet has at least one IP address as a unique identifier.
- Organizations will use a subnet to subdivide large networks into smaller, more efficient subnetworks. One goal of a subnet is to split a large network into a grouping of smaller, interconnected networks to help minimize traffic. This way, traffic doesn't have to flow through unnecessary routs, increasing network speeds. Subnetting, the segmentation of a network address space, improves address allocation efficiency.

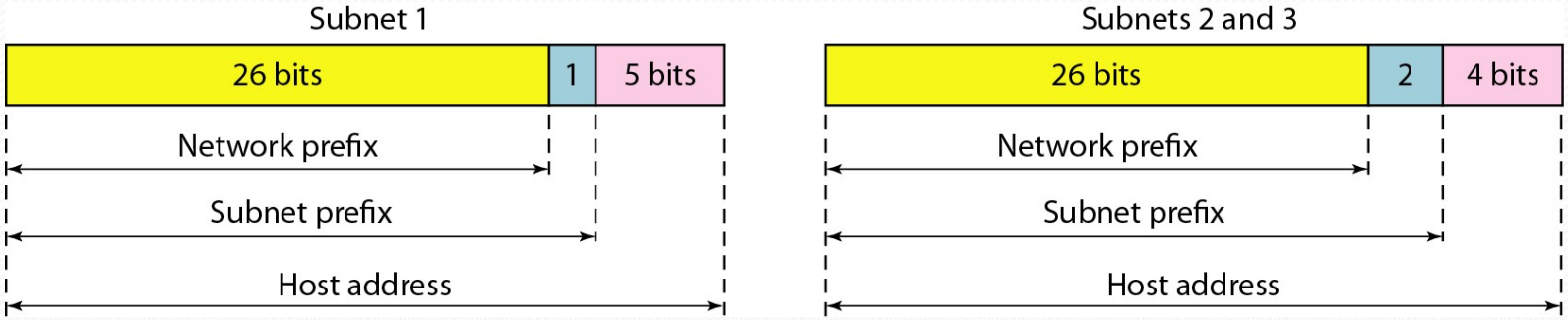
Subnet (subnetwork)(cont.)



Subnet (subnetwork)(cont.)



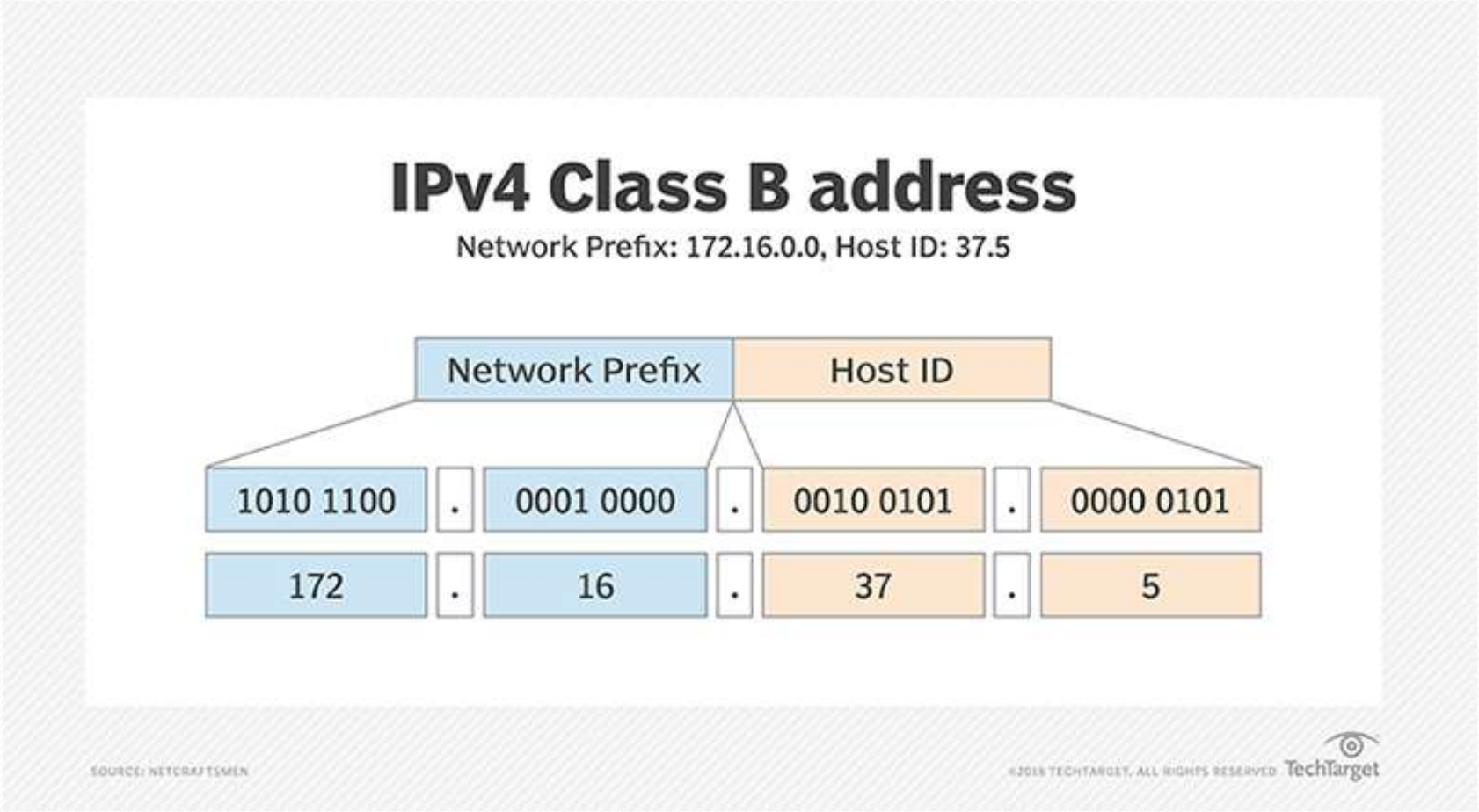
THREE-LEVEL HIERARCHY IN AN IPV4 ADDRESS



How subnets work

- Each subnet allows its connected devices to communicate with each other, while routers are used to communicate between subnets. The size of a subnet depends on the connectivity requirements and the network technology employed. A point-to-point subnet allows two devices to connect, while a data center subnet might be designed to connect many more devices.
- Each organization is responsible for determining the number and size of the subnets it creates, within the limits of the address space available for its use. Additionally, the details of subnet segmentation within an organization remain local to that organization.
- An IP address is divided into two fields: a Network Prefix (also called the Network ID) and a Host ID. What separates the Network Prefix and the Host ID depends on whether the address is a Class A, B or C address. The following figure shows an IPv4 Class B address, 172.16.37.5. Its Network Prefix is 172.16.0.0, and the Host ID is 37.5.

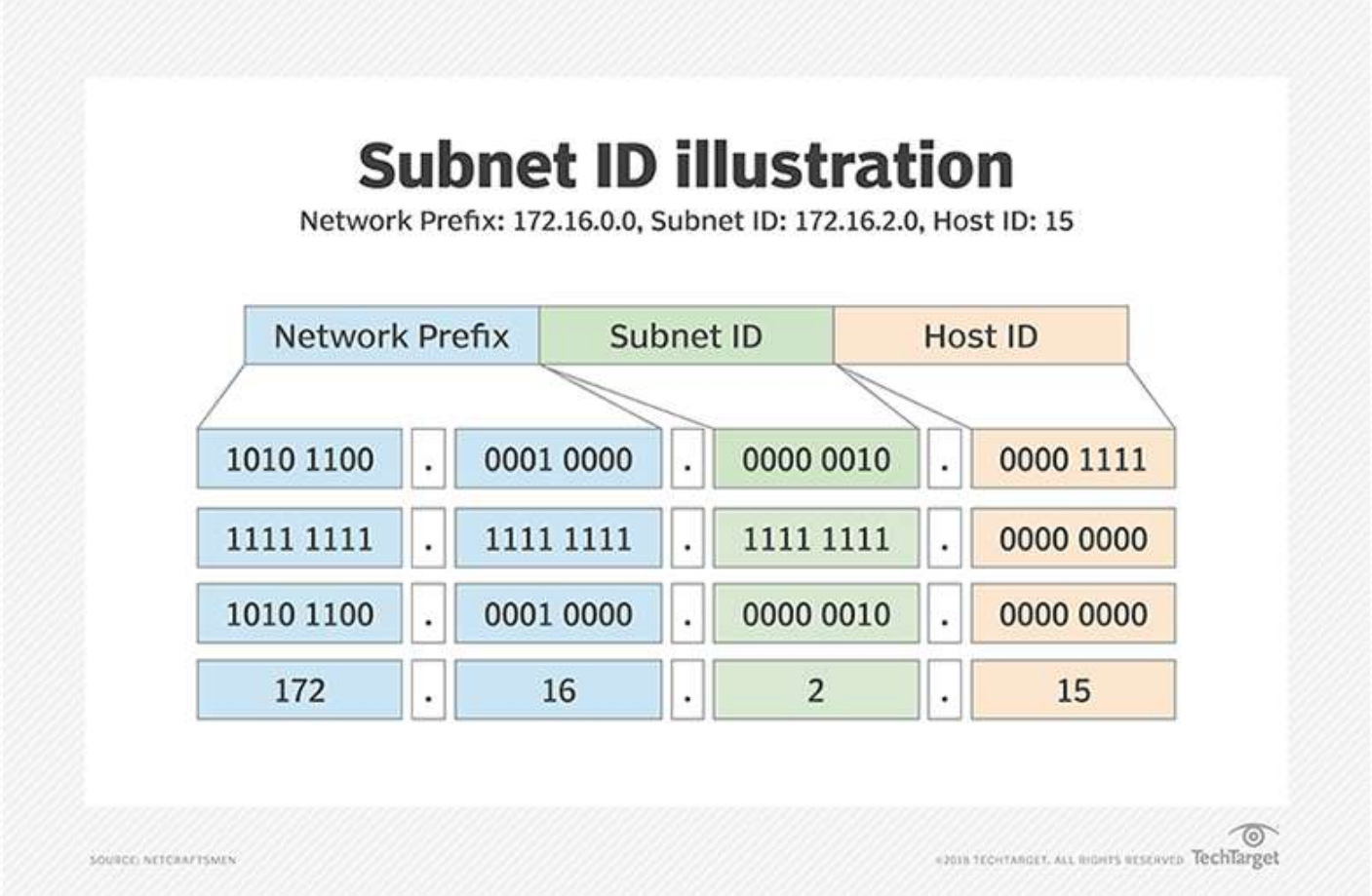
How subnets work(cont.)



How subnets work(cont.)

- The subnet mechanism uses a portion of the Host ID field to identify individual subnets. For example,the following figure, shows the third group of the 172.16.0.0 network being used as a Subnet ID. A subnet mask is used to identify the part of the address that should be used as the Subnet ID. The subnet mask is applied to the full network address using a binary AND operation. AND operations operate, assuming an output is "true" only when both inputs are "true." Otherwise, the output is "false." Only when two bits are both 1. This results in the Subnet ID.
- The following figure shows the AND of the IP address, as well as the mask producing the Subnet ID. Any remaining address bits identify the Host ID. The subnet in the figure is identified as 172.16.2.0, and the Host ID is 5. In practice, network staff will typically refer to a subnet by just the Subnet ID. It would be common to hear someone say, "Subnet 2 is having a problem today," or, "There is a problem with the dot-two subnet."

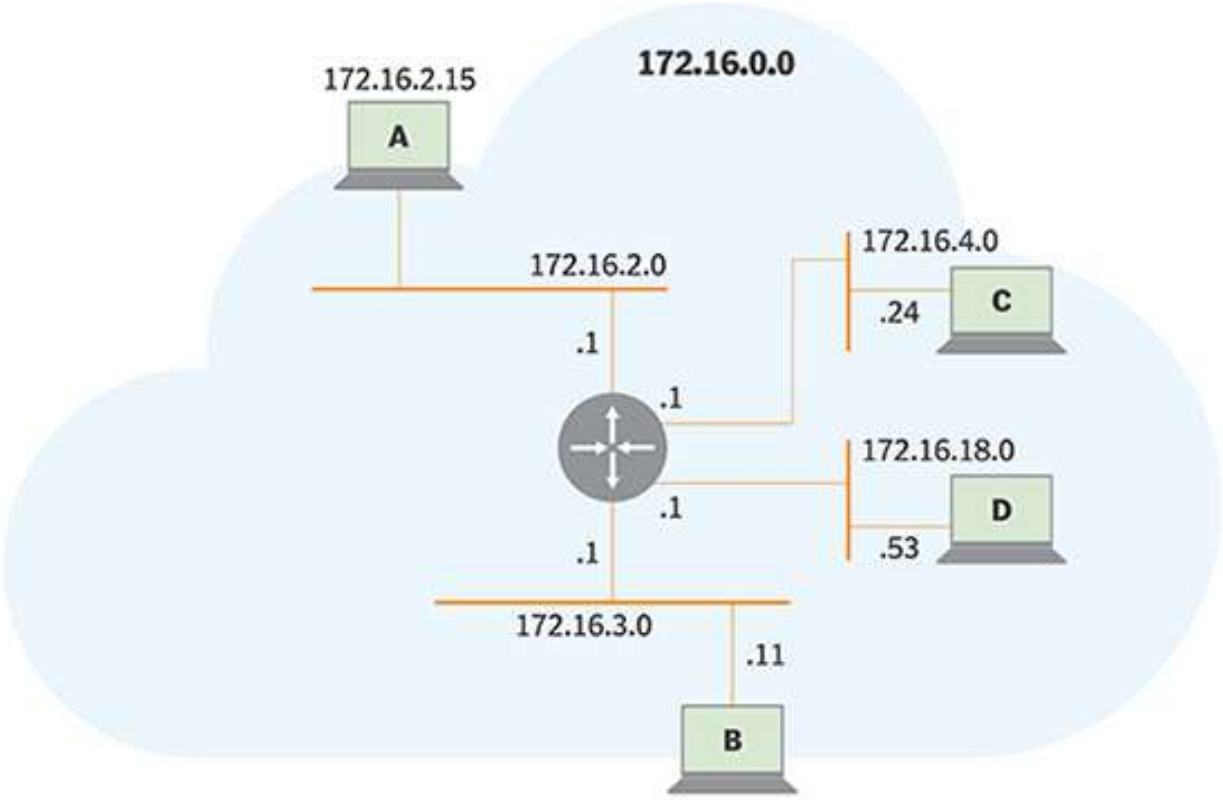
How subnets work(cont.)



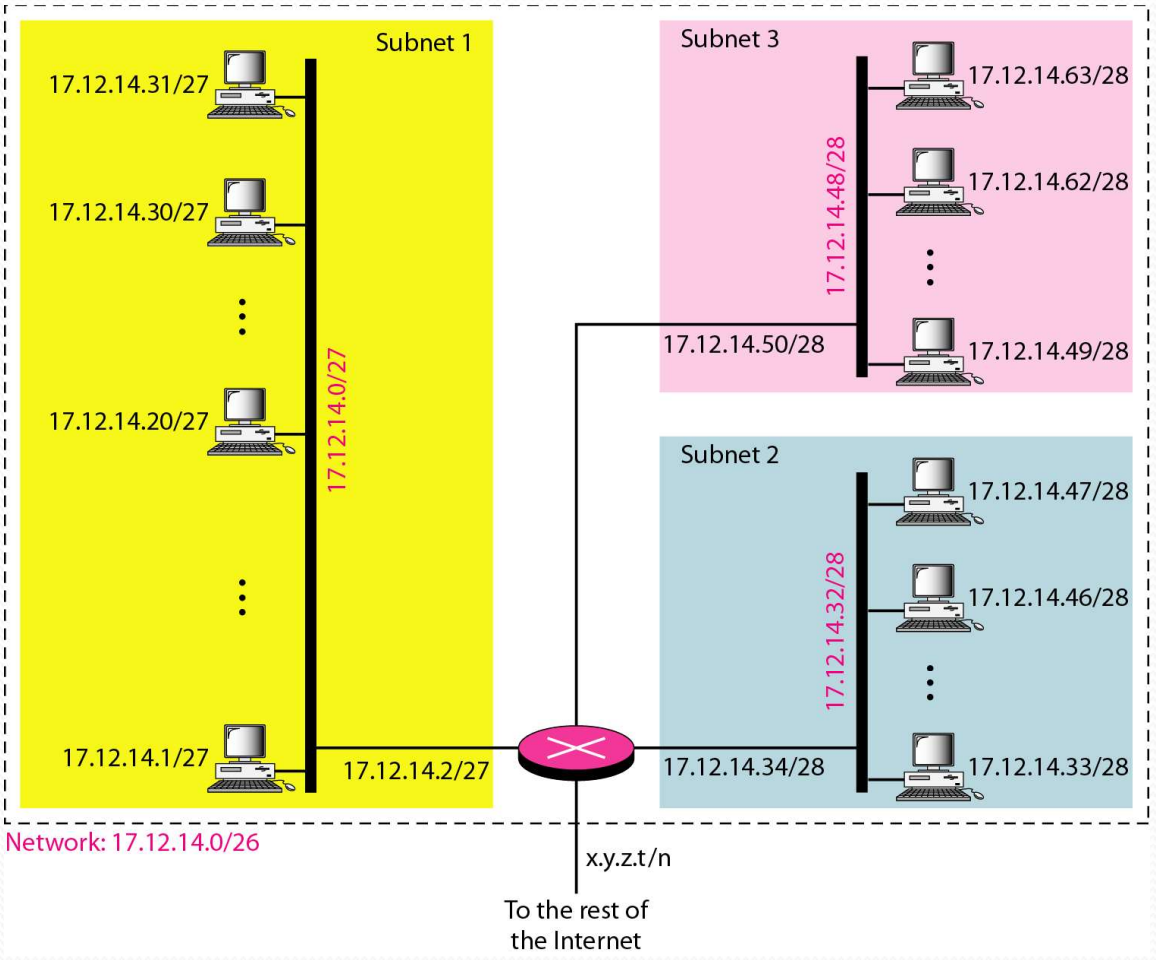
How subnets work(cont.)

- The Subnet ID is used by routers to determine the best route between subnetworks. The following figure shows the 172.16.0.0 network, with the third grouping as the Subnet ID. Four of the 256 possible subnets are shown connected to one router. Each subnet is identified either by its Subnet ID or the subnet address with the Host ID set to .0. The router interfaces are assigned the Host ID of .1 -- e.g., 172.16.2.1.
- When the router receives a packet addressed to a host on a different subnet than the sender -- host A to host C, for example -- it knows the subnet mask and uses it to determine the Subnet ID of host C. It examines its routing table to find the interface connected to host C's subnet and forwards the packet on that interface.
- **Subnet segmentation**
- A subnet itself also may be segmented into smaller subnets, giving organizations the flexibility to create smaller subnets for things like point-to-point links or for subnetworks that support a few devices. The example below uses an 8-bit Subnet ID. The number of bits in the subnet mask depends on the organization's requirements for subnet size and the number of subnets. Other subnet mask lengths are common. While this adds some complexity to network addressing, it significantly improves the efficiency of network address utilization.

Subnet segmentation illustrated



CONFIGURATION AND ADDRESSES IN A SUBNETTED



How subnets work(cont.)

- A subnet can be delegated to a suborganization, which itself may apply the subnetting process to create additional subnets, as long as sufficient address space is available. Subnetting performed by a delegated organization is hidden from other organizations. As a result, the Subnet ID field length and where subnets are assigned can be hidden from the parent (delegating) organization, a key characteristic that allows networks to be scaled up to large sizes.
- In modern routing architectures, routing protocols distribute the subnet mask with routes and provide mechanisms to summarize groups of subnets as a single routing table entry. Older routing architectures relied on the default Class A, B and C IP address classification to determine the mask to use. CIDR notation is used to identify Network Prefix and Mask, where the subnet mask is a number that indicates the number of ones in the Mask (e.g., 172.16.2.0/24). This is also known as Variable-Length Subnet Masking (VLSM) and CIDR. Subnets and subnetting are used in both IPv4and IPv6 networks, based on the same principles.

How subnets work(cont.)

- The subnet mask (formal term: extended network prefix), is not an address, but determines which part of an IP address is the network field and which part is the host field. A subnet mask is 32 bits long and has 4 octets, just like an IP address. To determine the subnet mask for a particular subnetwork IP address follow these steps:
- Express the subnetwork IP address in binary form
- Replace the network and subnet portion of the address with all 1s
- Replace the host portion of the address with all 0s
- As the last step convert the binary expression back to dotted-decimal notation.
- The term “operations” in mathematics refers to rules that define how one number combines with other numbers. The basic Boolean operations are AND, OR, and NOT.

How subnets work(cont.)

- **And Function**
- In order to route a data packet, the router must first determine the destination network/subnet address by performing a logical AND using the destination host's IP address and the subnet mask.The result will be the network/subnet address.The router has received a packet for host 131.108.2.2 – it uses the AND operation to learn that this packet should be routed to subnet 131.108.2.0. The process used to apply the subnet mask involves Boolean Algebra to filter out non-matching bits to identify the network address.Boolean Algebra is a process that applies binary logic to yield binary results. Working with subnet masks, you need only 4 basic principles of Boolean Algebra:
- 1 and 1 = 1
- 1 and 0 = 0
- 0 and 1 = 0
- 0 and 0 = 0.
- In another words, the only way you can get a result of a 1 is to combine 1 & 1. Everything else will end up as a 0. The process of combining binary values with Boolean Algebra is called Anding.

How subnets work(cont.)

- A subnet mask is a mask that divides the IP address into a network address and a host address. Subnet masks are the same size as the IP address and can be written in dot-decimal notation(ex. 255.255.255.0).

How subnets work(cont.)

Subnet Mask

Suffix	Hosts	32-Borrowed=CIDR	2^Borrowed = Hosts	Binary=> dec = Suffix
.255	1	/32	0	11111111
.254	2	/31	1	11111110
.252	4	/30	2	11111100
.248	8	/29	3	11111000
.240	16	/28	4	11110000
.224	32	/27	5	11100000
.192	64	/26	6	11000000
.128	128	/25	7	10000000

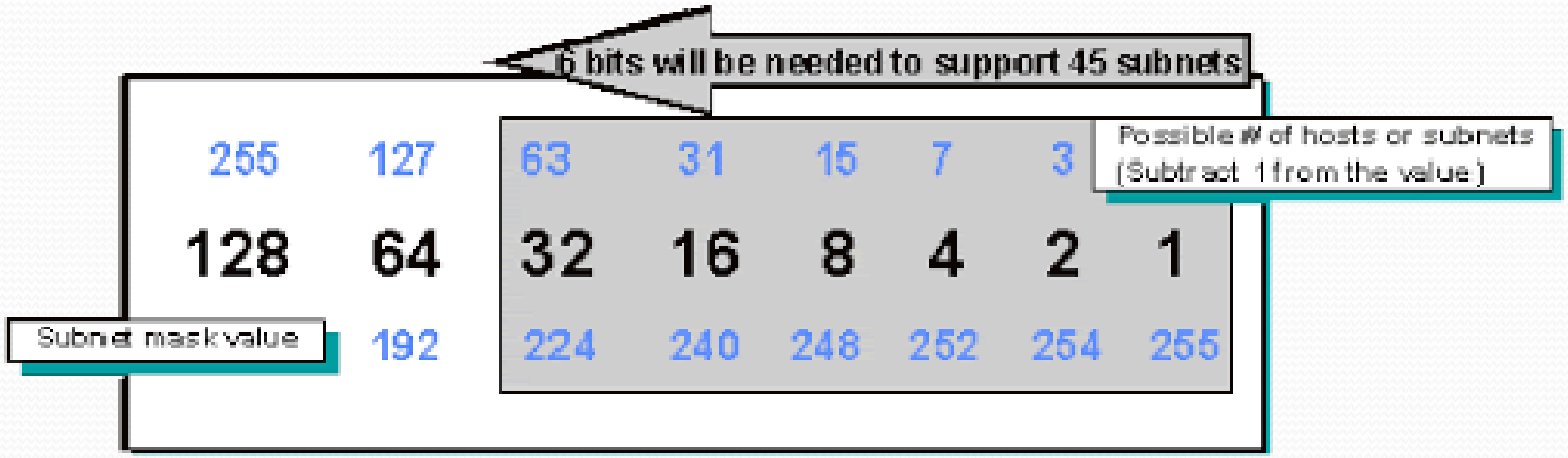
How subnets work(cont.)

- **Defining a Subnet Mask**
- You have an IP address of 138.45.0.0 which you need to subnetwork into 45 individual networks.

- **Step 1.** Determine the class and the default subnet mask of the IP address you have been given.
- *IP address 138.45.0.0 is a Class B address with a default subnet mask of 255.255.0.0*
- **Step 2.** Identify the number of subnetworks (subnets) that are required.
- *45 individual networks (subnets) will be required.*
- **Step 3.** Determine how many bits are required to support the total number of subnets.
- *You can determine this by figuring the binary value of 45 which is 00101101. This tells us that it takes a total of **6** bits to support the value of 45, 101101.*
- ** The fastest way to figure the number of bits required is to use the IP address cheat chart. (Remember to subtract 1 from the Possible # of hosts or subnets section).*

How subnets work(cont.)

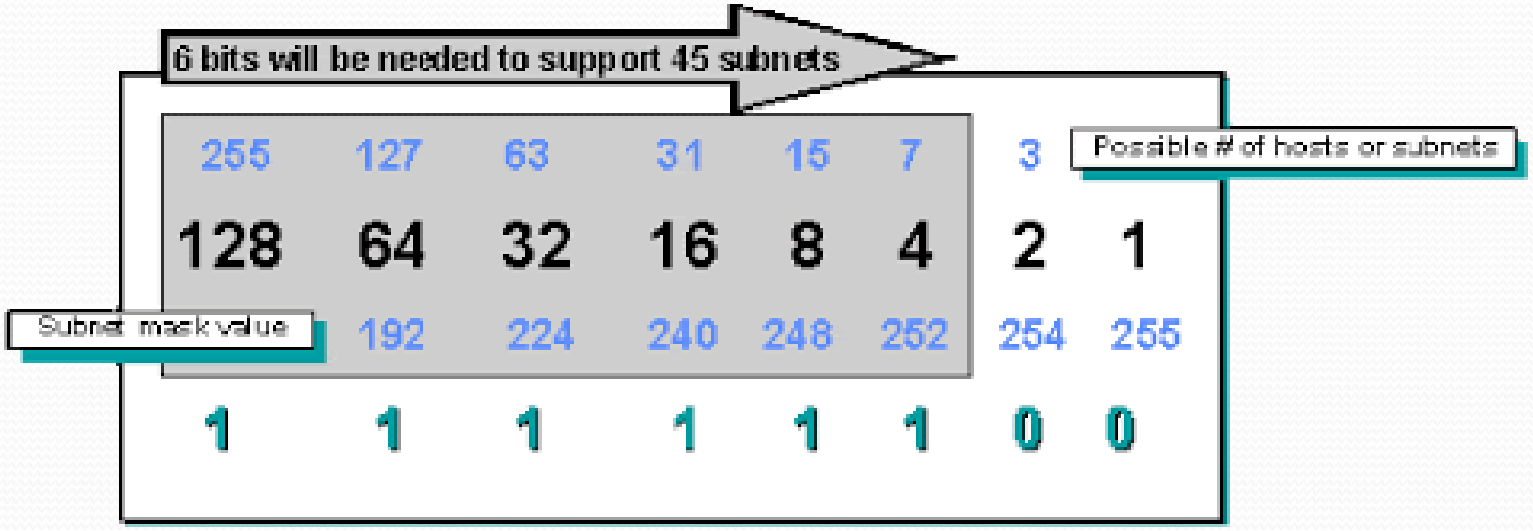
IP Address Cheat Chart



* To calculate the number of bits required to support hosts or subnets, add each value from right to left until you reach the first value high enough to support the required number. Then count the number of bits it took to get to that value.

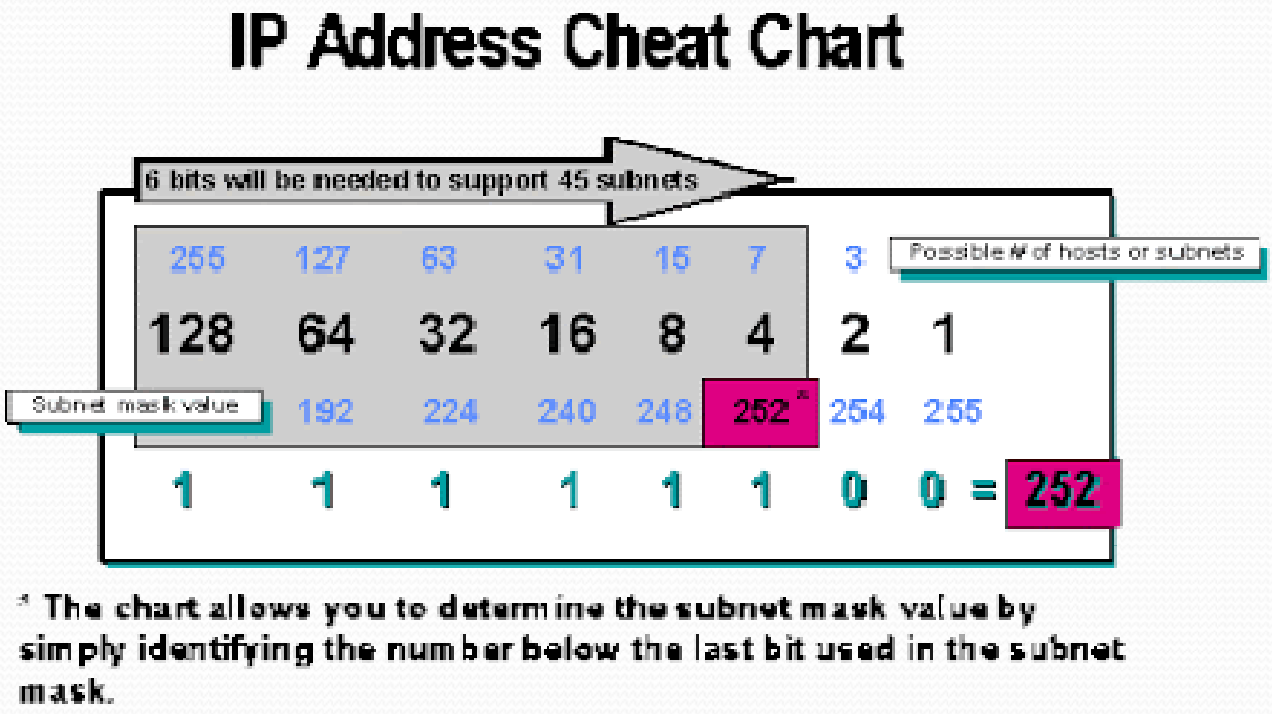
How subnets work(cont.)

- **Step 4.** Starting from the left hand side of the binary chart, count out the number of bits required to support the subnet mask.
- **IP Address Cheat Chart**



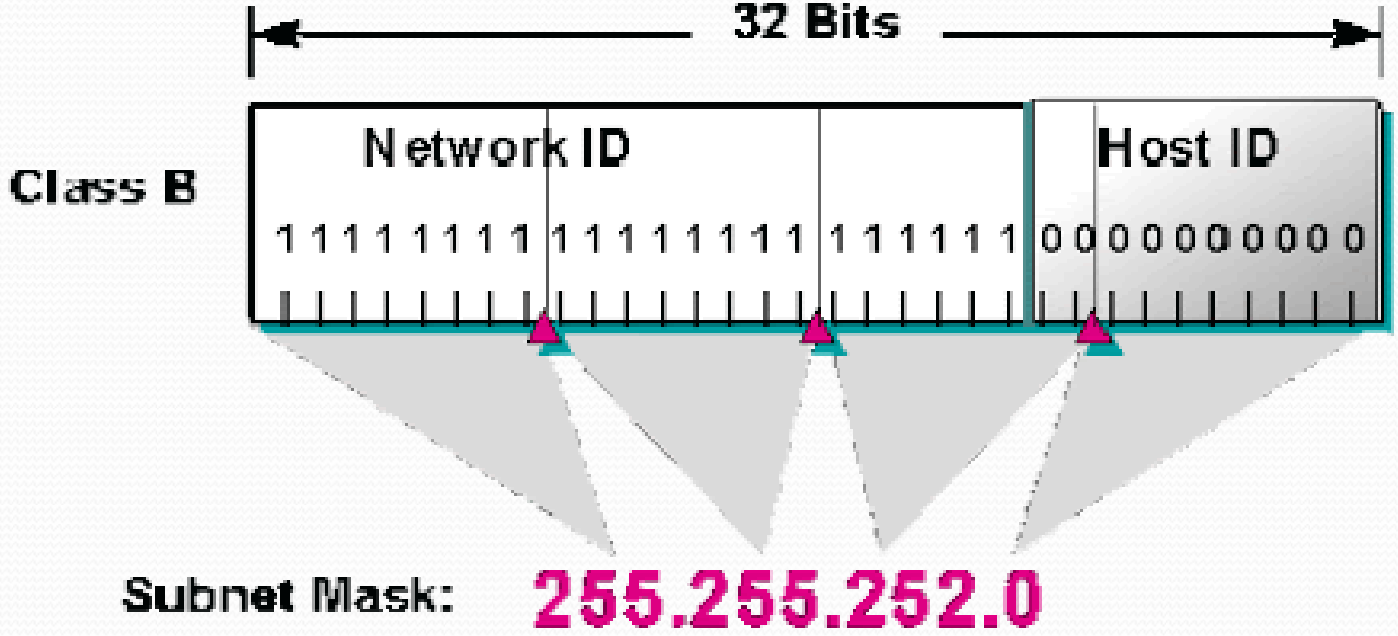
How subnets work(cont.)

- **Step 5.** To determine the subnet mask value, perform a binary to decimal conversion on your previous result or use the IP cheat chart.

- 

example

- To support 45 individual networks with a given network ID of 138.45.0.0 we would have to use a subnet mask of 255.255.252.0



example

- Given the subnet mask of 255.255.252.0, how many host addresses could you support per each subnetwork?
- **Answer:**
- To solve this question, you will simply determine the number of bits that are in the host portion of the IP address. Since there are 10 bits remaining in the host ID portion of the IP address, you would take 2^{10} which is 1,024 - 2 (for the invalid addresses) = 1,022 total hosts per subnetwork.

Beneficial uses of subnets

- **Reallocating IP addresses.** Each class has a limited number of host allocations; for example, networks with more than 254 devices need a Class B allocation. If a network administrator is working with a Class B or C network and needs to allocate 150 hosts for three physical networks located in three different cities, they would need to either request more address blocks for each network -- or divide a network into subnets that enable administrators to use one block of addresses on multiple physical networks.
- **Relieving network congestion.** If much of an organization's traffic is meant to be shared regularly between the same cluster of computers, placing them on the same subnet can reduce network traffic. Without a subnet, all computers and servers on the network would see data packets from every other computer.
- **Improving network security.** Subnetting allows network administrators to reduce network-wide threats by quarantining compromised sections of the network and by making it more difficult for trespassers to move around an organization's network.

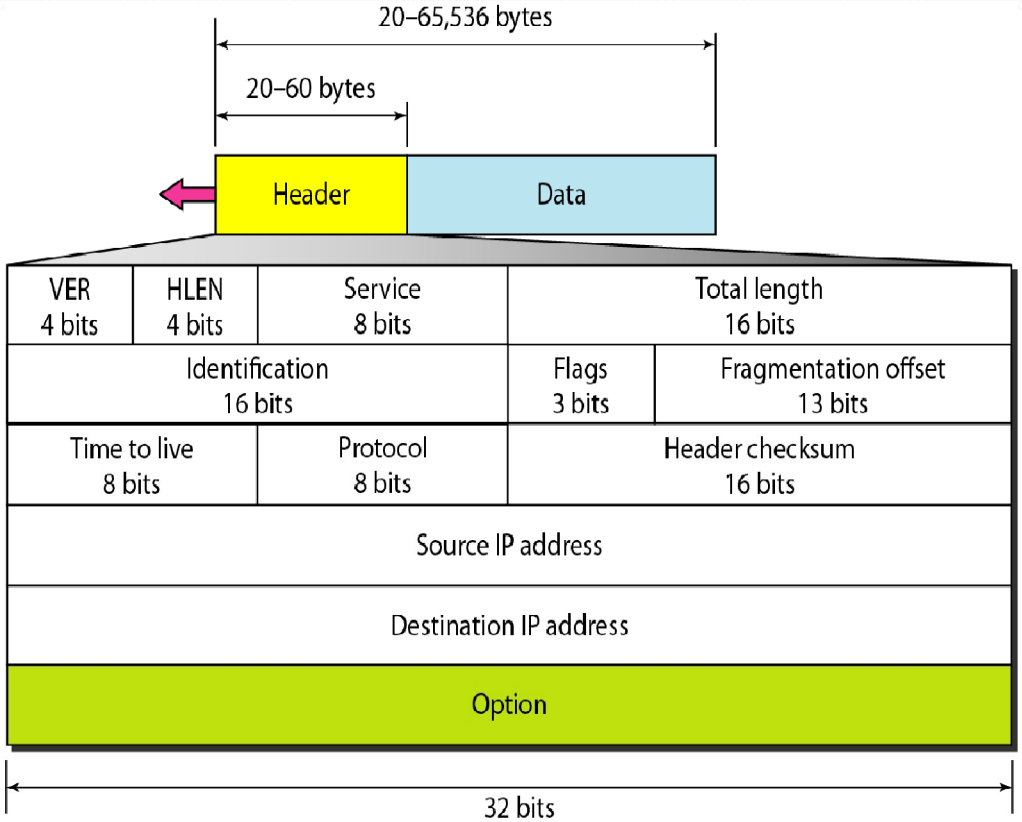
INTERNET PROTOCOL(IP)(Cont.)

- The number of addresses in the block can be found by using the formula 2^{32-n}.
- Each address in the block can be considered as a two-level hierarchical structure:
  the leftmost *n* bits (prefix) define the network;
- the rightmost 32 − n bits define the host.

ADDRESSES FOR PRIVATE NETWORKS

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

IPV4 DATAGRAM FORMAT

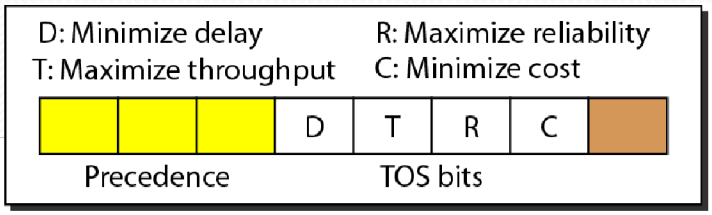


IPV4 DATAGRAM FORMAT

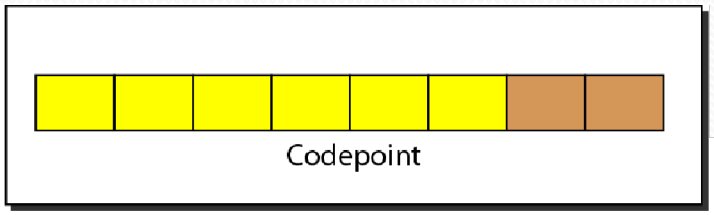
- **Version (VER):** This 4-bit field defines the version ofthe IPv4 protocol.
- **Header length (HLEN):**This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
- **Service Type:** In this interpretation, the first 3 bits are called precedence bits. The next 4 bits are called type of service (TOS) bits, and the last bit is not used.

SERVICE TYPE OR DIFFERENTIATED SERVICES

- **Differentiated Services:** In this interpretation, the first 6 bits make up the code point subfield, and the last 2 bits are not used. The codepoint subfield can be used in two different ways.
- When the 3 rightmost bits are Os, the 3 leftmost bits are interpreted the same as the precedence bits in the service type interpretation.
- When the 3 rightmost bits are not all Os, the 6 bits define 64 services based on the priority assignment by the Internet or local authorities.
- **Service type or differentiated services**



Service type



Differentiated services

DEFAULT TYPES OF SERVICE

Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

IPV4 DATAGRAM FORMAT

- **Total length:** This is a In-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. To find the length of the data coming from the upper layer, subtract the header length from the total length.

  Length of data=total length - header length

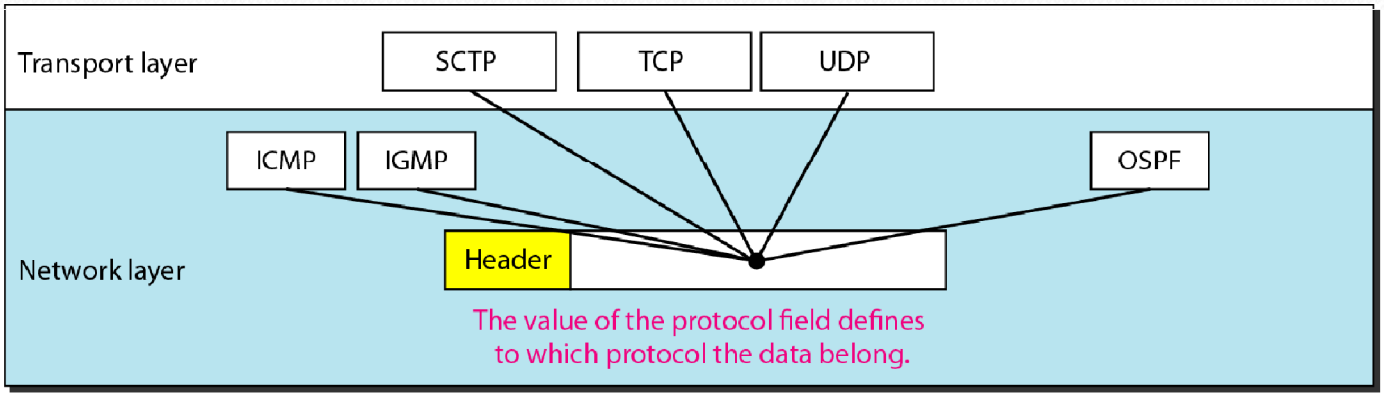
- **Time to live:** A datagram has a limited lifetime in its travel through an internet. This field was originally designed to hold a timestamp, which was decremented by each visited router. The datagram was discarded when the value became zero.

VALUES FOR CODEPOINTS

Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

IPV4 DATAGRAM FORMAT

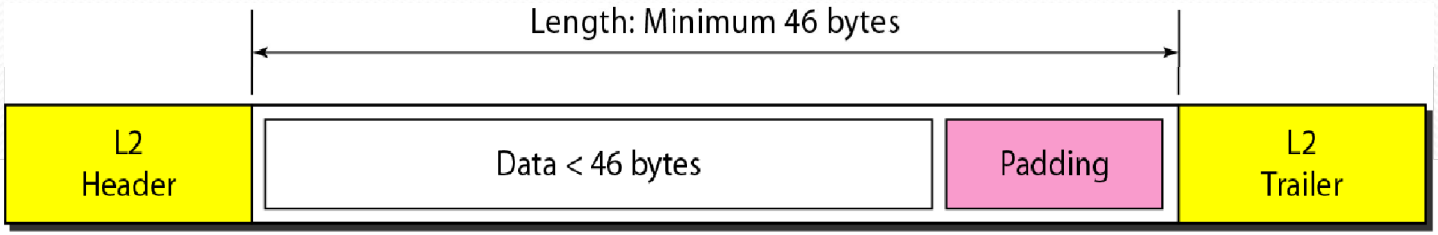
- **protocol field and encapsulated data:** This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IPv4 datagram is delivered.



Encapsulation of a small datagram in an ethernet frame

- **Fragmentation**
- A datagram can travel through different networks. Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size ofthe received frame depend on the protocol used by the physical network through which the frame has just traveled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.

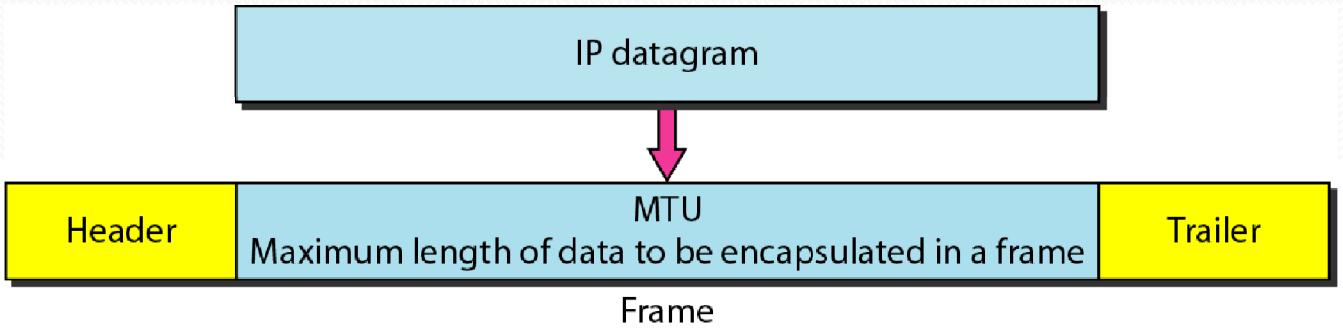
ENCAPSULATION OF A SMALL DATAGRAM IN AN ETHERNET FRAME



Maximum Transfer Unit (MTU)

- **Maximum Transfer Unit (MTU):** Each data link layer protocol has its own frame format in most protocols. One of the fields defined in the format is the maximum size of the data field. In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network. The value of the MTU depends on the physical network protocol

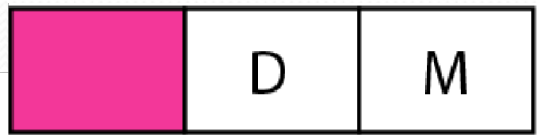
IPV4 DATAGRAM FORMAT



IPV4 DATAGRAM FORMAT

- **Identification :** This 16-bit field identifies a datagram originating from the source host. The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host.
- **Flags used in fragmentation**
- This is a 3-bit field. The first bit is reserved. The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If its value is 0, the datagram can be fragmented if necessary. The third bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment .

Flags used in fragmentation

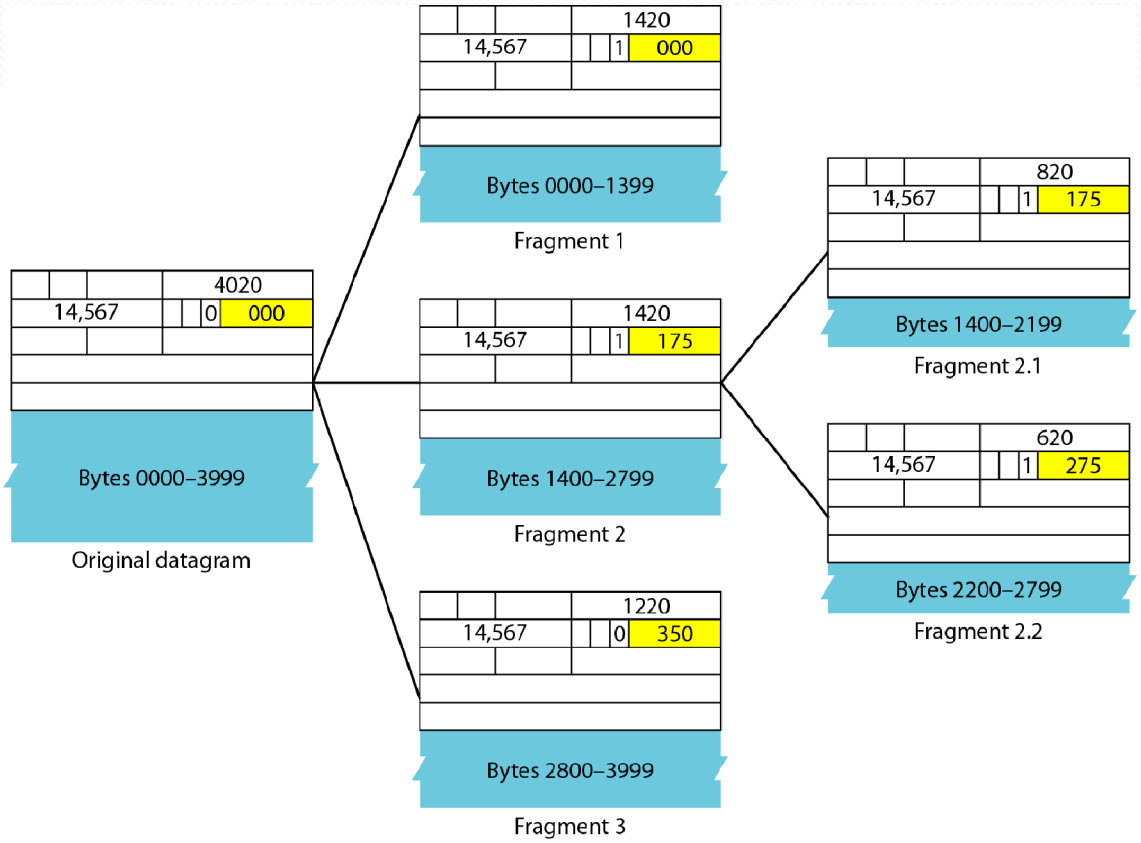


D: Do not fragment
M: More fragments

IPV4 DATAGRAM FORMAT

- **Fragmentation offset.** This 13-bit field shows the relative position of this fragment with respect to the whole datagram. It is the offset of the data in the original datagram measured in units of 8 bytes.

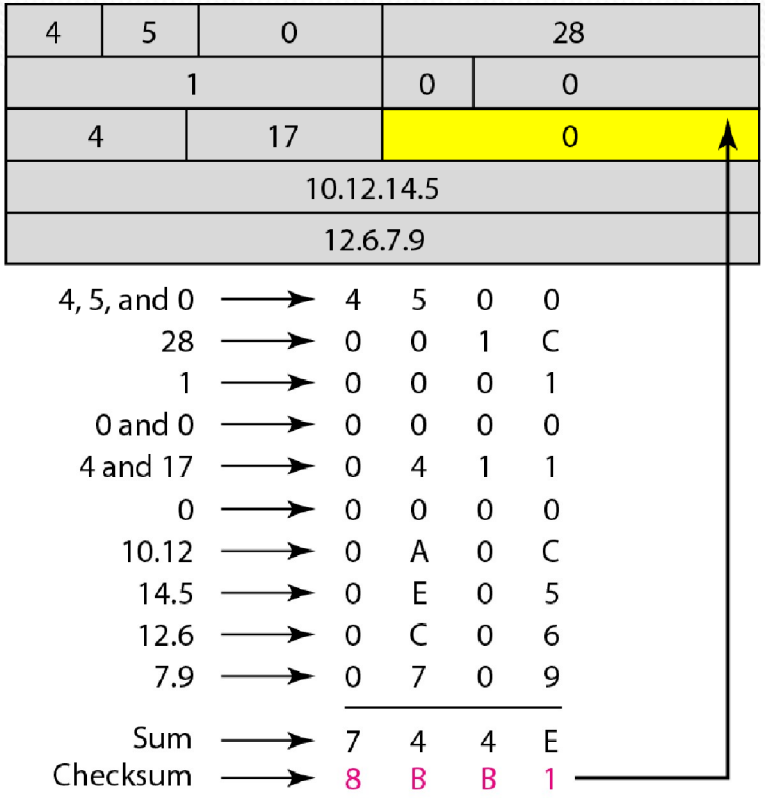
DETAILED FRAGMENTATION EXAMPLE



IPV4 DATAGRAM FORMAT

- **Checksum** : It is used to detect if there is any error in the header of IP datagram. It detects the error by attaching the checksum to the data at the sender and by adding all the segments including checksum at the receiver. If it is zero, then there is no error during transmission.

EXAMPLE OF CHECKSUM CALCULATION IN IPV4



IPV4 DATAGRAM FORMAT

- **Source address**: This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.
- **Destination address**: This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.
- **IP Options:** This field is optional. It is included for network testing and debugging.
- **Padding:** It represents bits containing zero that may be needed to ensure that the datagram header extends to an exact multiple of 32 bits.

Internet service provider (ISP)

- **An Internet service provider (ISP)** is an organization that provides services for accessing or using the Internet. The ISP is equipped with all tools and technologies to provide access to the Internet services. The connection to ISP can be made over a telephone line, leased line or wireless/radio link connections.
- They offer various services:
- Internet Access
- Domain name registration
- Dial-up access
- Leased line access
- **ISP Types**
- ISPs can broadly be classified into five categories as follows:

Internet service provider (ISP)

- **Access providers**
- They provide access to internet through telephone lines, cable wi-fi or fiber optics.
- **Mailbox Provider**
- Such providers offer mailbox hosting services.
- **Hosting ISPs**
- Hosting ISPs offers e-mail, and other web hosting services such as virtual machines, clouds etc.
- **Virtual ISPs**
- Such ISPs offer internet access via other ISP services.
- **Free ISPs**
- Free ISPs do not charge for internet services.

Factors for choosing the right ISP

- **1.Type of connection:**

  There are two primary types of internet service. Standard (also known as High Speed or broadband service) and High Availability service. The first group includes options like cable and DSL and typically offer higher speeds, but lower quality and reliability of service. This option is significantly cheaper in most cases. The High Availability class of services provides a Service Level Agreement for uptime that usually exceeds 99.99% or approximately 2 hours of downtime per year. These connections include Fiber Optic connections .According to our requirement of dependency on an internet connection, we can choose the Service.

Factors for choosing the right ISP(Cont.)

- 2.**Speed:**

  It is very important to ensure that we have enough speed for everyday use, including peak times (such as large meetings or training evolutions). when choosing an ISP, it's necessary to ensure they can provide the speeds we need. Based on our location, and the type of Internet access we are looking for (i.e. Fiber vs Fixed Wireless vs DSL etc) bandwidth availability may fluctuate from carrier to carrier.

  3.Availability: While it would be ideal to have access to High Availability Fiber Optic, not every business has this option. Even the availability of cable and DSL internet can be limited in new construction areas where lines of service have yet to be established. In these cases, it may take up to 6 months for construction and installation of service.

Factors for choosing the right ISP(Cont.)

- **4.Redundancy:**
  In cases when the need to be continually connected is extreme and you cannot afford even one or two minutes of downtime, you want to secure some level of redundancy. Redundancy is a fail over internet connection that switches in the event your main line has gone down. This is more common with standard internet service, but can be important to have even with High Availability services with SLAs if a business cannot afford a moment of downtime.
- **5.Cost:**
  High Availability service comes with a high price tag and depending on the types of connections and service area – the price can be significant. As an example, a client that was quoted one High Availability fiber connection for $1000 per month for 20MB of service. Conversely, two diverse broadband connections (one cable at 100MB and one Broadband Fiber at 50MB) came in at only $400 per month – more speed, better availability for less cost. The service costs from your ISP will vary widely depending upon a number of factors.
-

Factors for choosing the right ISP(Cont.)

- **6. Customer Support:**
- While in an ideal world , businesses would never have to engage with their ISP past service installation, Whether a client has billing questions, service issues, needs technical support, has upgrade inquiries or product add-ons, at some point or another, chances are a business will have to engage with an ISP's customer support team. Therefore, research what type of support the company offers.
- A larger carrier, for example, might make you sit through an automated phone menu, place you on a lengthy hold, and eventually transfer you to a contracted employee outside of the U.S. Alternatively, a medium sized ISP, such as GeoLinks, offers 24/7 in-house customer support; customers are even able to ask for customer support reps by name.
- Another element to consider is overall responsiveness. If your business does experience a technical issue, how long does it take a provider to respond and address the issue? Time is money, so whether it be hours wasted on hold, or weeks waiting on a repair, how an ISP handles customer relations directly affects its business customer's bottom line.

Factors for choosing the right ISP(Cont.)

- **7. Agility and Flexibility**
- As a business grows and changes, its overall telecom needs will change as well. For example, if a law firm hires 10 more associates, they will likely need to upgrade their overall bandwidth. Furthermore, if juggling multiple carriers and multiple bills becomes too large of a strain on a company's accounting apartment, a business may wish to streamline all their telecom needs with a single carrier.
- Some ISPs offer additional services such as VoIP and SD-WAN, while others do not. Therefore, when selecting an ISP, make sure to explore their entire product suite and offerings. Choosing an aggregator, (an ISP that is capable of reselling multiple ISP products and services) such as GeoLinks, ensures that no matter the growth or changes in a business, a single provider will be able to upgrade and adapt to evolving business needs.

Factors for choosing the right ISP(Cont.)

- 8. **Personal disk space:**

  ISP s also provide desk space to your PC for the purpose of keeping your mails. The total size of your mail should not exceed the space reserved.

- 9. **Application Services Offered:**
- Also enquire about the various application services like email, FTP,news groups and online chat services offered by the ISPs .

DOMAIN NAME SYSTEMS(DNS)

- There are several applications in the application layer of the Internet model that follow the client/server paradigm. The client/server programs can be divided into two categories: those that can be directly used by the user, such as e-mail, and those that support other application programs. The Domain Name System (DNS) is a supporting program that is used by other programs such as e-mail.
- When the Internet was small, mapping was done by using a host file. The host file had only two columns: name and address. Every host could store the host file on its disk and update it periodically from a master host file.
- Today, however, it is impossible to have one single host file to relate every address with a name and vice versa. Another solution, the one used today, is to divide this huge amount of information into smaller parts and store each part on a different computer. In this method, the host that needs mapping can contact the closest computer holding the needed information. This method is used by the Domain Name System (DNS).

DOMAIN NAME SYSTEMS(DNS)

Name Space: To be unambiguous, the names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses .

Flat Name Space:

In a flat name space, a name is assigned to an address. A name in this space is a sequence of characters without structure. The main disadvantage of a fiat name space is that it cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication.

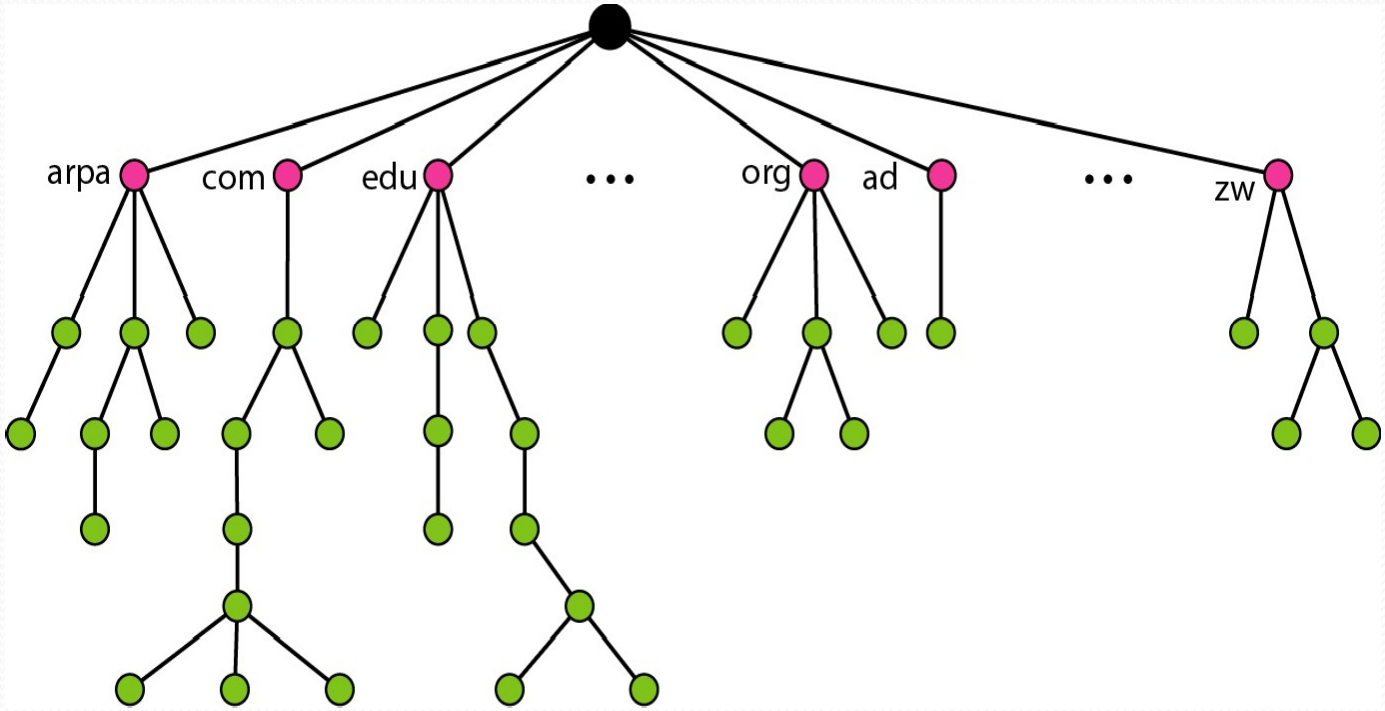
Hierarchical Name Space:

In a hierarchical name space, each name is made up of several parts. The first part can define the nature of the organization, the second part can define the name of an organization, the third part can define departments in the organization, and so on. In this case, the authority to assign and control the name spaces can be decentralized. A central authority can assign the part of the name that defines the nature of the organization and the name of the organization. The responsibility of the rest of the name can be given to the organization itself.

Domain Name Space

- **Domain Name Space:**To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127.

DOMAIN NAME SPACE



DOMAIN NAMES AND LABELS

- **Label**

  Each node in the tree has a label, which is a string with a maximum of 63 characters. The root label is a null string (empty string). DNS requires that children of a node (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.

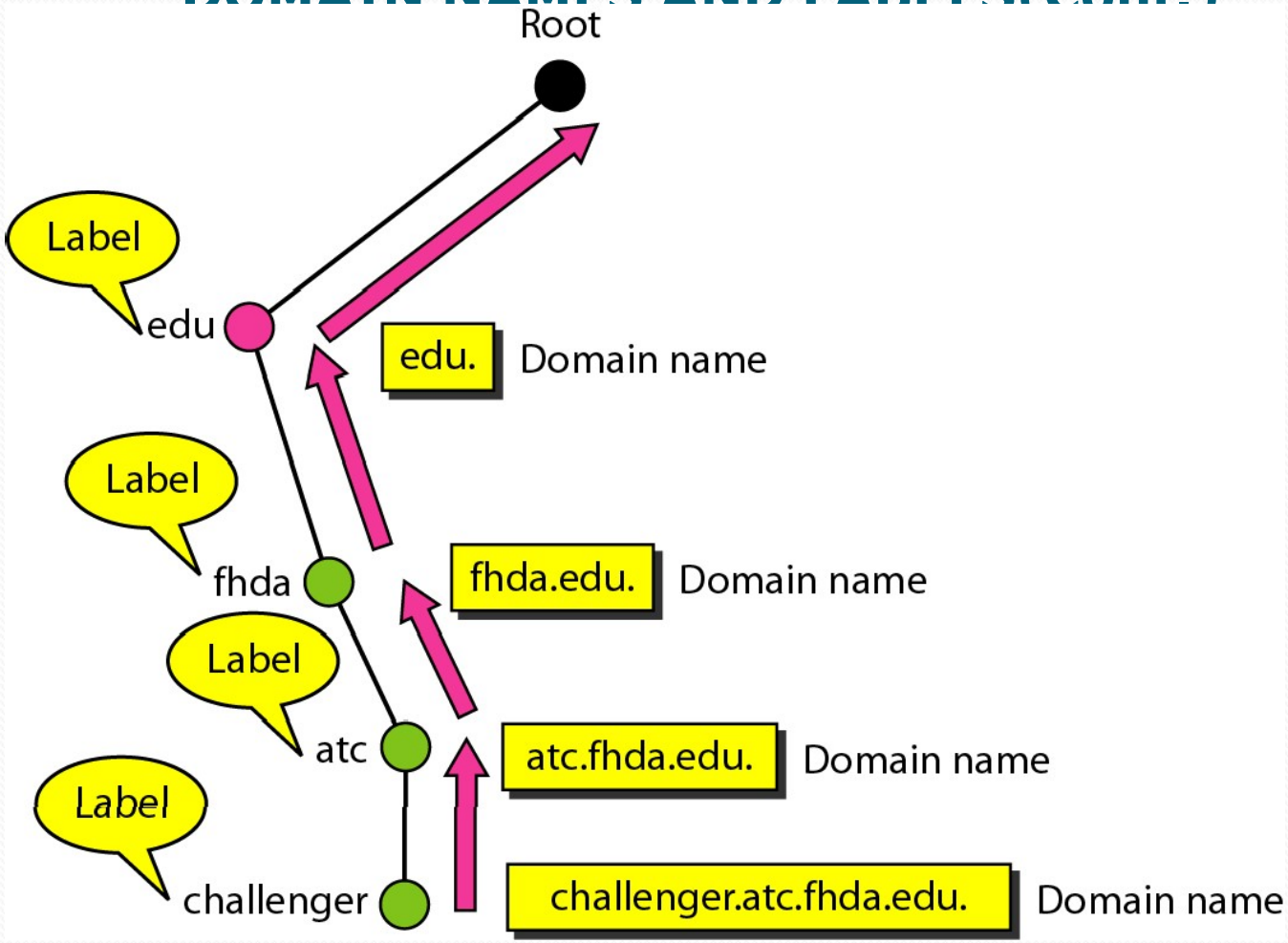
- **Domain Name**

  Each node in the tree has a domain name. A full domain name is a sequence of labels separated by dots (.). The domain names are always read from the node up to the root. The last label is the label ofthe root (null). This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing, called a fully qualified domain name (FQDN). An FQDN is a domain name that contains the full name of a host that uniquely define the name of the host.

  For example, the domain name

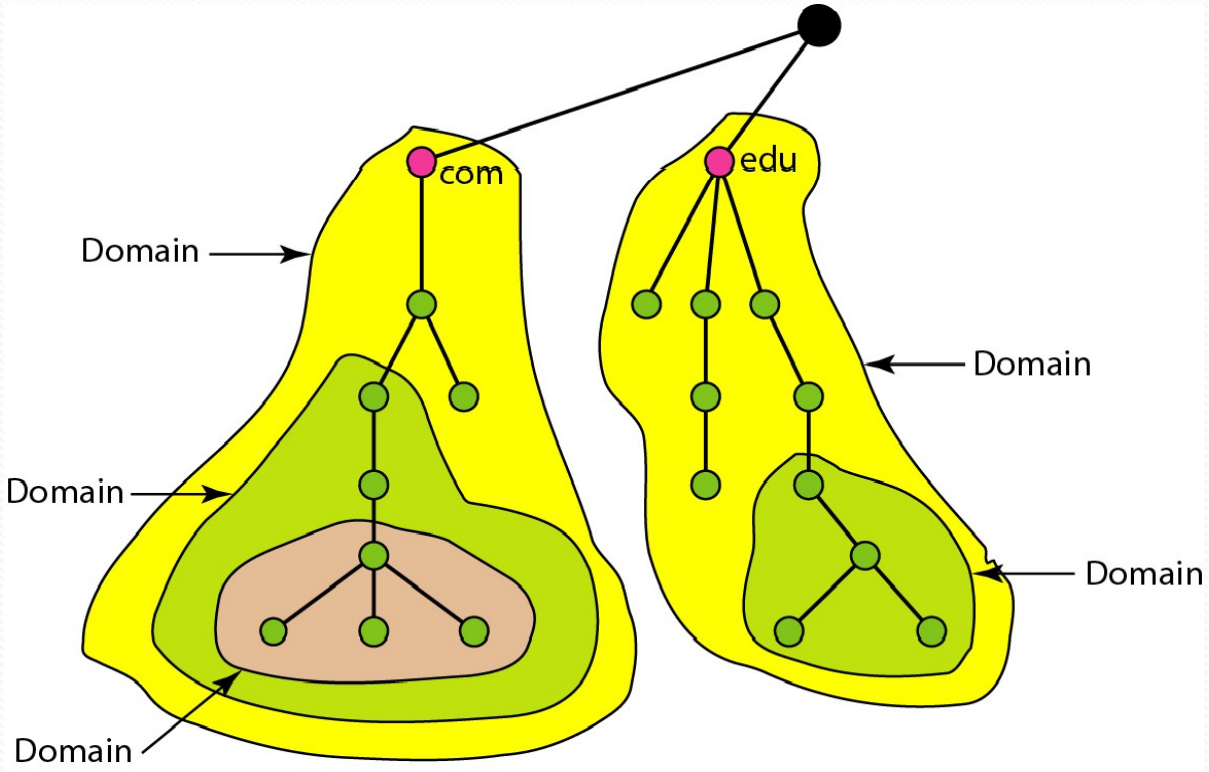
  challenger.ate.tbda.edu.

DOMAIN NAMES AND LABELS(Cont.)



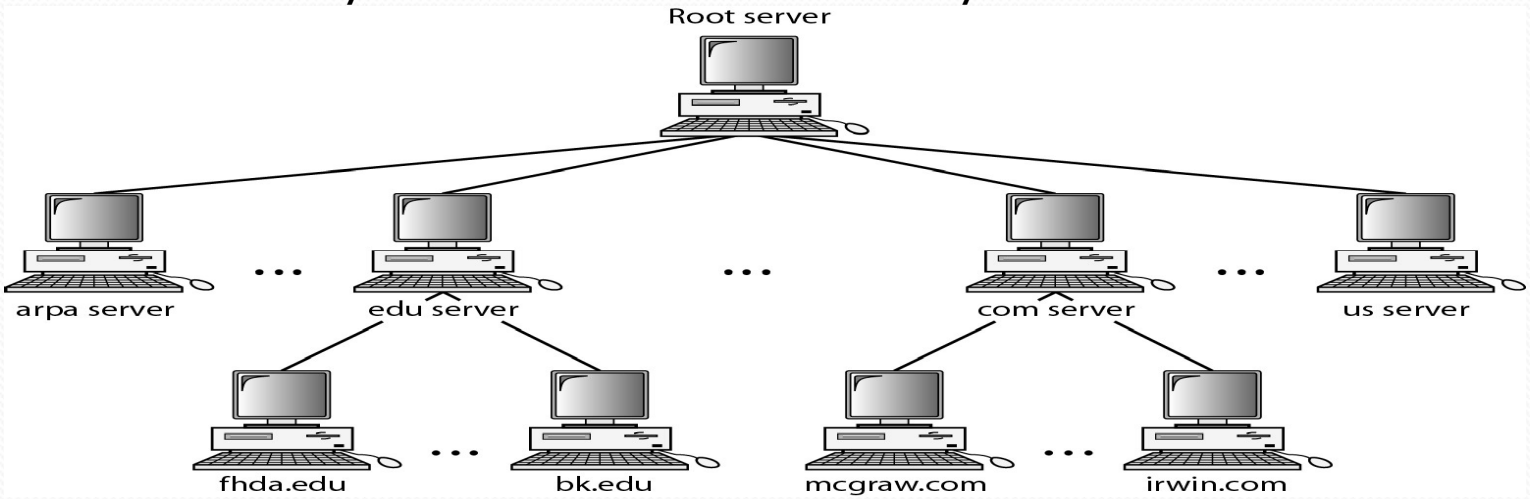
DOMAINS

A domain is a subtree of the domain name space. The name of the domain is the domain name of the node at the top of the subtree.



DISTRIBUTION OF NAME SPACE

- The information contained in the domain name space must be stored. However, it is very inefficient and also unreliable to have just one computer store such a huge amount of information.
- **Hierarchy of name servers:** we have a hierarchy of servers in the same way that we have a hierarchy of names.

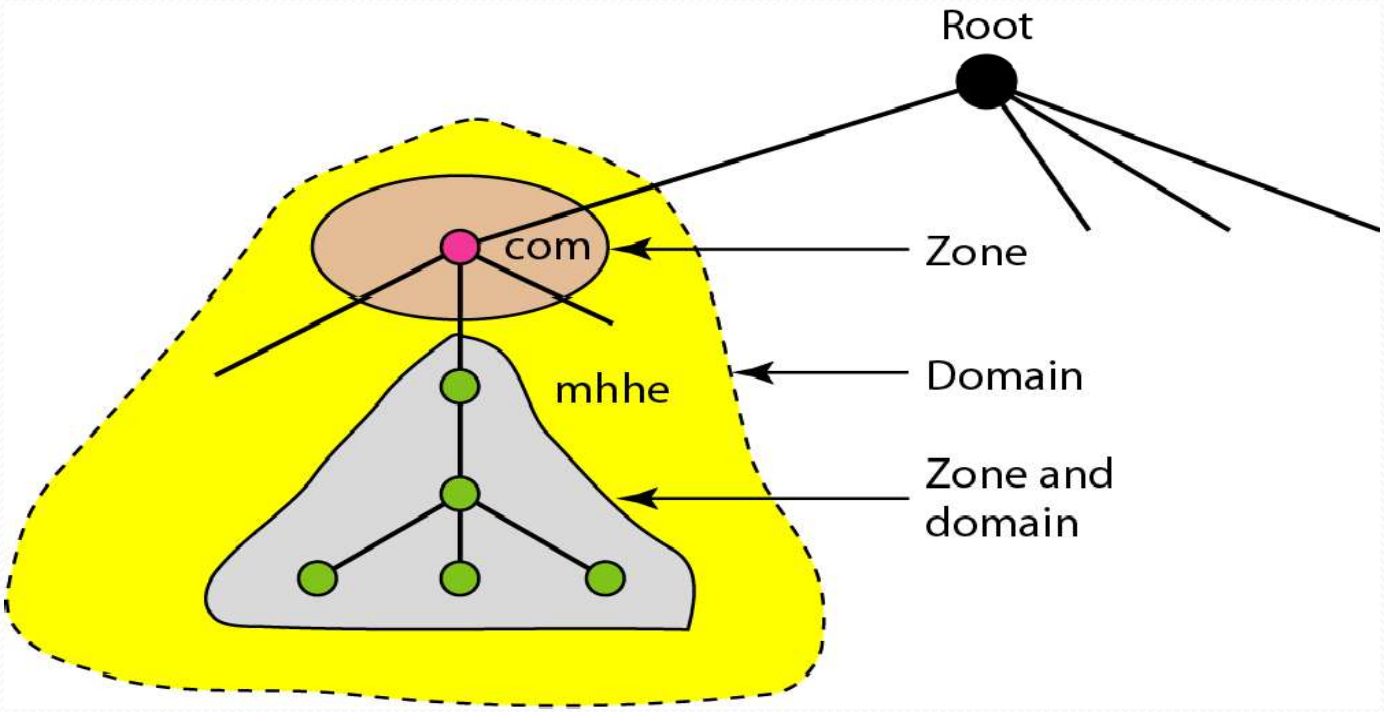


ZONES AND DOMAINS

- The server makes a database called a zonefile and keeps all the information for every node under that domain. The information about the nodes in the subdomains is stored in the servers at the lower levels, with the original server keeping some sort of reference to these lower-level servers. In this case, its zone is made of detailed information for the part of the domain that is not delegated and references to those parts that are delegated.

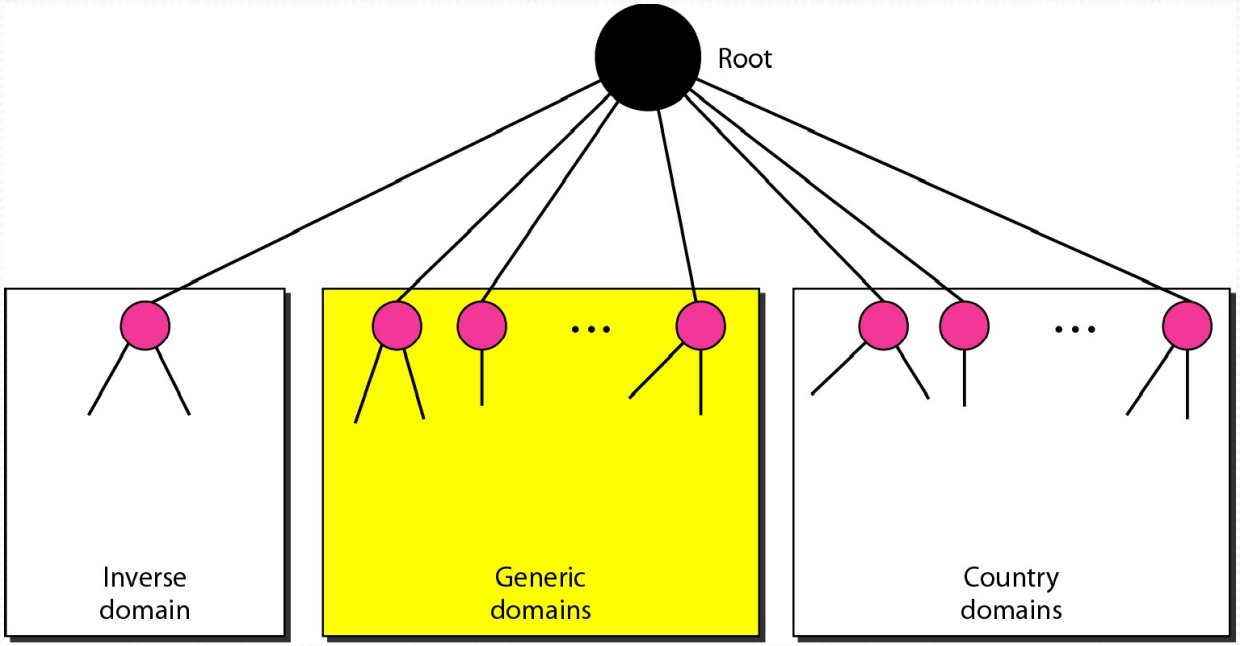
- A root server is a server whose zone consists of the whole tree. A root server usually does not store any information about domains but delegates its authority to other servers, keeping references to those servers.
- A primary server is a server that stores a file about the zone for which it is an authority. It is responsible for creating, maintaining, and updating the zone file. It stores the zone file on a local disk
- A secondary server is a server that transfers the complete information about a zone from another server (primary or secondary) and stores the file on its local disk. The secondary server neither creates nor updates the zone files
- When the secondary downloads information from the primary, it is called zone transfer.

ZONES AND DOMAINS



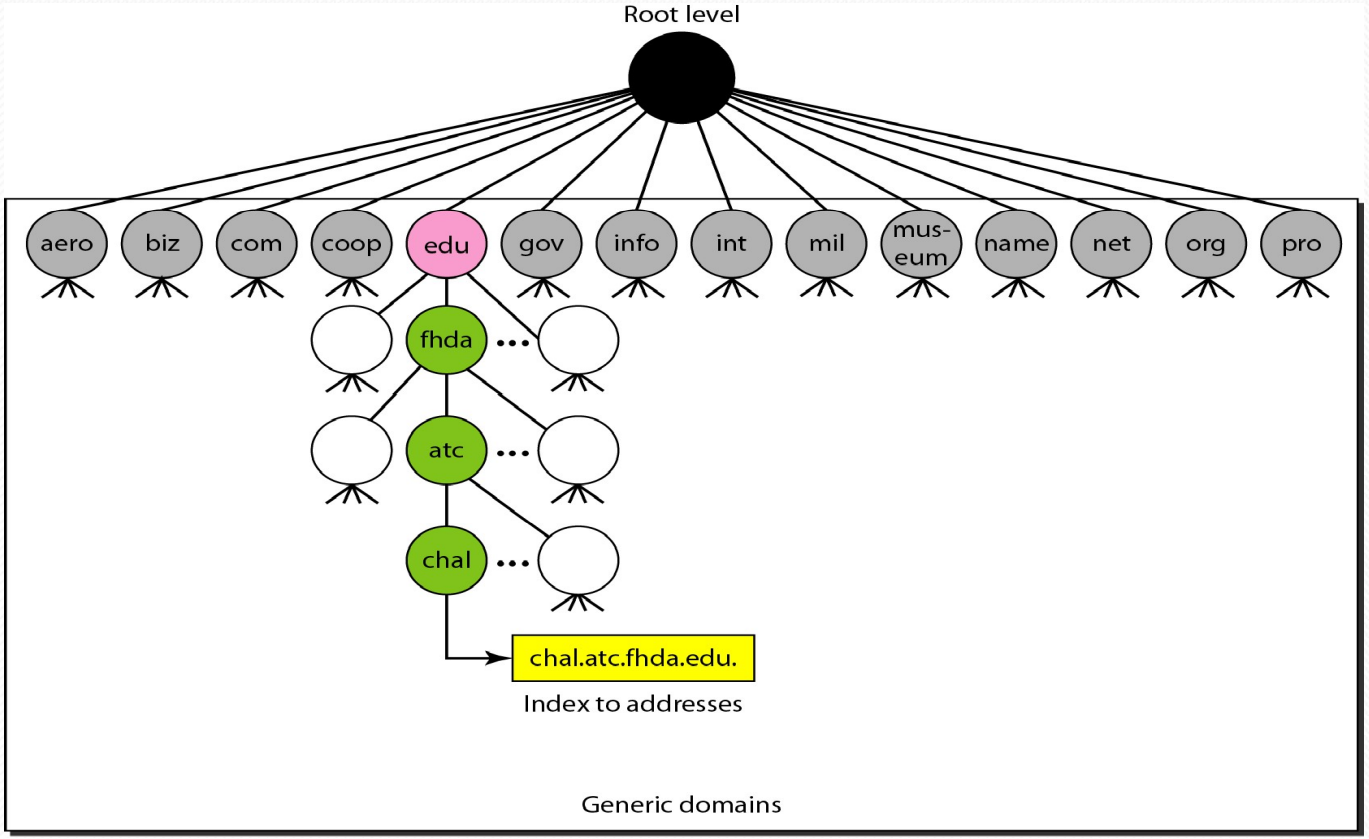
DNS IN THE INTERNET

- DNS is a protocol that can be used in different platforms. In the Internet, the domain name space (tree) is divided into three different sections: generic domains, country domains, and the inverse domain.



GENERIC DOMAINS

The generic domains define registered hosts according to their generic behavior. Each node in the tree defines a domain, which is an index to the domain name space database

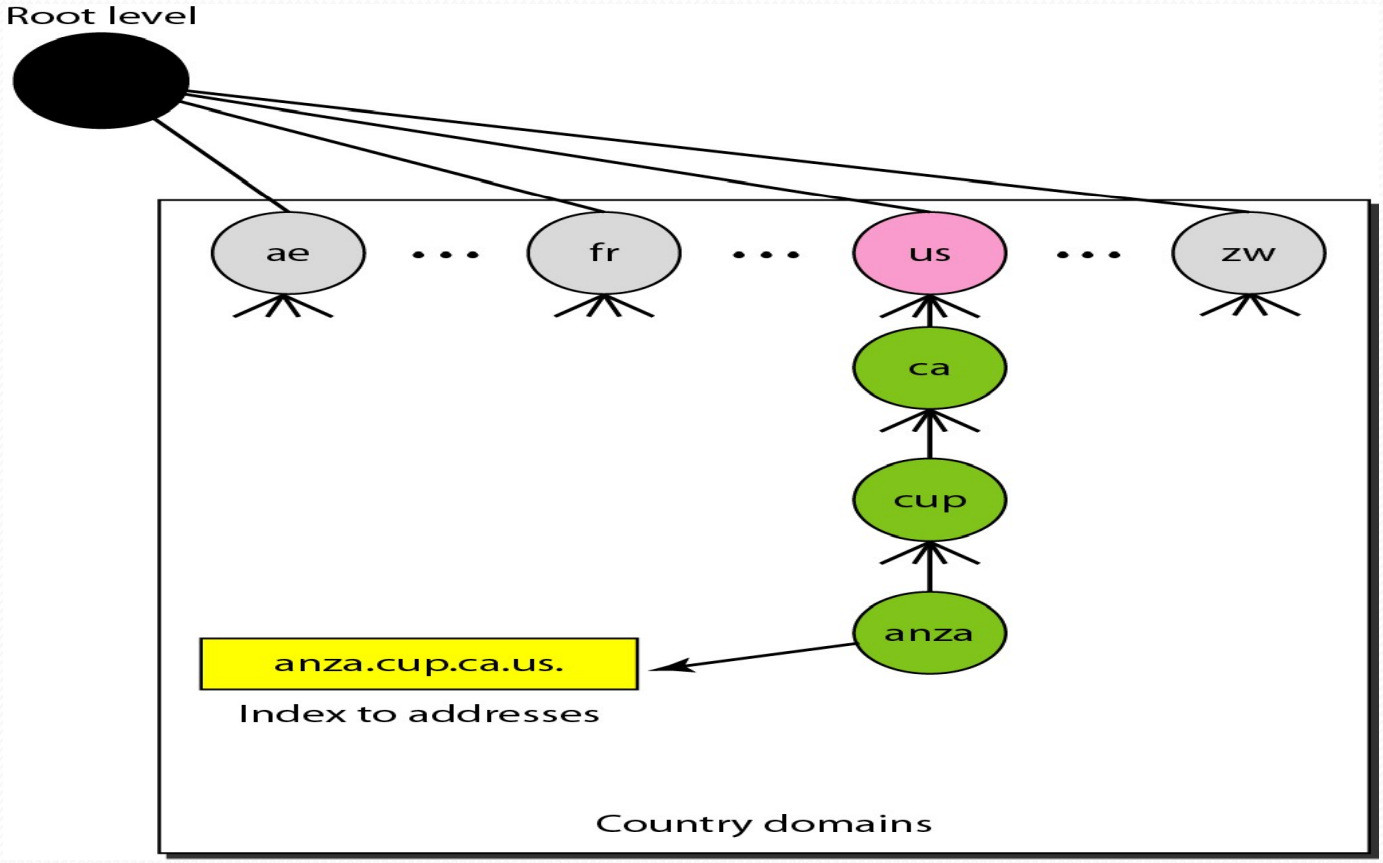


GENERIC DOMAIN LABELS

Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

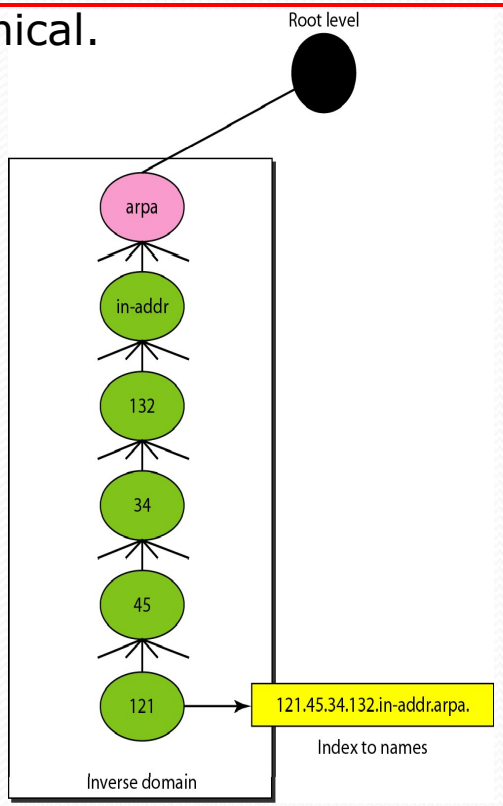
COUNTRY DOMAINS

The country domains section uses two-character country abbreviations (e.g., us for United States). Second labels can be organizational, or they can be more specific, national designations



INVERSE DOMAIN

The inverse domain is used to map an address to a name.
This type of query is called an inverse or pointer (PTR) query. To handle a pointer query, the inverse domain is added to the domain name space with the first-level node called arpa (for historical reasons). The second level is also one single node named in-addr (for inverse address). The rest ofthe domain defines IP addresses. The servers that handle the inverse domain are also hierarchical.



RESOLUTION

Mapping a name to an address or an address to a name is called name-address resolution.

- **RESOLVER:**

  DNS is designed as a client/server application. A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver. The resolver accesses the closest DNS server with a mapping request. If the server has the information, it satisfies the resolver; otherwise, it either refers the resolver to other servers or asks other servers to provide the information. After the resolver receives the mapping, it interprets the response to see if it is a real resolution or an error, and finally delivers the result to the process that requested it.

RESOLUTION(Cont.)

- **MAPPING NAMES TO ADDRESSES**

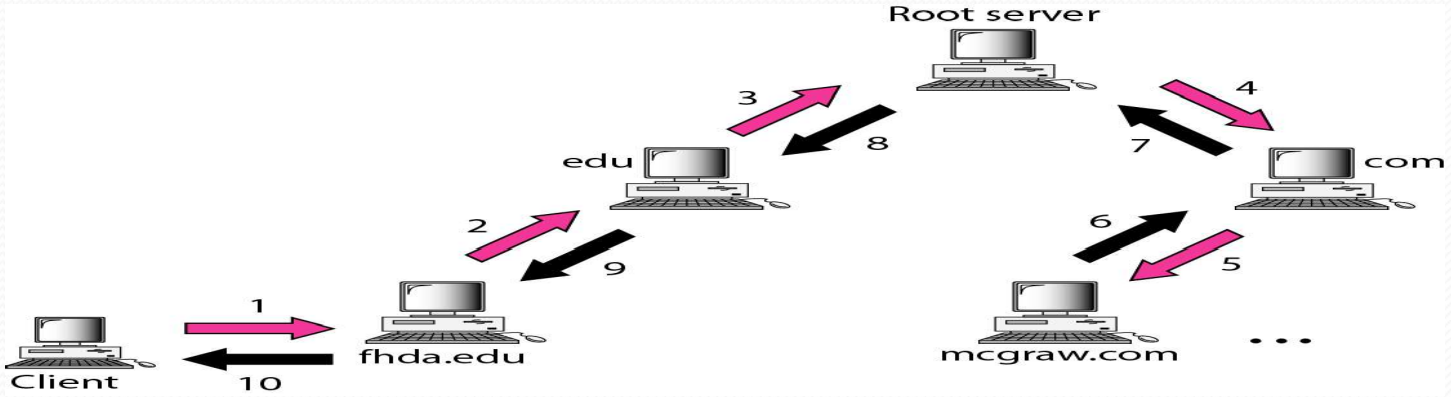
  Most of the time, the resolver gives a domain name to the server and asks for the corresponding address. In this case, the server checks the generic domains or the country domains to find the mapping. If the domain name is from the generic domains section, the resolver receives a domain name such as "chal.atc.jhda.edu.". The query is sent by the resolver to the local DNS server for resolution. If the local server cannot resolve the query, it either refers the resolver to other servers or asks other servers directly.

- **MAPPING ADDRESSES TO NAMES**

  A client can send an IP address to a server to be mapped to a domain name. To answer queries of this kind, DNS uses the inverse domain. However, in the request, the IP address is reversed and the two labels in-addr and arpa are appended to create a domain acceptable by the inverse domain section. For example, if the resolver receives the IP address 132.34.45.121, the resolver first inverts the address and then adds the two labels before sending. The domain name sent is "121.45.34.132.in-addr.arpa." which is received by the local DNS and resolved.

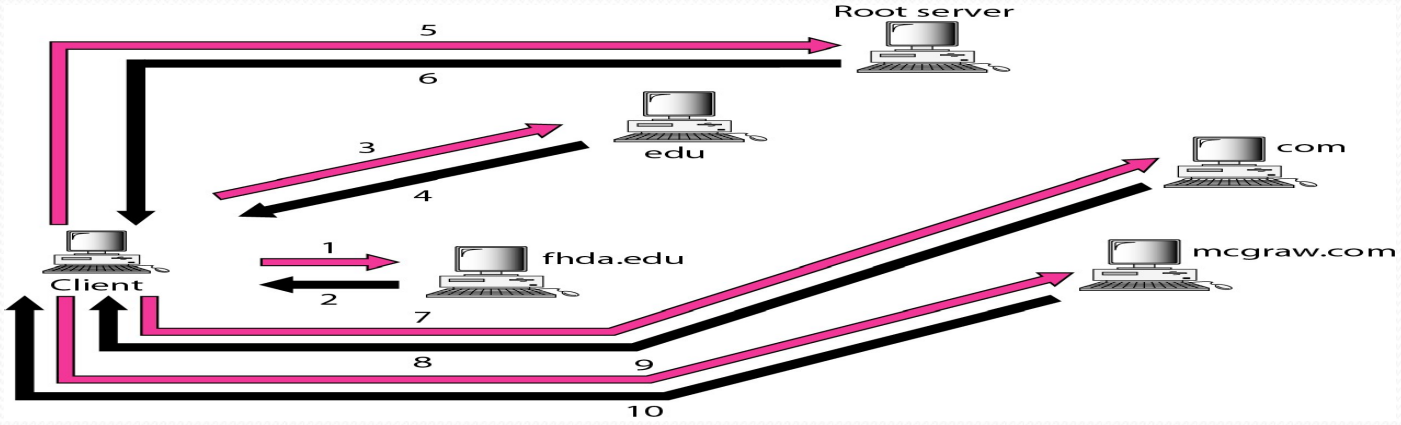
RESOLUTION

- **Recursive Resolution:** The client (resolver) can ask for a recursive answer from a name server. This means that the resolver expects the server to supply the final answer. Ifthe server is the authority for the domain name, it checks its database and responds. Ifthe server is not the authority, it sends the request to another server (the parent usually) and waits for the response. If the parent is the authority, it responds; otherwise, it sends the query to yet another server. When the query is finally resolved, the response travels back until it finally reaches the requesting client. This is called recursive resolution.



RESOLUTION(Cont.)

- **Iterative Resolution:** If the client does not ask for a recursive answer, the mapping can be done iteratively. If the server is an authority for the name, it sends the answer. Ifit is not, it returns (to the client) the IP address of the server that it thinks can resolve the query. The client is responsible for repeating the query to this second server. If the newly addressed server can resolve the problem, it answers the query with the IP address; otherwise, it returns the IP address of a new server to the client. Now the client must repeat the query to the third server. This process is called iterative resolution because the client repeats the same query to multiple servers.



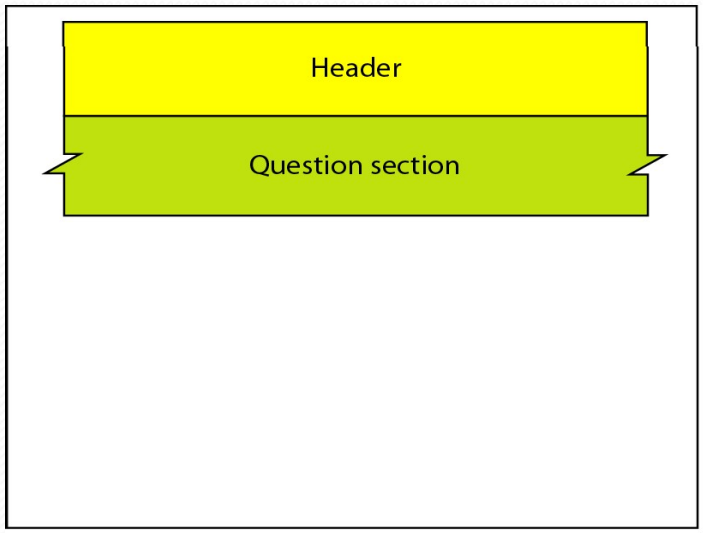
RESOLUTION(Cont.)

- **CACHING**

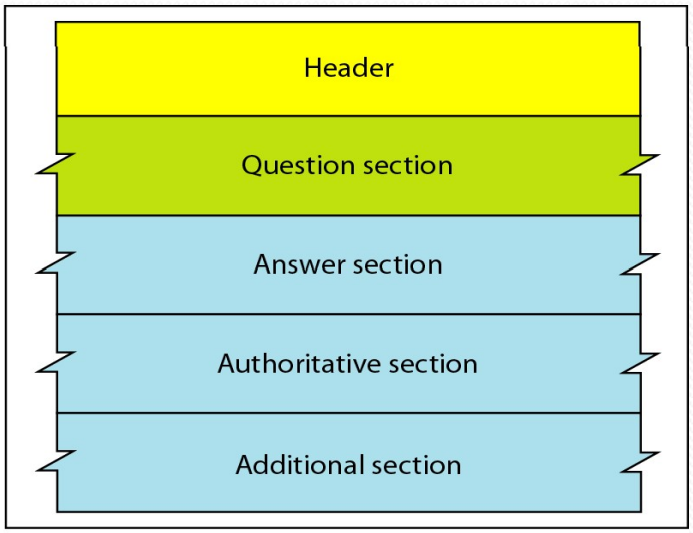
  Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address. Reduction of this search time would increase efficiency. DNS handles this with a mechanism called caching. When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client. If the same or another client asks for the same mapping, it can check its cache memory and solve the problem. Caching speeds up resolution, but it can also be problematic. If a server caches a mapping for a long time, it may send an outdated mapping to the client. To counter this, information to the mapping called time-to-live (TTL) is added. After the expiry of the time, the mapping is invalid .

DNS MESSAGES

- DNS has two types of messages: query and response.. Both types have the same format. The query message consists of a header and question records; the response message consists of a header, question records, answer records, authoritative records, and additional records.



a. Query



b. Response

HEADER FORMAT

Identification	Flags
Number of question records	Number of answer records (all 0s in query message)
Number of authoritative records (all 0s in query message)	Number of additional records (all 0s in query message)

DOMAIN NAME SYSTEMS(DNS)(Cont.)

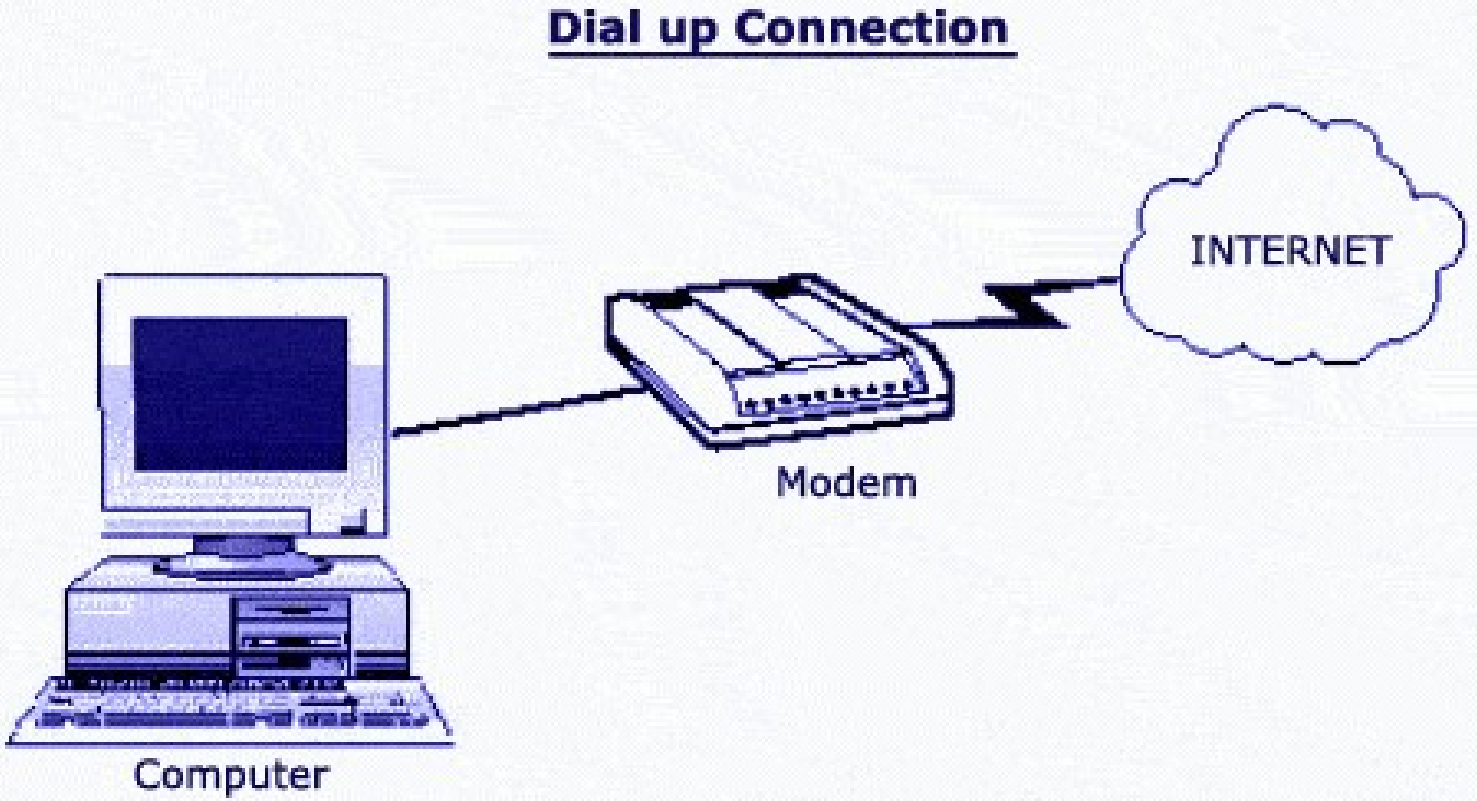
- Two types of records are used in DNS. The question records are used in the question section of the query and response messages. The answer records are used in the answer, authoritative, and additional information sections of the response message.

- The DNS master file must be updated dynamically. The Dynamic Domain Name System (DDNS), therefore was devised to respond to this need. In DDNS, when a binding between a name and an address is determined, the information is sent, usually by DHCP to a primary DNS server. The primary server updates the zone. The secondary servers are notified either actively or passively.

Dial Up Connection

- The technology most often used to access internet services is dialup networking. Most ISPs offer this kind of telephone-based service. To use dialup access, a computer must have a modem that connects to the phone lines. The modem is known as one type of data communication equipment. Once properly configured, it instructs the modem to call to number provided by the ISP. At the ISP end there exists another modem, which answers the call and agrees to send Internet packets.
- Dial-Up Line is any telecommunications link that is serviced by a modem. Dial-up lines are ordinary phone lines used for voice communication, while dedicated or leased lines are digital lines with dedicated circuits. Dial-Up Lines connect the modem to the internet. Dial-up lines are generally much less expensive to use, but they have less available bandwidth.

Dial Up Connection(Cont.)



Dial Up Connection(Cont.)

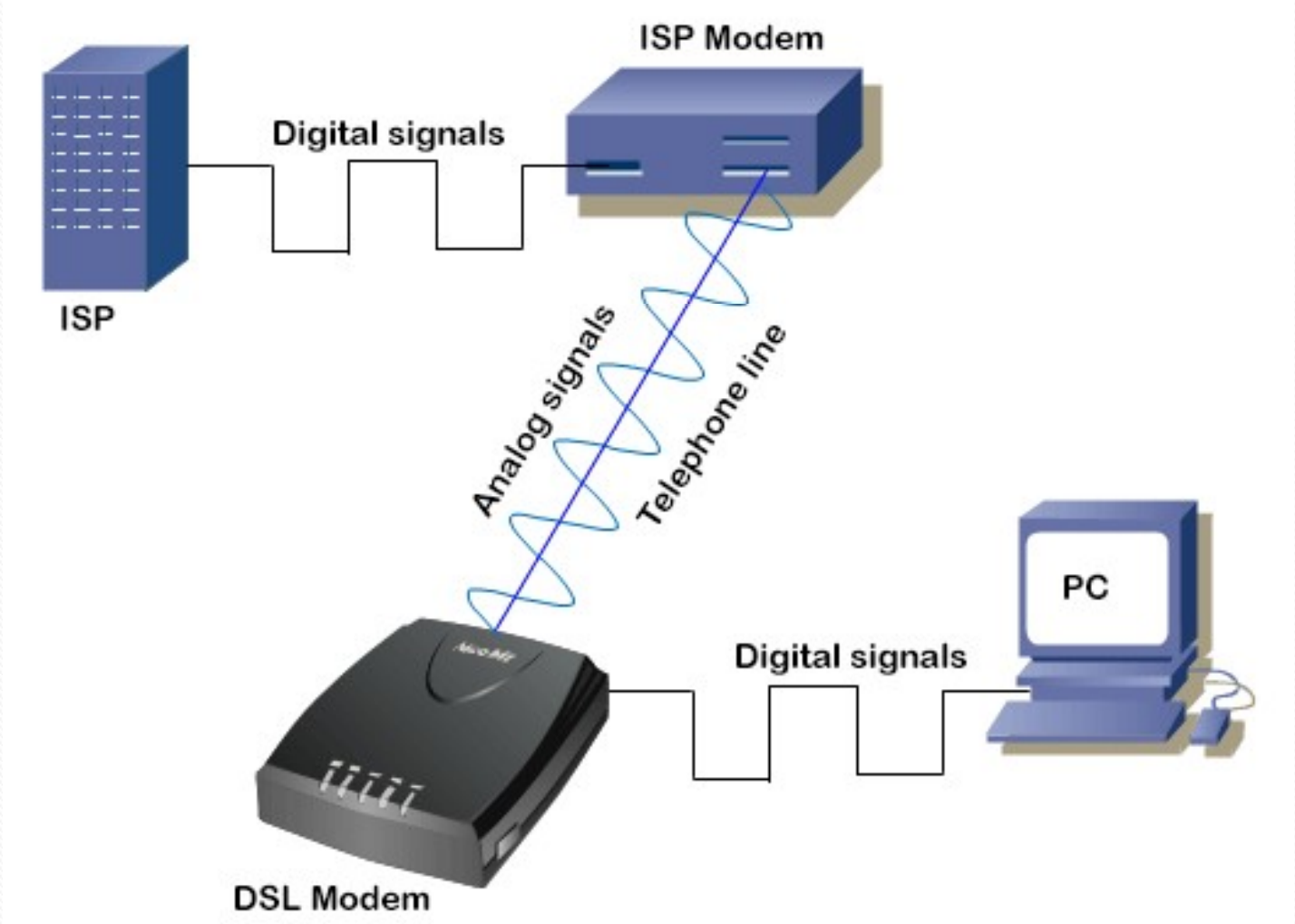
- A dedicated access has more bandwidth and instant connection to the net. In the dialup access there is a tedious procedure of establishing the connection to the web through modem dialing. The user has to wait for modem to dial the required number and wait for ISP's response every time he/she wishes to logon to the net. Once ISP's modem and user's modem gets synchronised then only the user can start browsing through another application software called web browser.

- In dialup connection the user dials the number provided by the ISP

MODEM (MODULATOR-DEMODULATOR)

- A modem (short form of modulator-demodulator) is a device, which is used to convert digital signals to analog signals so that they can be transferred over the standard telephone line. At the receiving end another modem is connected which reconverts the analog signals back to the digital signals. Digital signals are converted to analog signals by the first modem so that information can be transferred over analog telecommunication lines. At the receiving end, it is reconverted by the second modem to digital signals so that the message is available in its original form. In order to connect to the Internet, you have to first connect your computer system with a modem, which in turn helps to establish a connection to the Internet with the help of telephone lines.

MODEM (MODULATOR-DEMODULATOR)(Cont.)



MODEM (MODULATOR-DEMODULATOR)(Cont.)

- **Modem is abbreviation for Modulator – De-modulator.** Modems are used for data transfer from one computer network to another computer network through telephone lines. The computer network works in digital mode, while analog technology is used for carrying massages across phone lines.
- **Modulator** converts information from **digital mode to analog mode** at the transmitting end and de-modulator converts the same from **analog to digital at receiving end**. The process of converting analog signals of one computer network into digital signals of another computer network so that they can be processed by a receiving computer is **referred to as digitizing.**
- When an analog facility is used for data communication between two digital devices called Data Terminal Equipment (DTE), modems are used at each end. DTE can be a terminal or a computer.
- The modem at the transmitting end converts the digital signal generated by DTE into an analog signal by modulating a carrier. This modem at the receiving end demodulates the carrier and hand over the demodulated digital signal to the DTE.

MODEM (MODULATOR-DEMODULATOR)(Cont.)

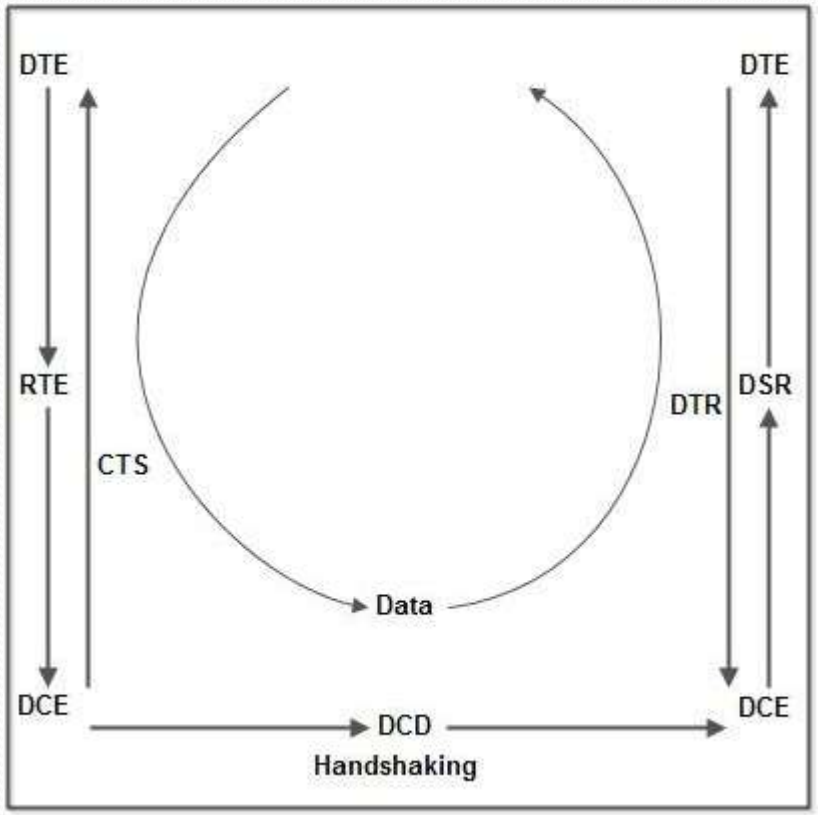
- The transmission medium between the two modems can be dedicated circuit or a switched telephone circuit. If a switched telephone circuit is used, then the modems are connected to the local telephone exchanges. Whenever data transmission is required connection between the modems is established through telephone exchanges.

MODEM (MODULATOR-DEMODULATOR)(Cont.)

- **Ready to Send**

- To begin with the Data Terminal Equipment or DTE (better known as a computer) sends a Ready To Send or RTS signal to the Data Communication Equipment or DCE (better known as a modem). This is sometimes known as a wakeup call and results in the modem sending a Data Carrier Detect or DCD signal to the receiving modem. There then follows a series of signals passed between the two until the communication channel has been established. This process is known as handshaking and helps to explain why, even now, some companies like CompuServe use the symbol of two hands grasping each other to mean being on-line. Of course, after that all it takes is for the second modem to send a Data Set Ready or DSR signal to its computer and wait for the Data Terminal Ready or DTR reply. When that happens the first modem sends a Clear To Send or CTS signal to the computer that started the whole process off and data can then be transmitted.

MODEM (MODULATOR-DEMODULATOR)(Cont.)



Types of Modems

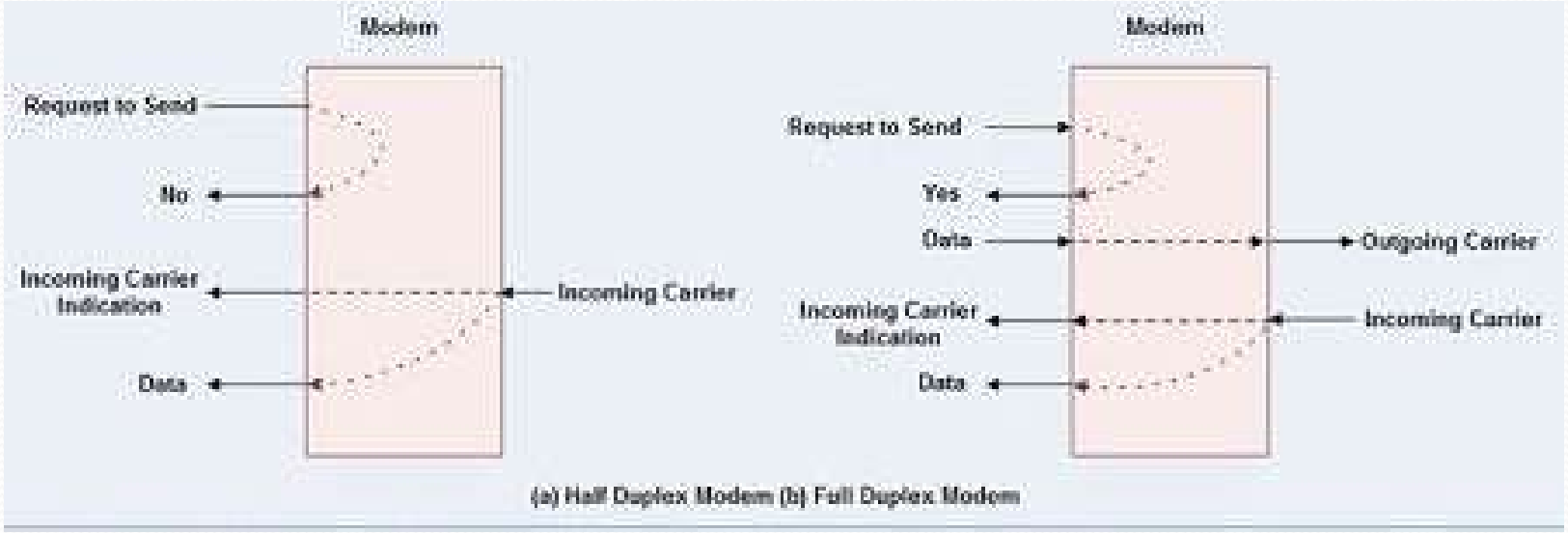
- Categorization is usually based on the following basic modem features:
- 1. Directional capacity: half duplex modem and full duplex modem.
- 2. Connection to the line: 2-wire modem and 4-wire modem.
- 3. Transmission mode: asynchronous modem and synchronous modem.
- **Half duplex**
- 1. A **half duplex modem** permits transmission in one direction at a time.
- 2. If a carrier is detected on the line by the modem, It gives an indication of the incoming carrier to the DTE through a control signal of its digital interface.
- 3. As long as the data is being received; the modem does not give permission to the DTE to transmit data.

Half duplex and Full duplex Modems

- **Full duplex**

- A **full duplex modem** allows simultaneous transmission in both directions.
- Therefore, there are two carriers on the line, one outgoing and the other incoming.

Half duplex and Full duplex Modems



2-Wire and 4-wire Modems

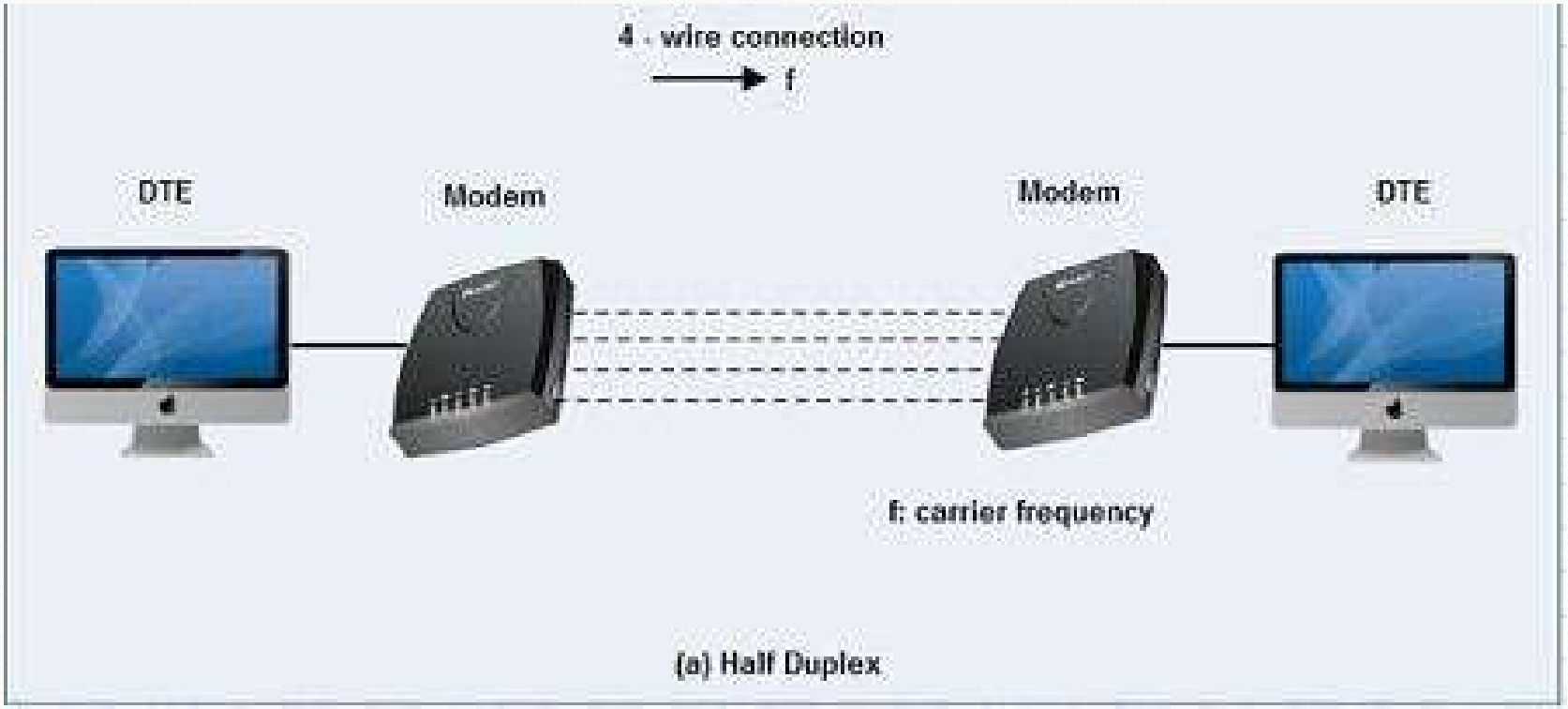
- In a 4-wire connection, one pair of wires is used for the outgoing carrier and the other pair is used for incoming carrier.
- Full duplex and half duplex modes of data transmission are possible on a 4- wire connection.
- As the physical transmission path for each direction is separate, the same carrier frequency can be used for both the directions.

2-Wire and 4-wire Modems

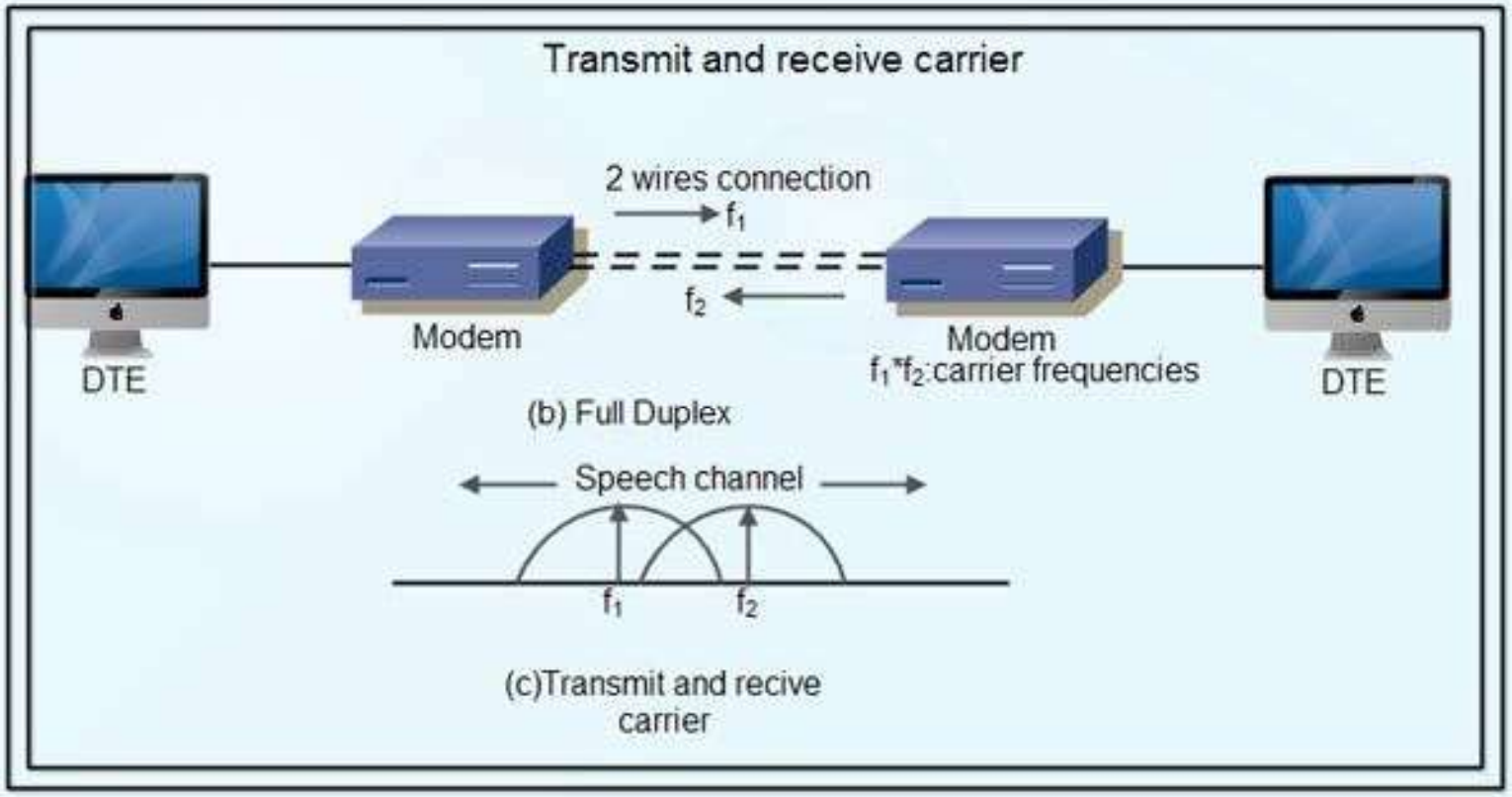
2-wire Modem

- 2-wire modems use the same pair of wires for outgoing and incoming carriers. A leased 2-wireconnection is usually cheaper than a 4-wire connection as only one pair of wires is extended to the subscriber's premises.The data connection established through telephone exchange is also a 2-wire connection.
- In 2-wire modems, half duplex mode of transmission that uses the same frequency for the incoming and outgoing carriers can be easily implemented.
- For full duplex mode of operation, it is necessary to have two transmission channels, one for transmit direction and the other for receive direction.
- This is achieved by frequency division multiplexing of two different carrier frequencies. These carriers are placed within the bandwidth of the speech channel.

2-Wire and 4-wire Modems



2-Wire and 4-wire Modems



Asynchronous & Synchronous Modems

- **Asynchronous Modem**

• Asynchronous modems can handle data bytes with start and stop bits.

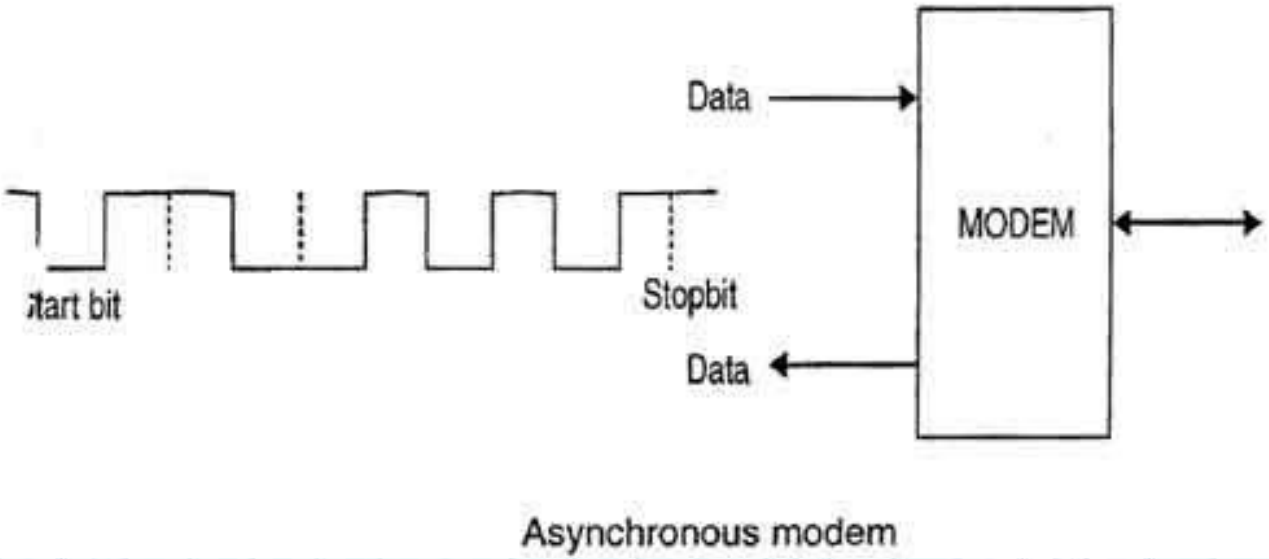
• There is no separate timing signal or clock between the modem and the DTE.

• The internal timing pulses are synchronized repeatedly to the leading edge of the start pulse

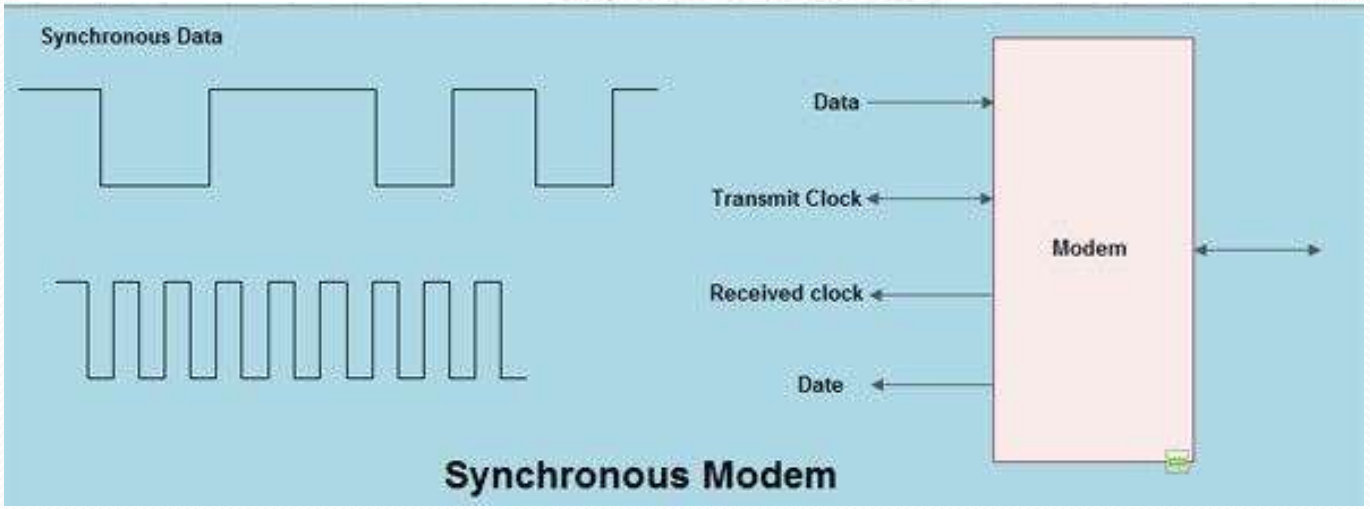
Asynchronous & Synchronous Modems(Cont.)

- **Synchronous Modem**
- Synchronous modems can handle a continuous stream of data bits but requires a clock signal.
- The data bits are always synchronized to the clock signal.
- There are separate clocks for the data bits being transmitted and received.
- For synchronous transmission of data bits, the DTE can use its internal clock and supply the same to the modem.

Asynchronous & Synchronous Modems(Cont.)



Asynchronous modem



NEWER TECHNOLOGIES

1.Cable modem:

- A ***cable modem is a digital modem that sends and receives digital data over the cable television (CATV) network.*** It makes use of the already laid cables meant for TV viewing. A cable modem has a small electronic box that connects customer's computer to the cable system. In addition to the cable modem at each customer's site, the cable company needs cable modems at its end. The modems carry the data traffic over the cable TV's coaxial lines without interfering with other TV channels. This is made possible by using FDM (Frequency Division Multiplexing) technique (that is how several TV channels coexist on a single coaxial cable).
- They are faster than dialup connection.
- Provides continuous and instant connection.
- Cheaper than leased lines.
- No extra wiring is needed.
- As the number of users grow, there is a performance penalty.

NEWER TECHNOLOGIES

2. **Asymmetric Digital Subscriber Line (ASDL)**

- Asymmetric Digital Subscriber Line was invented to provide high-speed internet access over the existing telephone lines. ASDL should not be confused with dialup access because the former does not use modem. Instead, it uses only the wiring. These telephone wires carry digital signals without affecting the telephone signals and vice versa.
- Uses existing telephone wires.
- Allows simultaneous use of Internet and phone
- ADSL provides high data rates comparable with that of cable modem.
- Each user has separate pair of wires and thus no sharing of bandwidth.
- Continuous and instant connection.
- Cheaper than leased lines.

NEWER TECHNOLOGIES

3. **Wireless technology**

- To provide internet access to remote areas, engineers have developed wireless access technology. They use same technology as cell phone but need not dial a number to access the Internet. The transmitter runs all the time and thus providing continuous and instant access. More over wireless technology offers high data transfer rates like cable modem and ADSL.

NEWER TECHNOLOGIES

Network Devices

- Cable Modem
  - A type of modem that provides access to a data signal sent over the cable television infrastructure primarily used to deliver broadband Internet access

- DSL Modem
  - Digital Subscriber Line
  - DSL or xDSL, is a family of technologies that provide digital data transmission over the wires of a local telephone network

- Wireless Access Point (AP)
  - A device that connects wireless communication devices together to form a wireless network, usually connects to a wired network to relay data between wireless devices and wired devices
  - Eliminates need to string cables and provides users with greater mobility

FACTORS TO BE CONSIDERED WHILE BUYING A MODEM

- While buying modems the following factors are to be taken into account :

(a) Transmission speed

(b) Data compression schemes

(c) Error Correction Protocols

(d) Type of Modem, i.e., Internal vs. External

Transmission Speed

- Transmission speed is the speed with which the data is transmitted. It is measured in bits per second (bps). Modems come in different speeds like 300 bps, 1200 bps, 2400 bps, 4800 bps, 9600 bps, 14,400 bps (14.4 kbps) and 28,800 bps (28.8 kbps). The faster the transmission speed of the modem, higher will be its cost ,as data are transferred at faster speeds. This implies that if the transmission channels permit these speeds then the modem will attain that speed, otherwise it will depend on the speed of the media. These days modems of speeds 28.8 kbps, 33.6 kbps, and 56 kbps are gaining popularity.

Data Compression Schemes

- Since voluminous data are to be transferred, data has to be compressed. In order to bring about standardization of the compressed codes generated by different modems, various standards have evolved.
- V.32 standard has achieved a transmission speed of 9,600 bps.
- V.32 b transmits data at a speed of 14,400 kbps.
- V.34 standard allows a transmission speed of upto 28,800 bps.
- V.42 provides four-fold data compression.

Error Correction Protocols

- Since data travels over telephone lines many errors can be introduced in the signal because of noise, which also travels in waves along with the data. Therefore, error correction protocols are used to free data from errors. Some popular systems are MNP (Microcom Networking Protocol) and V. 42. Examples of error-correction protocols of MNP are MNP2, MNP3, MNP4. V.42 is a standard for error correction based on Link Access Procedure for Modem (LAPM) standards.
- These standards are available in all modems so that the user is not troubled.

Basic Types of Modems

- **Internal** - A modem card that you can plug into an expansion slot on the motherboard. It is advisable to remove the telephone line when not used

Internal Modem

- **External** - Connected to the PC through a cable, which is plugged into serial port on the back of the system unit.

External Modem

THANK YOU