MODULE-1

COMPUTER NETWORKS & PROTOCOLS (BEC702)

COMPUTER NETWORKS & PROTOCOLS			
Course Code	BEC702	CIE Marks	50
Hours / Week	03	Exam Hours	03
Total Hours	40	Exam Marks	50
CREDITS 04			

Text book:

1) Behrouz A Fourouzan, “Data Communication and Networking”, 5th Edition McGraw Hill, 2013, ISBN:1-25-906475-3.

Reference text Book:

1) James J Kurose, Keith W Ross, “Computer Networks”, Pearson Education.
2) Wayne Tomasi, “Introduction to Data Communication and Networking”, Pearson Education.
3) Andrew S tanenbaum, “Computer Networks”, Prentice Hall.
4) William Stallings, “Data and Computer Communications”, Prentice Hall.

Module No.	Contents	Teaching Hour
1	**Introduction:** Data communication: Components, Data representation, Data flow, Networks: Network criteria, Physical Structures, Network types: LAN, WAN, Switching, The Internet.. **Network Models:** TCP/IP Protocol Suite: Layered Architecture, Layers in TCP/IP suite, Description of layers, Encapsulation and Decapsulation, Addressing, Multiplexing and Demultiplexing, The OSI Model: OSI Versus TCP/IP. **Data-Link Layer:** Introduction: Nodes and Links, Services, Two Categories' of link, Sublayers, Link Layer addressing: Types of addresses, ARP (1.1,1.2, 1.3.1to 1.3.4,2.2, 2.3 ,9.1, 9.2.1, 9.2.2)	8
2	**Data Link Control (DLC) services:** Framing, Flow and Error Control. **Media Access Control:** Random Access: ALOHA, CSMA, CSMA/CD, CSMA/CA. **Connecting Devices:** Hubs, Switches, Virtual LANs: Membership, Configuration, Communication between Switches, Advantages. **Wired and Wireless LANs:** Ethernet Protocol, Standard Ethernet. Introduction to wireless LAN: Architectural Comparison, Characteristics, Access Control. (11.1,12.1,13.1, 13.2.1 to 13.2.5,15.1,17.1,17.2)	8

3	Network Layer: Introduction, Network Layer services: Packetizing, Routing and Forwarding, Other services, Packet Switching: Datagram Approach, Virtual Circuit Approach, IPV4 Addresses: Address Space, Classful Addressing, Classless Addressing, DHCP, Network Address Resolution Network Layer Protocols: Internet Protocol (IP): Datagram Format, Fragmentation, Options, Security of IPv4 Datagrams. IPv6 addressing and Protocol. Unicast Routing: Introduction, Routing Algorithms: Distance Vector Routing, Link State Routing, Path vector routing. (18.1(excluding 18.1.3), 18.2, 18.4,19.1,20.1, 20.2,22.1 and 22.2)	**8**
4	Transport Layer: Introduction: Transport Layer Services, Connectionless and Connection oriented Protocols, Transport Layer Protocols: Simple protocol, Stop and wait protocol, Go-BackN Protocol, Selective repeat protocol, Piggybacking Transport-Layer Protocols in the Internet: User Datagram Protocol: User Datagram, UDP Services, UDP Applications, Transmission Control Protocol: TCP Services, TCP Features, Segment, Connection, State Transition diagram, Windows in TCP, Error control, TCP congestion control. (23.1, 23.2.1, 23.2.2, 23.2.3, 23.2.4, 23.2.5,24.2, 24.3.1, 24.3.2, 24.3.3, 24.3.4, 24.3.6, 24.3.8, 24.3.9)	**8**
5	Application Layer: Introduction: providing services, Application- layer paradigms, Standard Client Server Protocols: Hyper Text Transfer Protocol, FTP: Two connections, Control Connection, Data Connection, Electronic Mail: Architecture, Domain Name system: Name space, DNS in internet, Resolution, DNS Messages, Registrars, DDNS, security of DNS. Quality of Service (25.1, 26.1.2, 26.2, 26.3, 26.6, 30.1, 30.2.)	**8**

MODULE-1

Introduction: Data communication: Components, Data representation, Data flow, Networks: Network criteria, Physical Structures, Network types: LAN, WAN, Switching, The Internet..

Network Models: TCP/IP Protocol Suite: Layered Architecture, Layers in TCP/IP suite, Description of layers, Encapsulation and Decapsulation, Addressing, Multiplexing and Demultiplexing, The OSI Model: OSI Versus TCP/IP.

Data-Link Layer: Introduction: Nodes and Links, Services, Two Categories' of link, Sublayers, Link Layer addressing: Types of addresses, ARP

(1.1,1.2, 1.3.1to 1.3.4,2.2, 2.3 ,9.1, 9.2.1, 9.2.2)

Total Lecture Houres-08

DATA COMMUNICATIONS

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. The effectiveness of a data communications system depends on four fundamental characteristics:

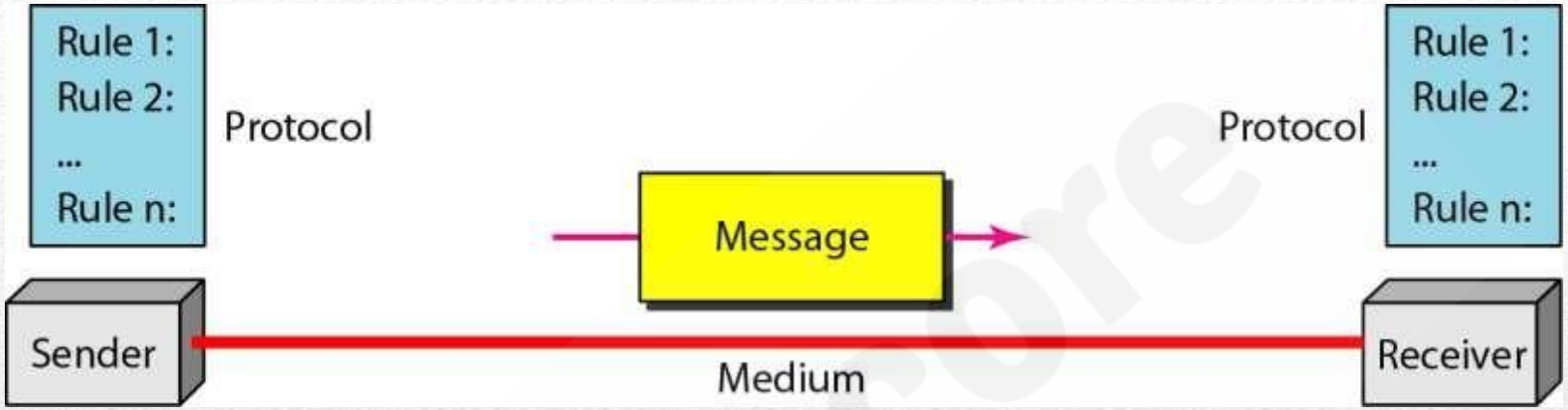
1. Delivery- The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy-The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. Timeliness- The system must deliver data in a timely manner. Late delivery of data is useless. Incase of video and audio timely delivering data as they are produced in the same order that they are produced and without significant delay. This kind of delivery is called real time transmission.

4. Jitter.-Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of the packets.

Components



1. **Message: The Message is the information to be communicated. Forms of information text, numbers, pictures, audio, video.**
2. **Sender: The sender is the device that sends data message. Eg: Computer, telephone handset, video camera**
3. **Receiver: The receiver is the device that receives message. Eg: Computer, telephone handset, video camera, television.**
4. **Transmission Medium: It is the physical path through which a message travels from sender to receiver.**
5. **Protocol: It is a set of rules that govern data communications. It represents an agreement between the communicating devices.**

Data Representation

- ***Text :*** *It is represented as bit patterns. Different set of bit patterns are designed to represent the bit patterns. Each set is called code and the process of representing symbols is called coding.*
- ***Numbers:*** *It is represented as bit patterns. Number is converted to binary number to simplify mathematical operations.*
- ***Images:*** *It is represented as bit patterns. Image is composed of matrix of pixels, where each pixel is a dot. Size of the pixel depends on the resolution. RGB (RED, Green, Blue) method is used to represent color image. In YCM (Yellow, Cyan, Magenta) method*

Data Representation

- ***Audio:*** *It refers to recording or broadcasting of sound or music. It is continuous, not discrete.*
- ***Video:*** *It refers to the recording or broadcasting of picture or movie. It can be produced as continuous entity (TV Camera) or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion*

Data Flow

Simplex

- Communication is unidirectional.
- Only one of the two devices on a link can transmit.
- Eg: Keyboards, monitor.

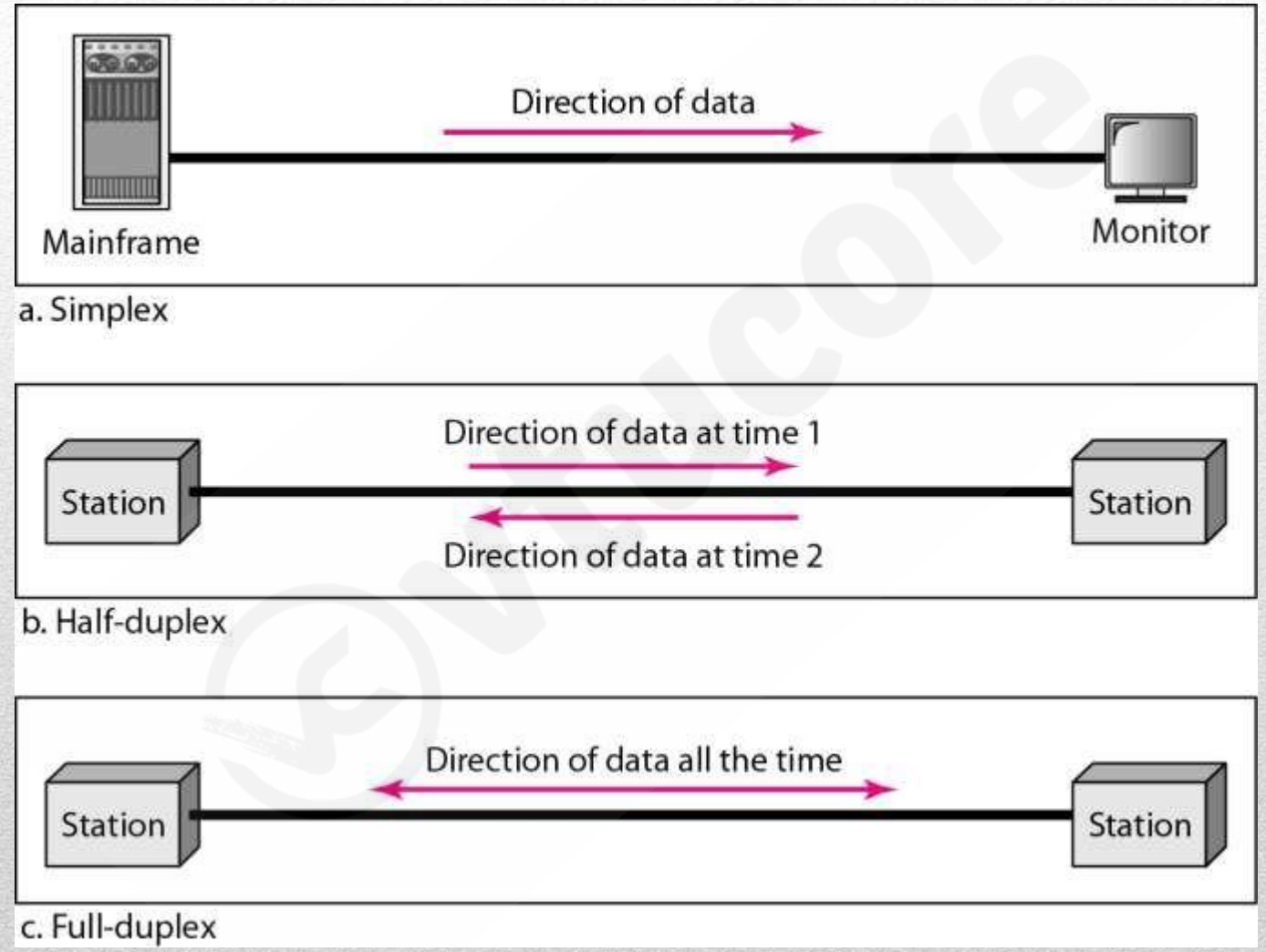
Half-Duplex

- Each station can both transmit and receive, but not at the same time.

Full –Duplex/ Duplex

- Both stations can transmit and receive simultaneously.
- Example: telephone network.
- It is used when communication in both direction is required all the time.
- The capacity of the channel must be divided between two directions.

Data Flow


Direction of data
Mainframe
Monitor
a. Simplex
Direction of data at time 1
Station
Station
Direction of data at time 2
b. Half-duplex
Direction of data all the time
Station
Station
c. Full-duplex

NETWORKS

- *A network is a interconnection of a set of devices (often referred to as nodes) capable of communication.*
- *Here device can be a host like large computer, desktop, laptop, workstation, cellular phone or security system.*
- *Here device can also be a connecting devices like router, a switch, a modem.*

Network Criteria

- **A network must meet certain number of criteria,**
- **Performance**
  - Performance can be measured in many ways, including transit time and response time.
  - Transit time is the amount of time required for a message to travel from one device to another.
  - Response time is the elapsed time between an inquiry and a response.
  - Performance is evaluated by two networking metrices: Delay and Throughput. More throughput and less delay is required.

- **Reliability**
  - Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure and the network's robustness in a catastrophe.
- **Security**
  - Network security issues include, protecting data from damage and development and implementing policies and procedures for recovery from breaches and data losses.
  - Data protection against corruption/loss of data due to:
    - Errors
    - Malicious users

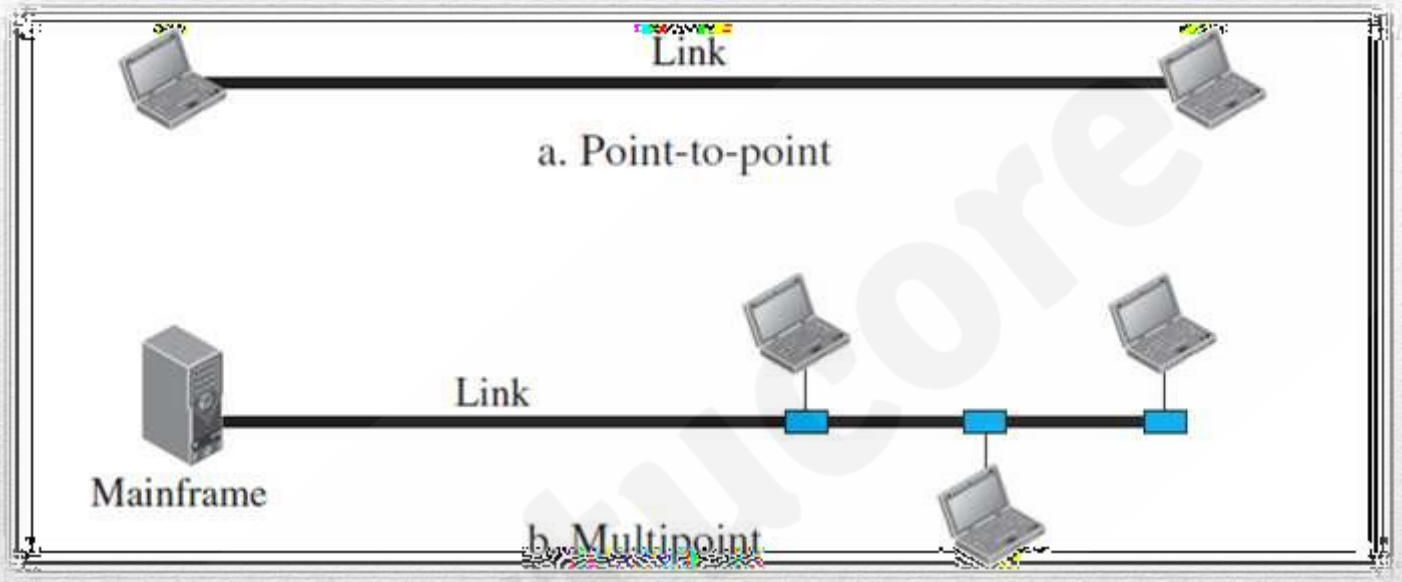
Physical Structures

Type of Connection

- A network is two or more devices connected through links.
- A link is a communications pathway that transfers data from one device to another.
- 2 possible types of connections,

  ->**Point to Point** - single transmitter and receiver
  - Provides dedicated link between two devices.
  - The entire capacity of the link is reserved for transmission between those two devices.
  - Eg : Televison and remote controller.

  -> **Multipoint/ Multidrop-** multiple recipients of single transmission
  - It is the one in which more than two specific devices share a single link.

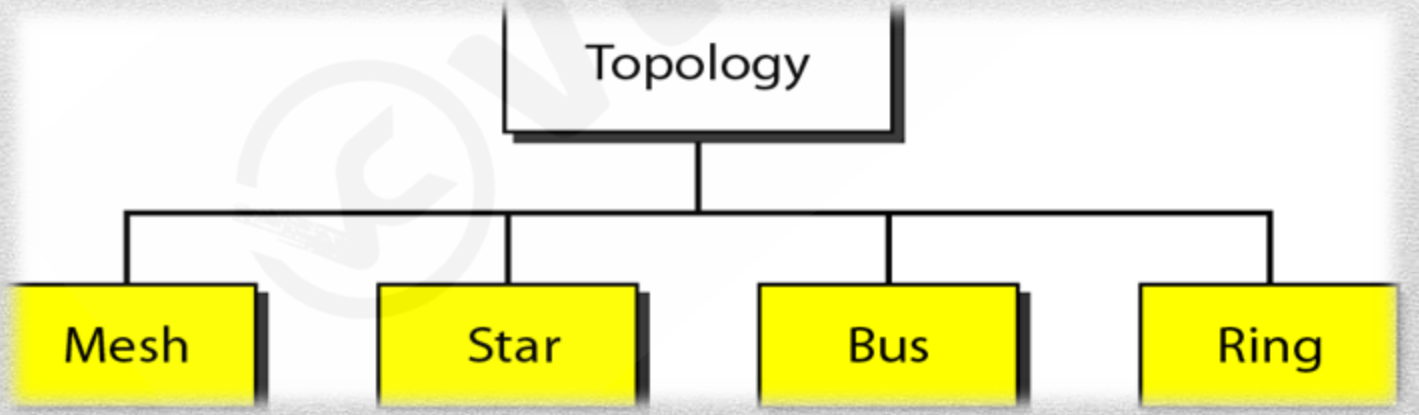


Types of connections: point-to-point and multipoint

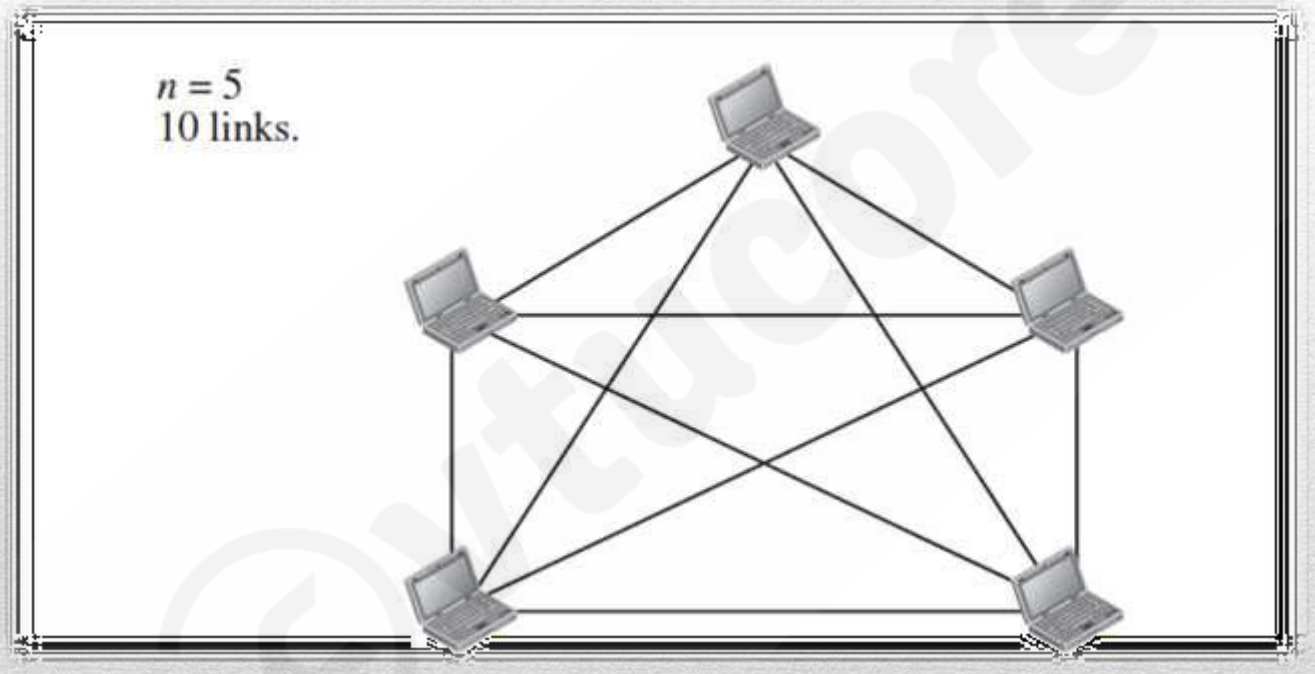
- If several devices can use the link simultaneously it is a spatially shared connection.
- If the users must take the turns to use the device then it is timeshared connection.

- **Physical Topology**
  - Physical topology refers to the way in which a network is laid out physically.
  - Two or more devices connect to a link, two or more link form topology
  - Type of transmission - Unicast, Mulitcast, Broadcast.
  - There are 4 basic topologies: Mesh, Star, Bus and Ring.

Categories of topology



Mesh Topology



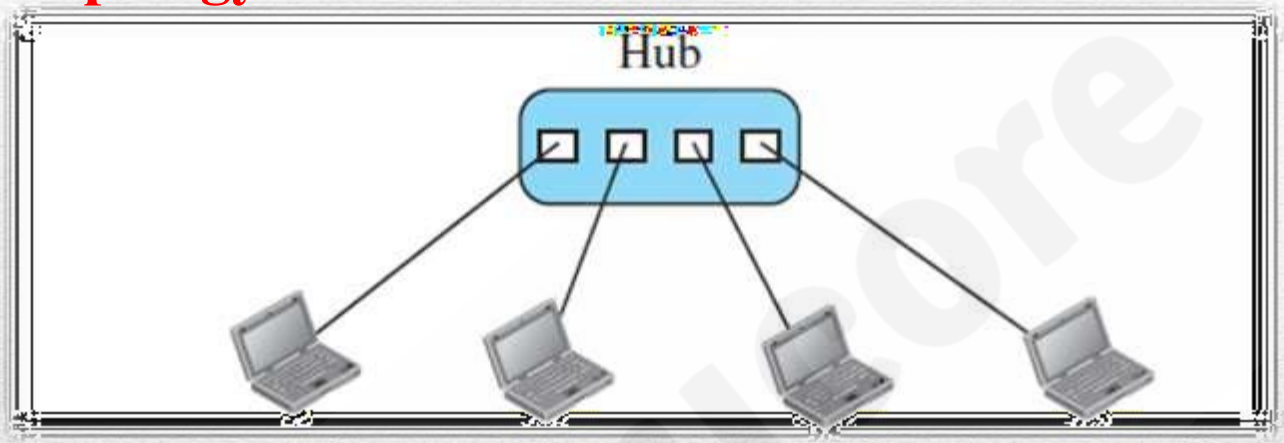
A fully connected mesh topology (five devices)

•Every device has a dedicated point to point link to every other devices.
•If n is the number of nodes, we need n(n-1) physical links .
•In duplex for communication in both direction we can divide the number of links by 2, so we need n(n-1)/2 duplex mode links.
•The use of dedicated links guarantee that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
•Mesh topology is robust.
• It provides privacy and security.
•Point to point links make fault identification and fault isolation easy.

Disadvantages:

• The amount of cabling and the number of I/O ports required.
• Every device must be connected to every other device, installation and reconnection are difficult.
•The bulk of wiring can be greater than the available space.
•Hardware required to connect each link can be expensive.

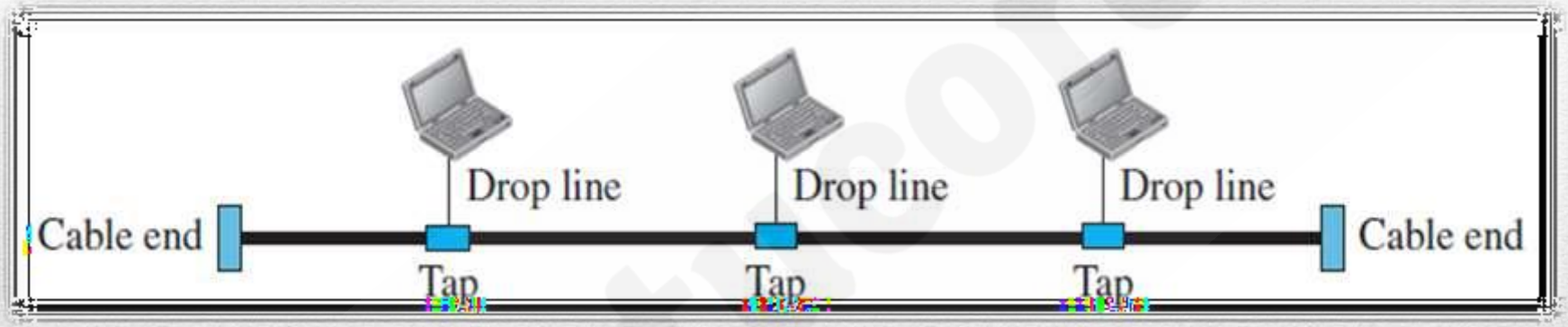
Star Topology



A star topology connecting four stations

- Here each device has dedicated point to point link only to a central controller called HUB. Devices are not directly connected to one another, sends data through controller.
- It is less expensive than mesh topology.
- Easy to install and reconfigure, less cabling is required.
- It is robust, if one link fails only that link is affected.
- Dependency of whole topology on one single point. If hub goes down, whole system will not work.
- Star Topology is used in LAN network.

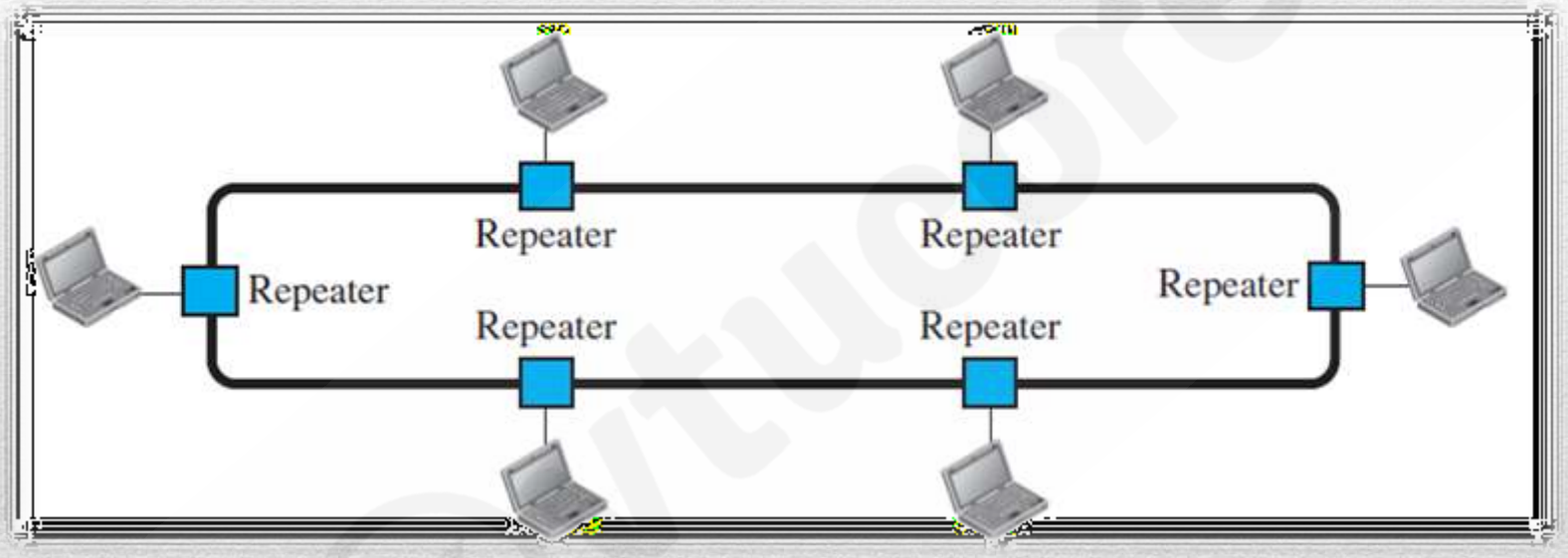
Bus Topology



A bus topology connecting three stations

- Bus topology is a multipoint.
- One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps.
- Drop line is the connection running between the device and the main cable.
- Tap is the connector that either splices or into the main cable or punctures the sheathing of the cable to create a contact with the metallic core.
- Advantages:
- Ease of Installation
- Disadvantage:
- Difficult reconnection and fault isolation .
- A bus is usually designed to be optimally efficient in installation. It can be difficult to add new devices.
- Signal reflection at the taps can cause degradation in quality.
- Fault or breakage in the bus cable stops a

Ring Topology



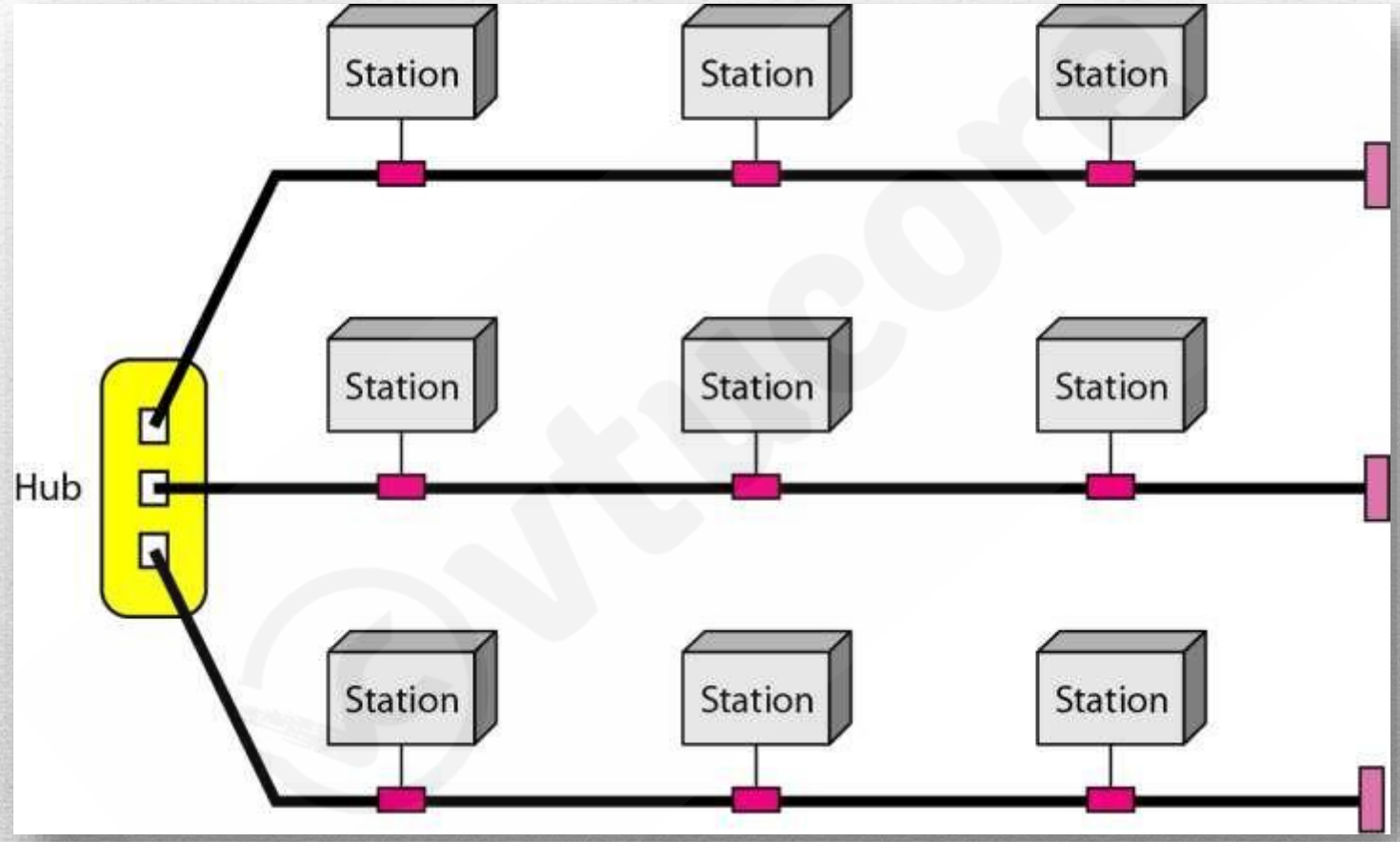
A ring topology connecting six stations

• In Ring topology, each device has a dedicated point to point connection with only 2 devices on either side of it.
• A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
•Each device in a ring incorporates a repeater.
•When a device receives signal intended for another device, its repeater regenerates the bits and passes them along.
• Ring is easy to install and reconfigure.
• Each device is linked to only its immediate neighbors.
• To add or delete a device requires changing only 2 connections.
• Fault isolation is simplifies.
• In ring signal is circulating at all times, if one device does not receive signal within a specified period, it can cause alarm.
•The alarm alerts the network operator to the problem and its location.

Disadvantage:

• Unidirectional traffic.
• Break in the ring can disable the entire network. This can be solved by using a dual ring or a switch capable of closing off the break.

Hybrid Topolology



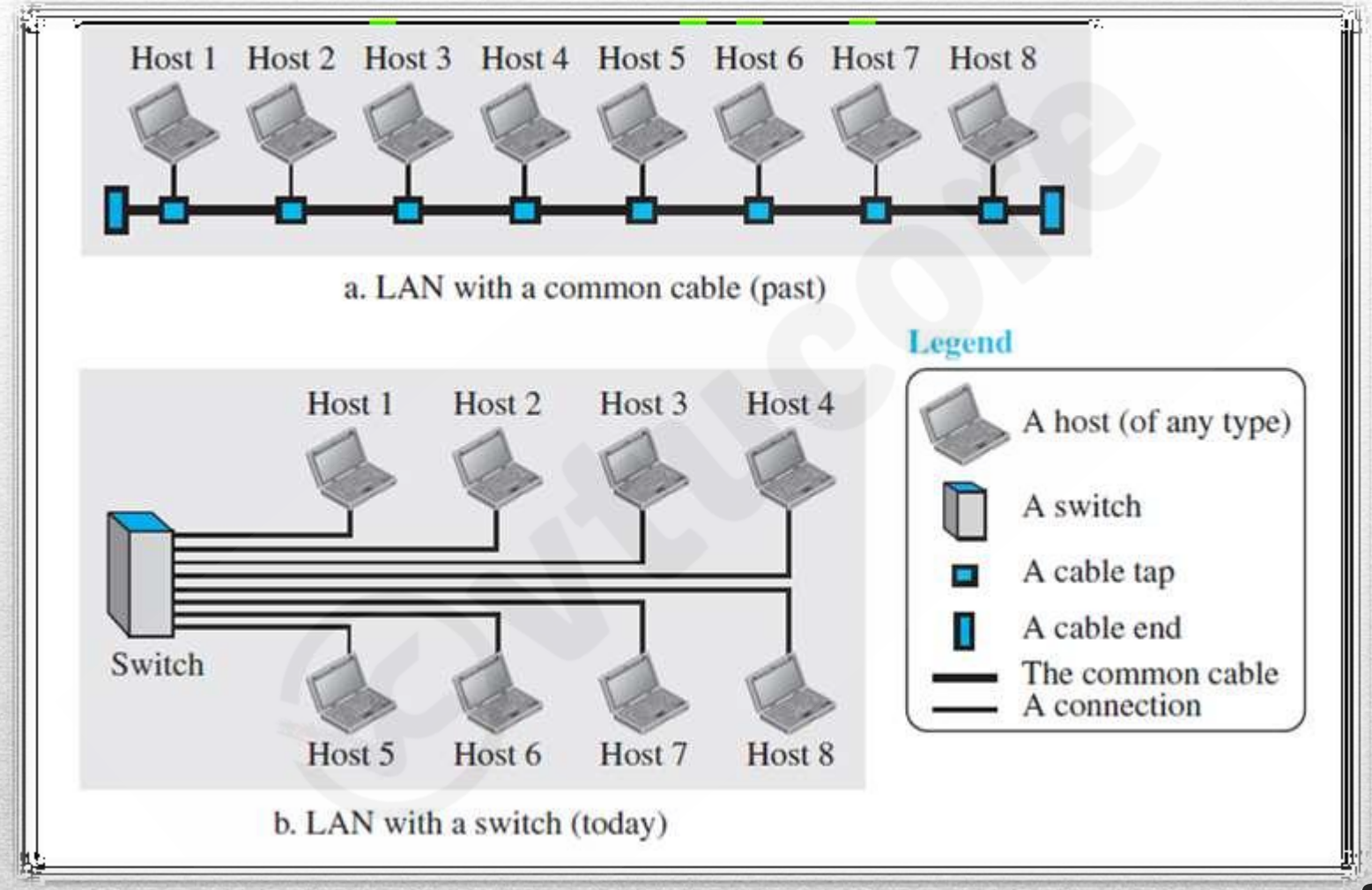
A hybrid topology: a star backbone with three bus networks

NETWORK TYPES

- Local Area Networks (LANs)
  - Short distances
  - Designed to provide local interconnectivity
- Wide Area Networks (WANs)
  - Long distances
  - Provide connectivity over large areas
- Metropolitan Area Networks (MANs)
  - Provide connectivity over areas such as a city, a campus

Local Area Networks (LANs):

- It is usually privately owned and connects some hosts in a single office, building or campus.
- A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus.
- Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN.
- A packet sent by a host to another host carries both the source host's and the destination host's addresses.
- In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet.
- Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts.



An isolated LAN in the past and today

Local Area Networks (LANs):

- When LANs were used in isolation, they were designed to allow resources to be shared between the hosts.
- LANs today are connected to each other and to WANs to create communication at a wider level.

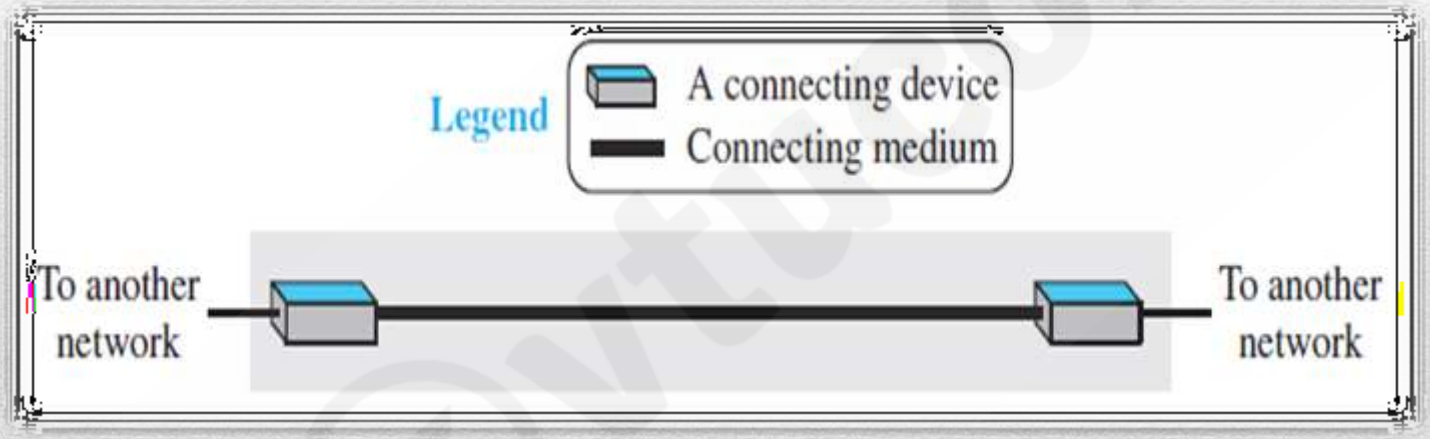
Wide Area Networks (WANs):

- A wide area network (WAN) is also an interconnection of devices capable of communication.
- A LAN is normally limited in size, spanning an office, a building, or a campus.
- WAN has a wider geographical span, spanning a town, a state, a country, or even the world. A LAN interconnects hosts.
- WAN interconnects connecting devices such as switches, routers, or modems.
- A LAN is normally privately owned by the organization that uses it.
- A WAN is normally created and run by communication companies and leased by an organization that uses it.
- 2 types of WANs : point-to-point WANs and switched WANs.

Wide Area Network

- **Point to Point WAN:**

- A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).



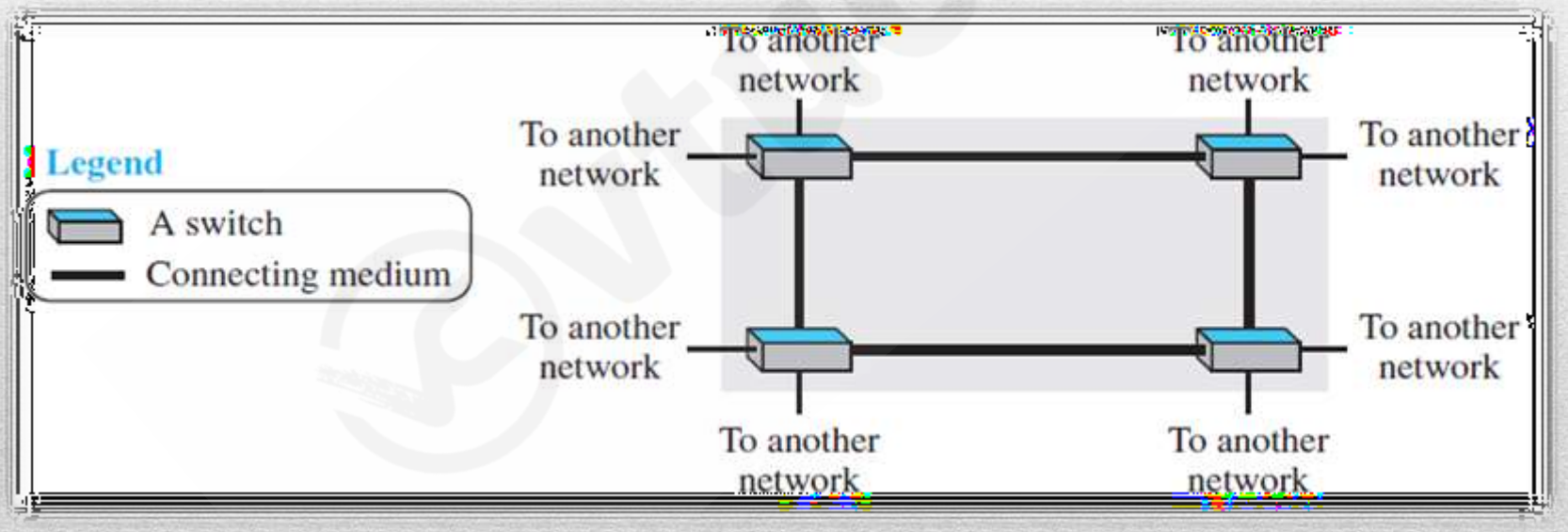
A point-to-point WAN

▪ Switched WAN:

•A switched WAN is a network with more than two ends.

•A switched WAN, is used in the backbone of global communication today.

•A switched WAN is a combination of several point-to-point WANs that are connected by switches.



A switched WAN

Internetwork

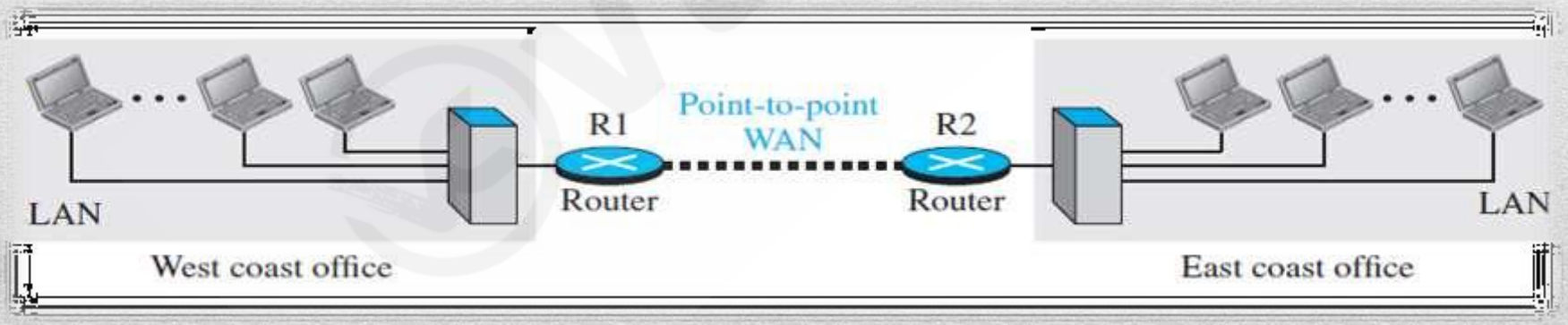
• When two or more networks are connected, they make an internetwork, or internet. As an example, assume that an organization has two offices, one on the east coast and the other on the west coast.

•Each office has a LAN that allows all employees in the office to communicate with each other.

•To make the communication between employees at different offices possible, the management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs.

•Now the company has an internetwork, or a private internet (with lowercase i).

•Communication between offices is now possible.



An internetwork made of two LANs and one point-to-point WAN

Internetwork

- When a host in the west coast office sends a message to another host in the same office, the router blocks the message, but the switch directs the message to the destination.
- When a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination.

Switching

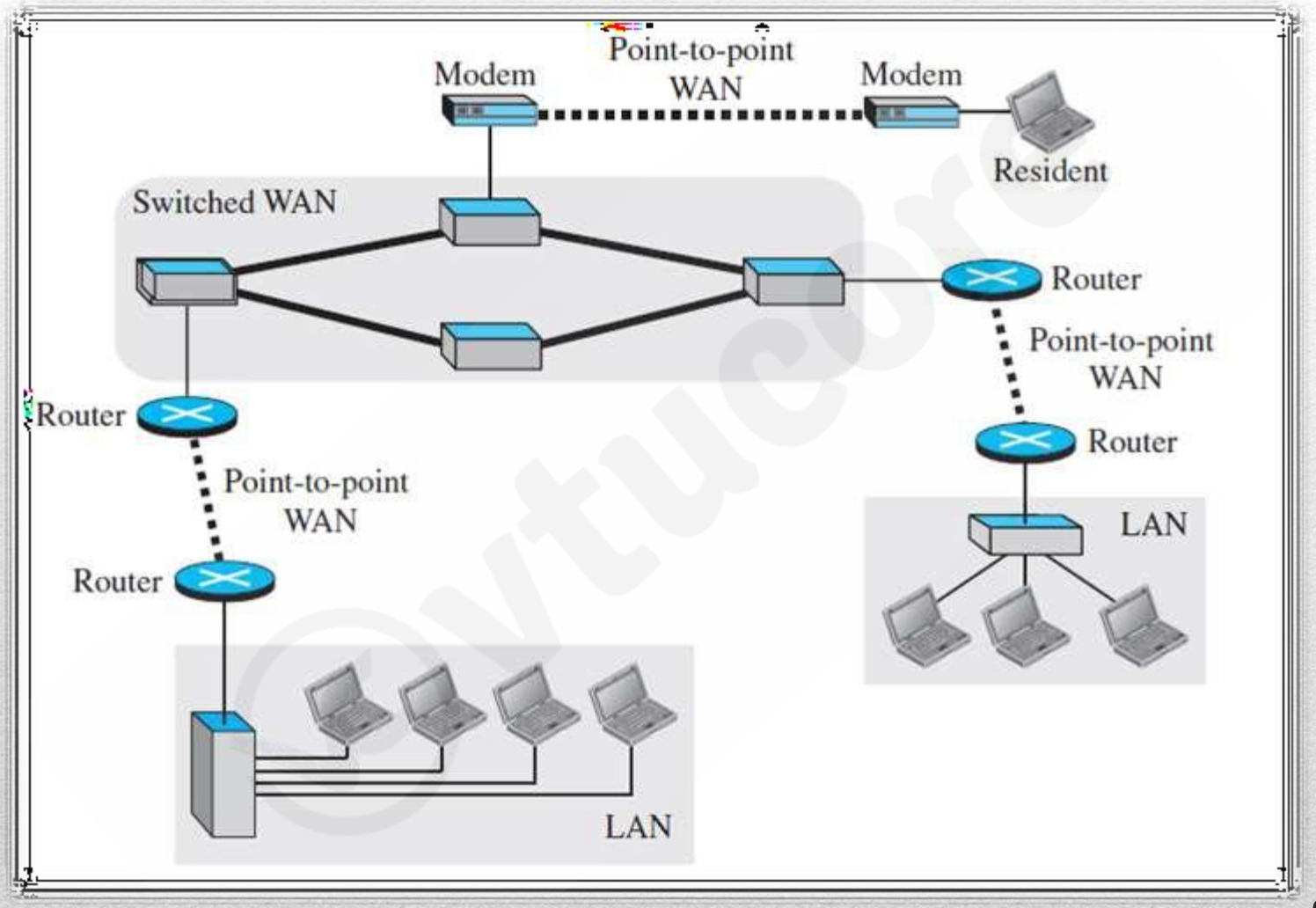
• An internet is a switched network in which a switch connects at least two links together.

•A switch needs to forward data from a network to another network when required.

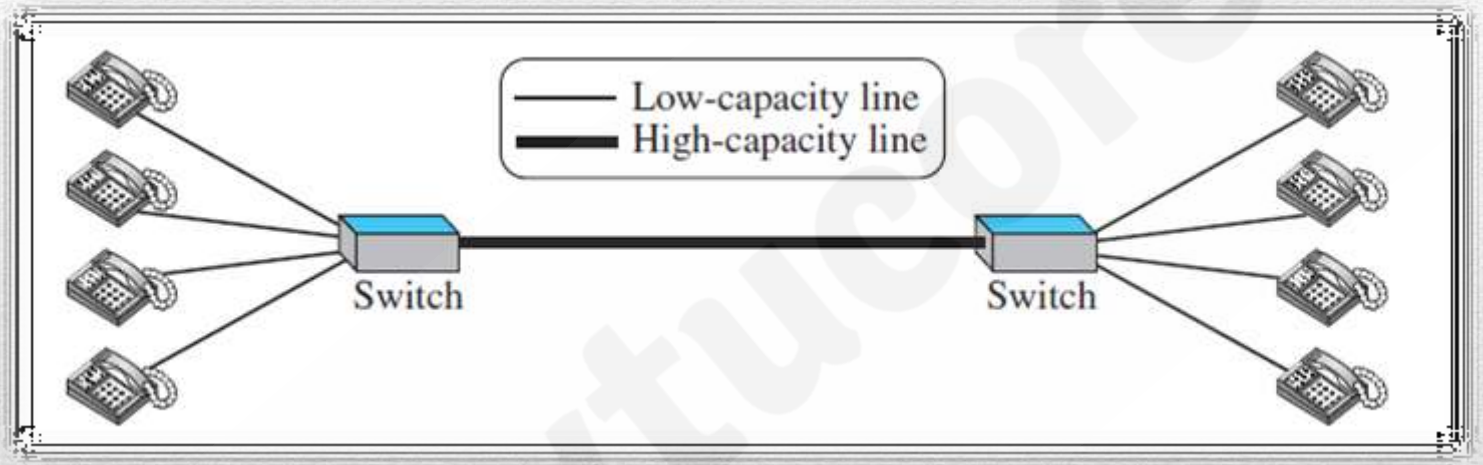
•The two most common types of switched networks are circuit-switched and packet-switched networks.

Circuit-Switched Network

- In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive.
- We have used telephone sets instead of computers as an end system because circuit switching was very common in telephone networks in the past, although part of the telephone network today is a packet-switched network.
- In Figure 1.13, the four telephones at each side are connected to a switch.
- The switch connects a telephone set at one side to a telephone set at the other side.
- The thick line connecting two switches is a high-capacity communication line that can handle four voice communications at the same time.
- The capacity can be shared between all pairs of telephone sets.
- The switches used in this example have forwarding tasks but no storing capability.



A heterogeneous network made of four WANs and three LANs



A circuit-switched network

- Two cases. In the first case, all telephone sets are busy; four people at one site are talking with four people at the other site; the capacity of the thick line is fully used.
- In the second case, only one telephone set at one side is connected to a telephone set at the other side; only one-fourth of the capacity of the thick line is used.
- This means that a circuit-switched network is efficient only when it is working at its full capacity; most of the time, it is inefficient because it is working at partial capacity.
- The reason that we need to make the capacity of the thick line four times the capacity of each voice line is that we do not want communication to fail when all telephone sets at one side want to be connected with all telephone sets at the other side.

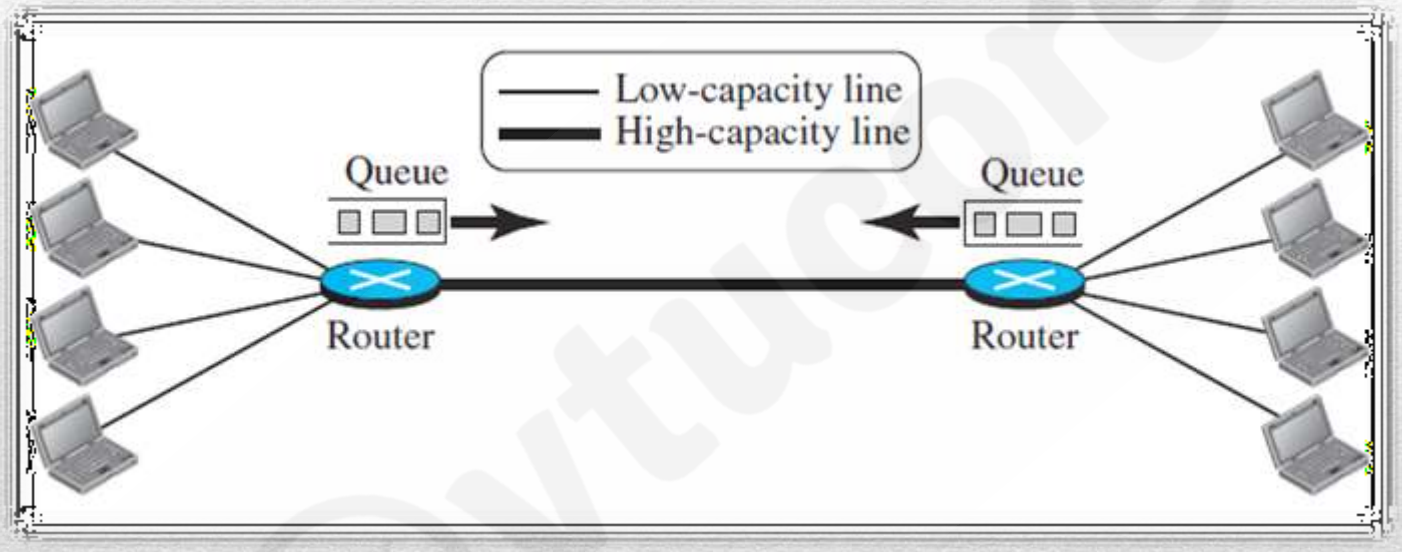
Packet Switched Network:

- In a computer network, the communication between the two ends is done in blocks of data called packets.
- Instead of the continuous communication we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers.
- This allows us to make the switche function for both storing and forwarding because a packet is an independent entity that can be stored and sent later.
- A router in a packet-switched network has a queue that can store and forward the packet.
- Assume that the capacity of the thick line is only twice the capacity of the data line connecting the computers to the routers.

•If only two computers need to communicate with each other, there is no waiting for the packets.

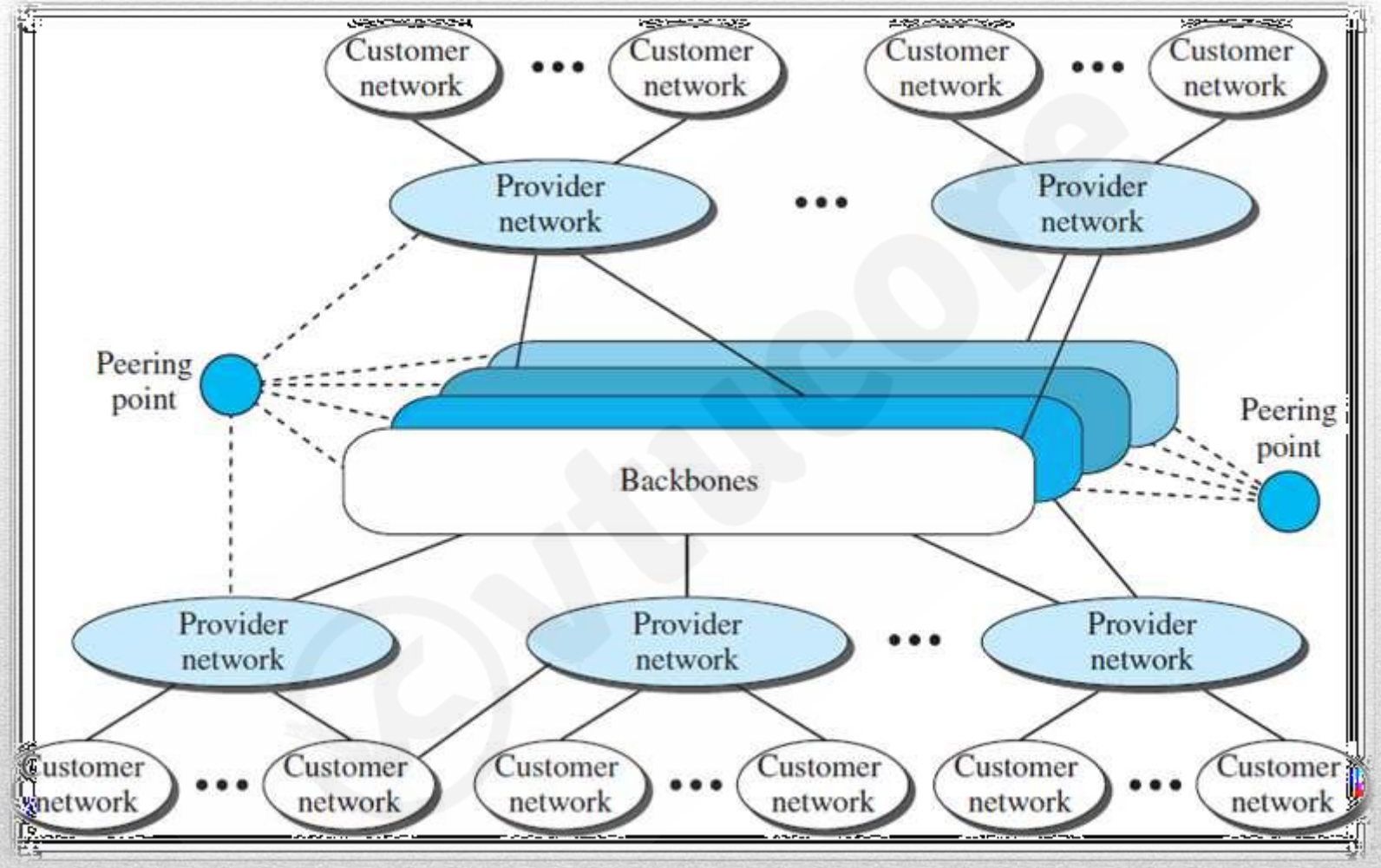
•However, if packets arrive at one router when the thick line is already working at its full capacity, the packets should be stored and forwarded in the order they arrived.

•The two simple examples show that a packet-switched network is more efficient than a circuit- switched network, but the packets may encounter some delays.



A packet-switched network

The Internet



The Internet today

•An internet is two or more networks that can communicate with each other.
•The Internet is composed of thousands of interconnected networks.
•The figure shows the Internet as several backbones, provider networks, and
•customer networks.
•At the top level, the backbones are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT.
•The back- bone networks are connected through some complex switching systems,
•called peering points.
•At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee.
•The provider networks are connected to backbones and sometimes to other provider networks.
•The customer networks are networks at the edge of the Internet that actually use the services provided by the Inter- net.
•They pay fees to provider networks for receiving services.
•Backbones and provider networks are also called Internet Service Providers (ISPs). The backbones are often referred to as international ISPs.
.The provider networks are often referred to as national or regional ISPs.

Module 1 PART 2
Network Models

TCP/IP PROTOCOL SUITE
(Transmission Control Protocol/Internet Protocol).

•TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today.

•It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality.

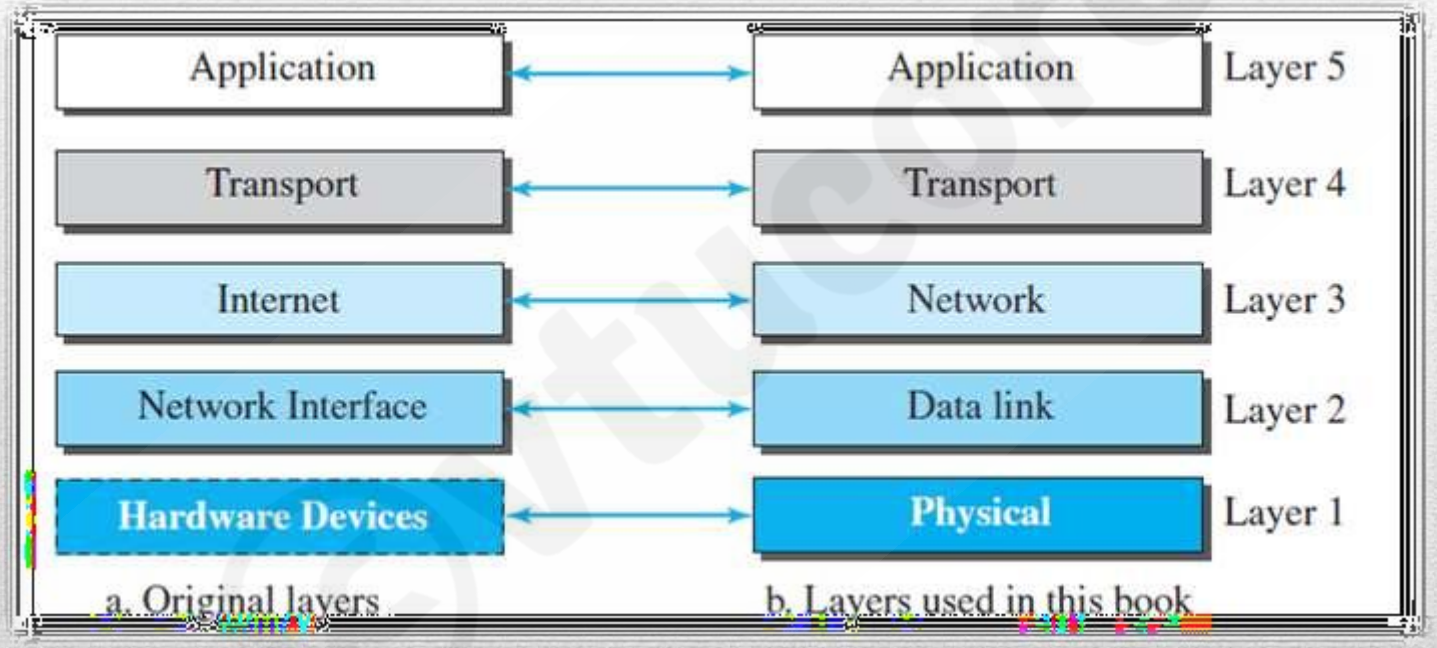
•The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols.

•The original TCP/IP protocol suite was defined as four software layers built upon the hardware.

•However, TCP/IP is thought of as a five-layer model.

TCP/IP PROTOCOL SUITE

1.5.1 Layered Architecture



Layered Architecture

•TCP/IP protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch.

•Let us assume that **computer A** communicates with **computer B**. We have five communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B).

•Each device is involved with a set of layers depending on the role of the device in the internet.

•The two hosts are involved in all five layers;

•The source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host.

•The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

•The router is involved in only three layers; there is no transport or application layer in a router as long as the router is used only for routing.

•Although a router is always involved in one network layer, it is involved in n combinations of link and physical layers in which n is the number of links the router is connected to.

•The reason is that each link may use its own data-link or physical protocol.

•For example, in the above figure, the router is involved in three links, but the message sent from source A to destination B is involved in two links.

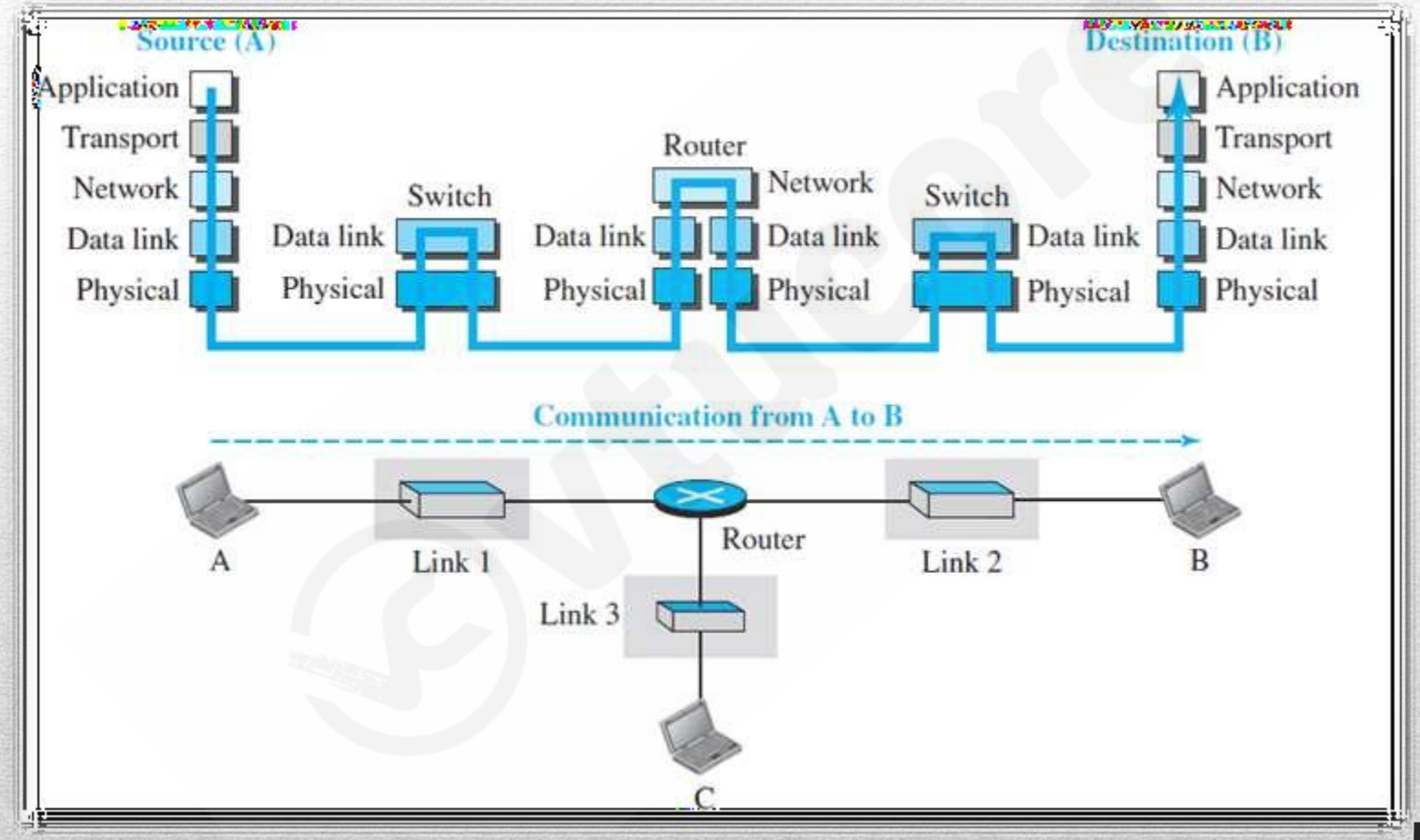
•Each link may be using different link-layer and physical-layer protocols; the router needs to receive a packet from link 1 based on one pair of protocols and deliver it to link 2 based on another pair of protocols.

•A link-layer switch in a link, however, is involved only in two layers, data-link and physical.

•Although each switch in the above figure has two different connections, the connections are in the same link, which uses only one set of protocols.

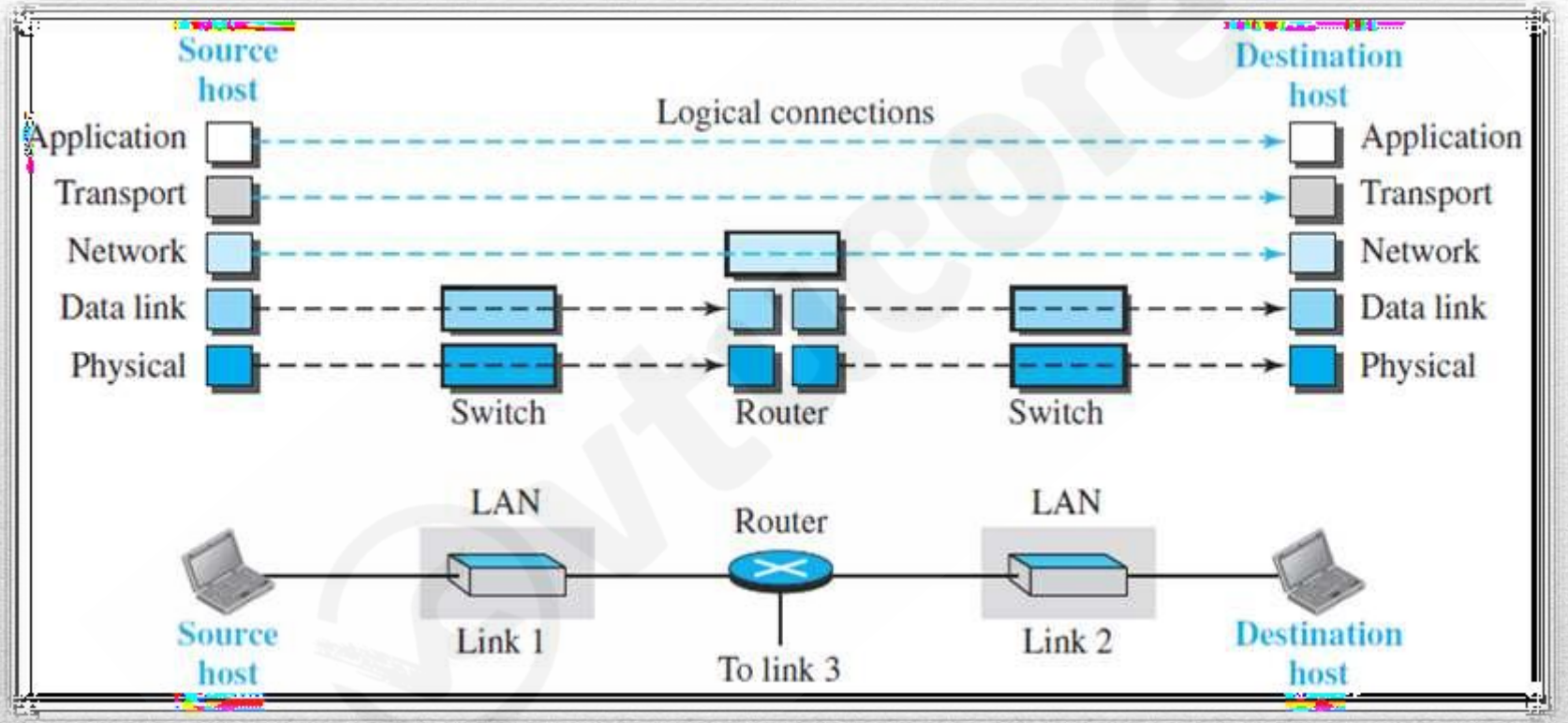
•This means that, unlike a router, a link-layer switch is involved only in one data-link and one physical layer.

Layered Architecture



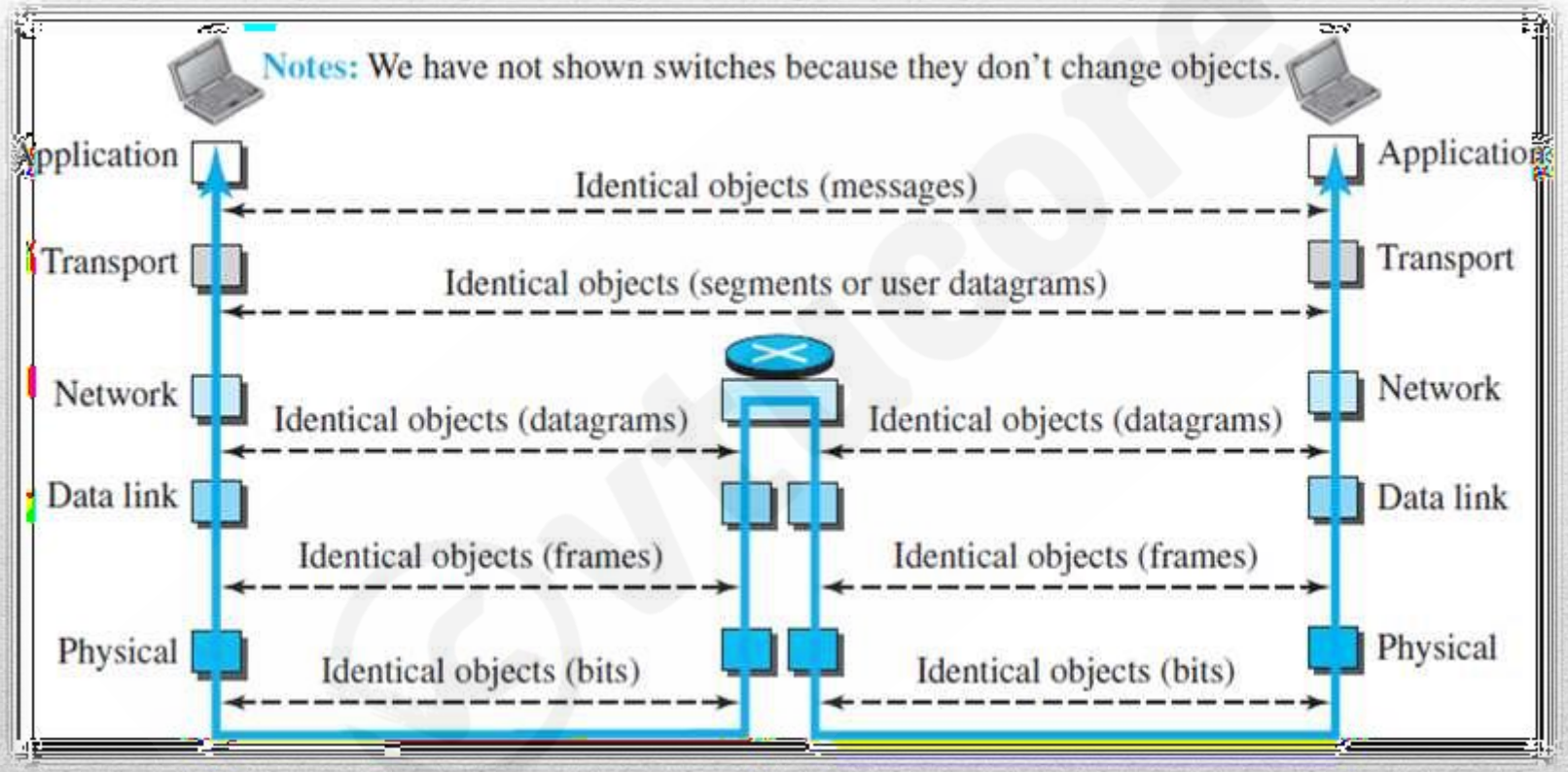
Communication through an internet

Layers in the TCP/IP Protocol Suite



Logical connections between layers of the TCP/IP protocol suite

•The duty of the application, transport, and network layers is end-to-end.
•However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router.
• In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.
•In the top three layers, the data unit (packets) should not be changed by any router or link-layer switch.
•In the bottom two layers, the packet created by the host is changed only by the routers, not by the link-layer switches.
•Although the logical connection at the network layer is between the two hosts, we can only say that identical objects exist between two hops in this case because a router may fragment the packet at the network layer and send more packets than received.
•Note that the link between two hops does not change the object.



Identical objects in the TCP/IP protocol suite

TCP/IP PROTOCOL SUITE

Description of Each Layer

- ***Physical Layer***
- ***Data-link Layer***
- ***Network Layer***
- ***Transport Layer***
- ***Application Layer***

Physical Layer:

- It is responsible for carrying individual bits in a frame across the link.
- Physical layer is the lowest level in the TCP/IP protocol suite.
- Two devices are connected by a transmission medium (cable or air). The transmission medium does not carry bits;
- It carries electrical or optical signals. So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a bit.
- There are several protocols that transform a bit to a signal.

Data-link Layer:

- An internet is made up of several links (LANs and WANs) connected by routers.
- There may be several overlapping sets of links that a datagram can travel from the host to the destination.
- The routers are responsible for choosing the best links.
- When the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link.
- The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.
- We can also have different protocols used with any link type.
- In each case, the data-link layer is responsible for moving the packet through the link.

•TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols. Any protocol that can take the datagram and carry it through the link suffices for the network layer. The data-link layer takes a datagram and encapsulates it in a packet called a frame.

•Each link-layer protocol may provide a different service.

•Some link-layer protocols provide complete error detection and correction, some provide only error correction.

Network Layer:

- The network layer is responsible for creating a connection between the source computer and the destination computer.
- The communication at the network layer is host-to-host.
- Since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet.
- The network layer is responsible for host-to-host communication and routing the packet through possible routes.
- We may ask ourselves why we need the network layer.
- We could have added the routing duty to the transport layer and dropped this layer.
- One reason, as we said before, is the separation of different tasks between different layers.
- The second reason is that the routers do not need the application and transport layers.

- Separating the tasks allows us to use fewer protocols on the routers.
- The network layer in the Internet includes the main protocol, Internet Protocol (IP), that defines the format of the packet, called a datagram at the network layer.
- IP also defines the format and the structure of addresses used in this layer.
- IP is also responsible for routing a packet from its source to its destination, which is achieved by each router forwarding the datagram to the next router in its path.
- IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services.
- This means that if any of theses services is required for an application, the application should rely only on the transport-layer protocol.
- The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols.
- A routing protocol does not take part in routing (it is the responsibility of IP), but it creates forwarding tables for routers to help them in the routing process.

•The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks.

•The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet.

•The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking.

•The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host.

•The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link layer address of a host or a router when its network-layer address is given.

Transport Layer:

•The logical connection at the transport layer is also end-to-end.

•The transport layer at the source host gets the message from the application layer, encapsulates it in a transport- layer packet (called a segment or a user datagram in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host.

•The transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host.

•We may ask why we need an end-to-end transport layer when we already have an end-to-end application layer.

•The reason is the separation of tasks and duties.

•The transport layer should be independent of the application layer.

•we have more than one protocol in the transport layer, which means that each application program can use the protocol that best matches its requirement.

•There are a few transport layer protocols in the Internet, each designed for some specific task.

•The main protocol, Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data.

•TCP provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination), error control (to guarantee that the segments arrive at the destination without error and resending the corrupted ones), and congestion control to reduce the loss of segments due to congestion in the network.

•The other common protocol, User Datagram Protocol (UDP), is a connectionless protocol that transmits user datagrams without first creating a logical connection.

•In UDP, each user datagram is an independent entity without being related to the previous or the next one (the meaning of the term connectionless).

• UDP is a simple protocol that does not provide flow, error or congestion control.

•A new protocol, Stream Control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia.

Application Layer

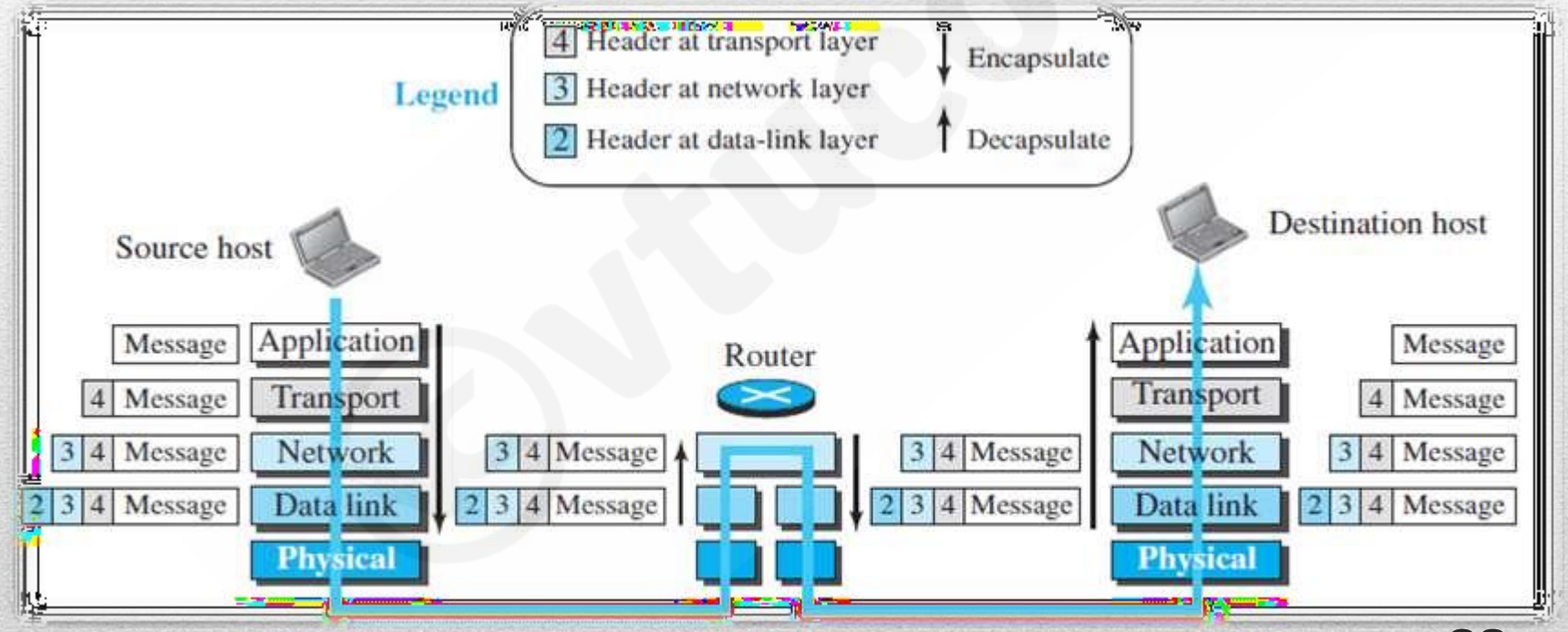
- The logical connection between the two application layers is end- to-end.
- The two application layers exchange messages between each other as though there were a bridge between the two layers.
- Communication at the application layer is between two processes (two programs running at this layer).
- To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer.
- The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.
- The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW).
- The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service.

•The File Transfer Protocol (FTP) is used for transferring files from one host to another.
•The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely.
•The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels.
•The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer.
•The Internet Group Management Protocol (IGMP) is used to collect membership in a group.

TCP/IP PROTOCOL SUITE

1.5.4 Encapsulation and Decapsulation

One of the important concepts in protocol layering in the Internet is encapsulation/ decapsulation.



• We have not shown the layers for the link-layer switches because no encapsulation/ decapsulation occurs in this device.

•Encapsulation in the source host, decapsulation in the destination host and encapsulation and decapsulation in the router.

Encapsulation at the Source Host:

•At the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a message. A message normally does not contain any header or trailer, but if it does, we refer to the whole as the message. The message is passed to the transport layer.
2. The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to- end delivery of the message, such as information needed for flow, error control, or congestion control. The result is the transport-layer packet, which is called the segment (in TCP) and the user datagram (in UDP). The transport layer then passes the packet to the network layer.

3. The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on. The result is the network-layer packet, called a datagram. The network layer then passes the packet to the data-link layer.

4. The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router, we have both decapsulation and encapsulation because the router is connected to two or more links.

1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.
2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered. The datagram is then passed to the data-link layer of the next link.
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

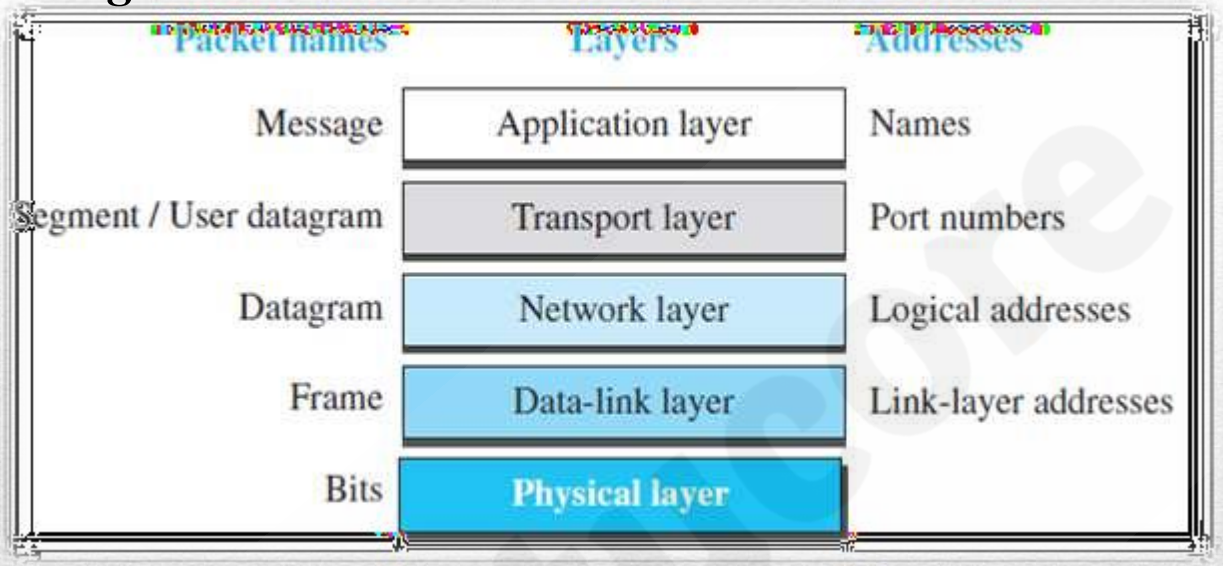
Decapsulation at the Destination Host

- At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer.
- It is necessary to say that decapsulation in the host involves error checking.

Addressing

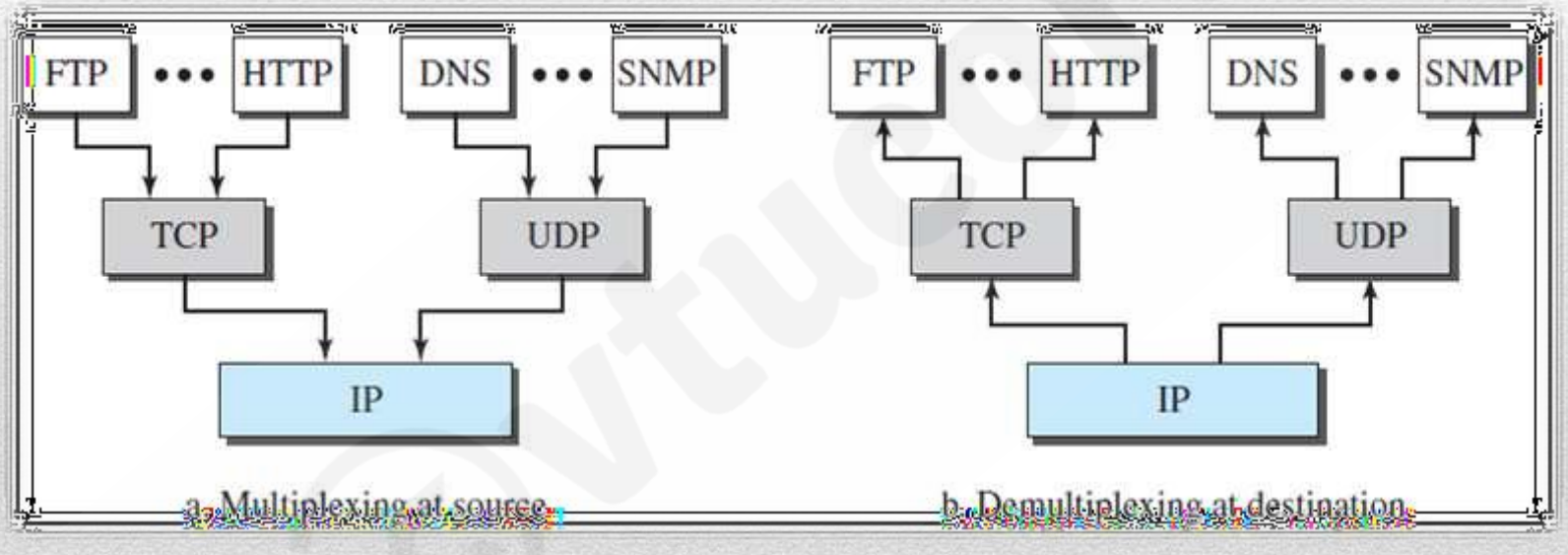
- Any communication that involves two parties needs two addresses: source address and destination address.
- Although it looks as if we need five pairs of addresses, one pair per layer, we normally have only four because the physical layer does not need addresses;
- The unit of data exchange at the physical layer is a bit, which definitely cannot have an address.
- At the application layer, we normally use names to define the site that provides services, such as someorg.com, or the e-mail address, such as somebody@coldmail.com.
- At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination.

Addressing



- Port numbers are local addresses that distinguish between several programs running at the same time.
- At the network-layer, the addresses are global. A network-layer address uniquely defines the connection of a device to the Internet.
- The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN).

Multiplexing and Demultiplexing



Multiplexing and Demultiplexing

• The TCP/IP protocol suite uses several protocols at some layers, we can say that we have multiplexing at the source and demultiplexing at the destination.
• Multiplexing in this case means that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time).
•Demultiplexing means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time).
•To be able to multiplex and demultiplex, a protocol needs to have a field in its header to identify to which protocol the encapsulated packets belong.
•At the transport layer, either UDP or TCP can accept a message from several application- layer protocols.
•At the network layer, IP can accept a segment from TCP or a user datagram from UDP. IP can also accept a packet from other protocols such as ICMP, IGMP, and so on.
•At the data-link layer, a frame may carry the payload coming from IP or other protocols such as ARP.

THE OSI MODEL

•TCP/IP protocol Suite was established in 1947, the International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards. Almost three-fourths of the countries in the world are represented in the ISO. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.

•It was first introduced in the late 1970s.

•An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

• The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.

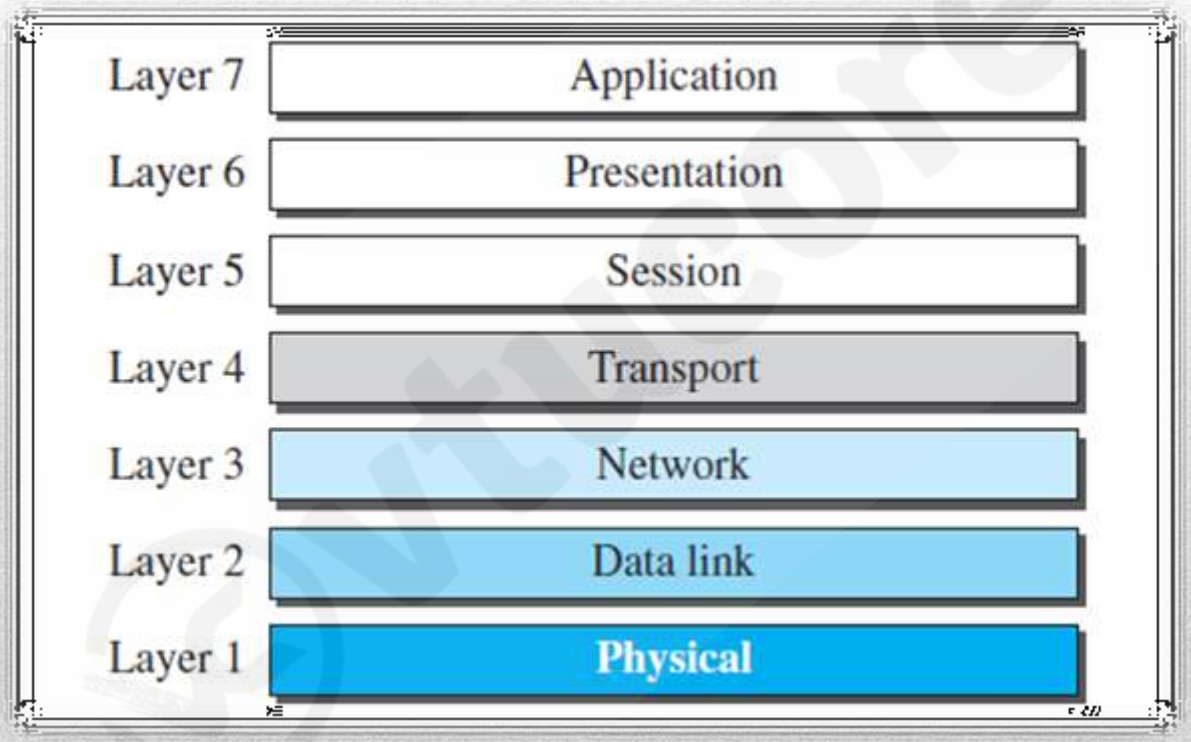
•The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

•The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.

•The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.

•It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.

THE OSI MODEL



OSI versus TCP/IP

• When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite.

•These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model.

•Two reasons were mentioned for this decision.

•First, TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport-layer protocols.

•Second, the application layer is not only one piece of software.

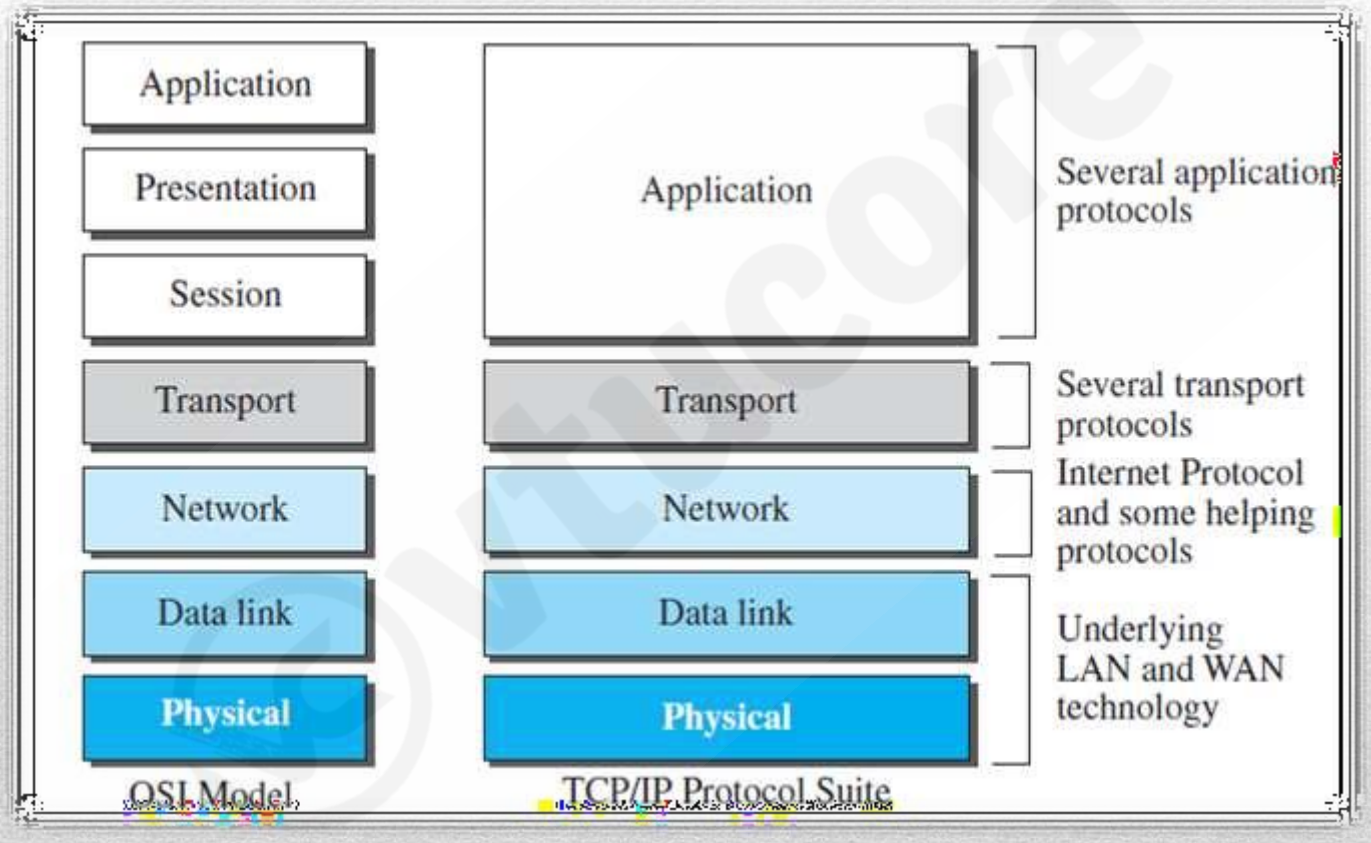
• Many applications can be developed at this layer.

•If some of the functionalities mentioned in the session and presentation layers are needed for a particular application, they can be included in the development of that piece of software.

OSI versus TCP/IP

- The OSI model appeared after the TCP/IP protocol suite.
- Most experts were at first excited and thought that the TCP/IP protocol would be fully replaced by the OSI model.
- This did not happen for several reasons, but we describe only three, which are agreed upon by all experts in the field.
- First, OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite; changing it would cost a lot.
- Second, some layers in the OSI model were never fully defined. For example, although the services provided by the presentation and the session layers were listed in the document, actual protocols for these two layers were not fully defined, nor were they fully described, and the corresponding software was not fully developed.
- Third, when OSI was implemented by an organization in a different application, it did not show a high enough level of performance to entice the Internet authority to switch from the TCP/IP protocol suite to the OSI model.

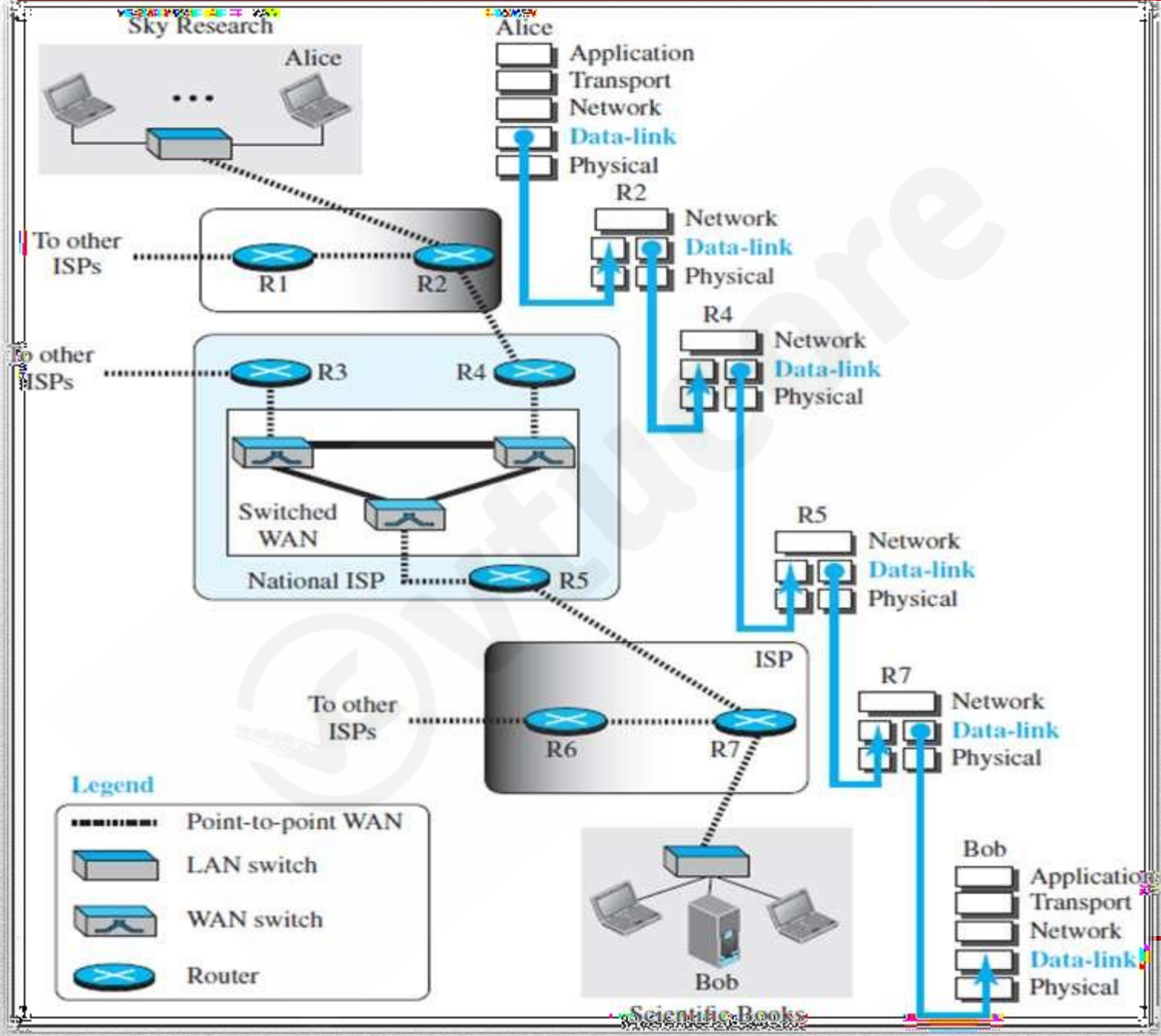
OSI versus TCP/IP



Module 1 Part 3
Data Link Layer

Introduction: (Datalink Layer)

- The Internet is a combination of networks glued together by connecting devices (routers or switches).
- If a packet is to travel from a host to another host, it needs to pass through these networks.
- Communication at the data-link layer is made up of five separate logical connections between the data-link layers in the path.
- The data-link layer at Alice's computer communicates with the data-link layer at router R2.
- The data-link layer at router R2 communicates with the data-link layer at router R4, and so on.
- Finally, the data-link layer at router R7 communicates with the data-link layer at Bob's computer.
- Only one data-link layer is involved at the source or the destination, but two data-link layers are involved at each router.
- The reason is that Alice's and Bob's computers are each connected to a single network, but each router take input from one network and sends output to another network.
- Switches are also involved in the data-link-layer communication.


Sky Research
Alice
Alice
Application
Transport
Network
Data-link
Physical
R2
Network
Data-link
Physical
R4
Network
Data-link
Physical
R5
Network
Data-link
Physical
R7
Network
Data-link
Physical
Bob
Application
Transport
Network
Data-link
Physical
To other ISPs
R1
R2
To other ISPs
R3
R4
Switched WAN
National ISP
R5
ISP
To other ISPs
R6
R7
Bob
Scientific Books
Legend
Point-to-point WAN
LAN switch
WAN switch
Router

Nodes and Links

•Communication at the data-link layer is node-to-node.

•A data unit from one point in the Internet needs to pass through many networks (LANs and WANs) to reach another point.

•Theses LANs and WANs are connected by routers.

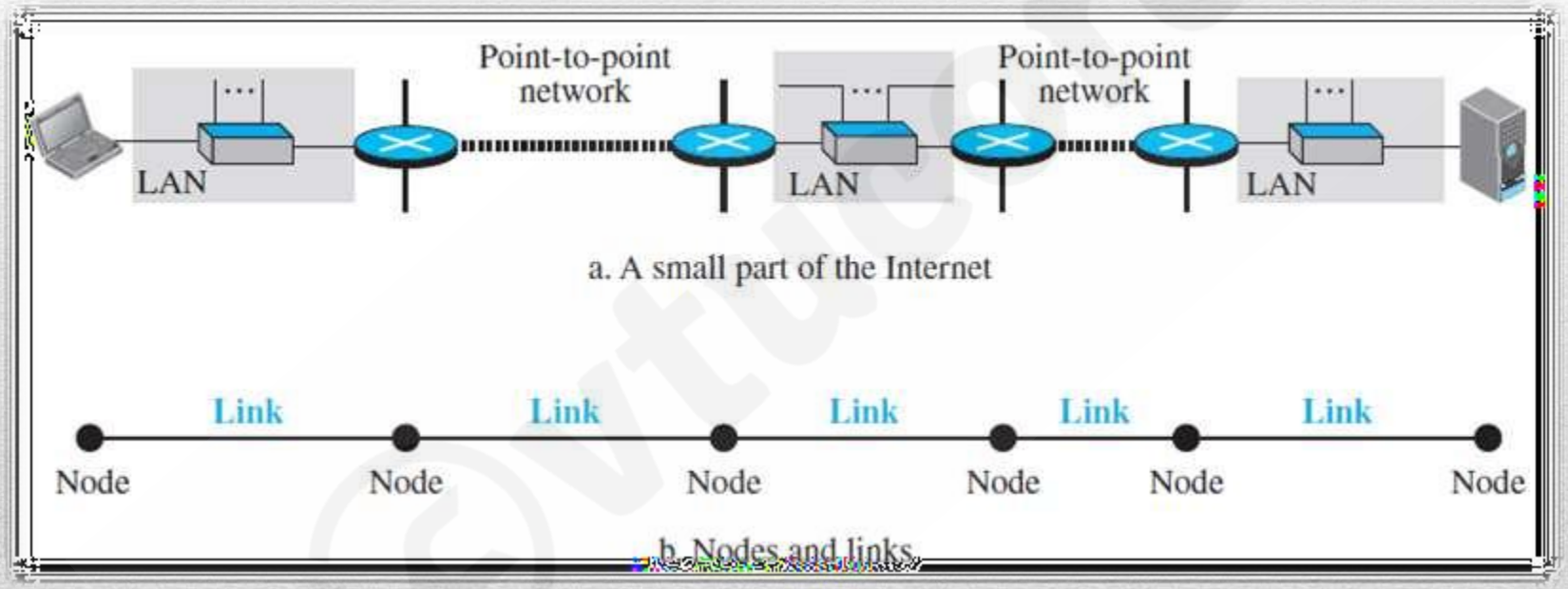
•It is customary to refer to the two end hosts and the routers as nodes and the networks in between as links.

•The first node is the source host; the last node is the destination host.

•The other four nodes are four routers.

•The first, the third, and the fifth links represent the three LANs; the second and the fourth links represent the two WANs.

Nodes and Links



Services

•The data-link layer is located between the physical and the network layers.
•The duty scope of the data-link layer is node-to-node.
•When a packet is travelling in the Internet, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.
•For this purpose, the data-link layer of the sending node needs to encapsulate the datagram received from the network in a frame, and the data-link layer of the receiving node needs to decapsulate the datagram from the frame.
•In other words, the data-link layer of the source host needs only to encapsulate, the data-link layer of the destination host needs to decapsulate, but each intermediate node needs to both encapsulate and decapsulate.
•why we need encapsulation and decapsulation at each intermediate node.

Services

•The reason is that each link may be using a different protocol with a different frame format.

•Even if one link and the next are using the same protocol, encapsulation and decapsulation are needed because the link-layer addresses are normally different.

•Assume a person needs to travel from her home to her friend's home in another city.

•The traveller can use three transportation tools.

•She can take a taxi to go to the train station in her own city, then travel on the train from her own city to the city where her friend lives, and finally reach her friend's home using another taxi.

•Here we have a source node, a destination node, and two intermediate nodes.

•The traveller needs to get into the taxi at the source node, get out of the taxi and get into the train at the first intermediate node (train station in the city where she lives), get out of the train and get into another taxi at the second intermediate node (train station in the city where her friend lives), and finally get out of the taxi when she arrives at her destination.

•A kind of encapsulation occurs at the source node, encapsulation and decapsulation occur at the intermediate nodes, and decapsulation occurs at the destination node.

•Our traveller is the same, but she uses three transporting tools to reach the destination.

•For simplicity, we have assumed that we have only one router between the source and destination.

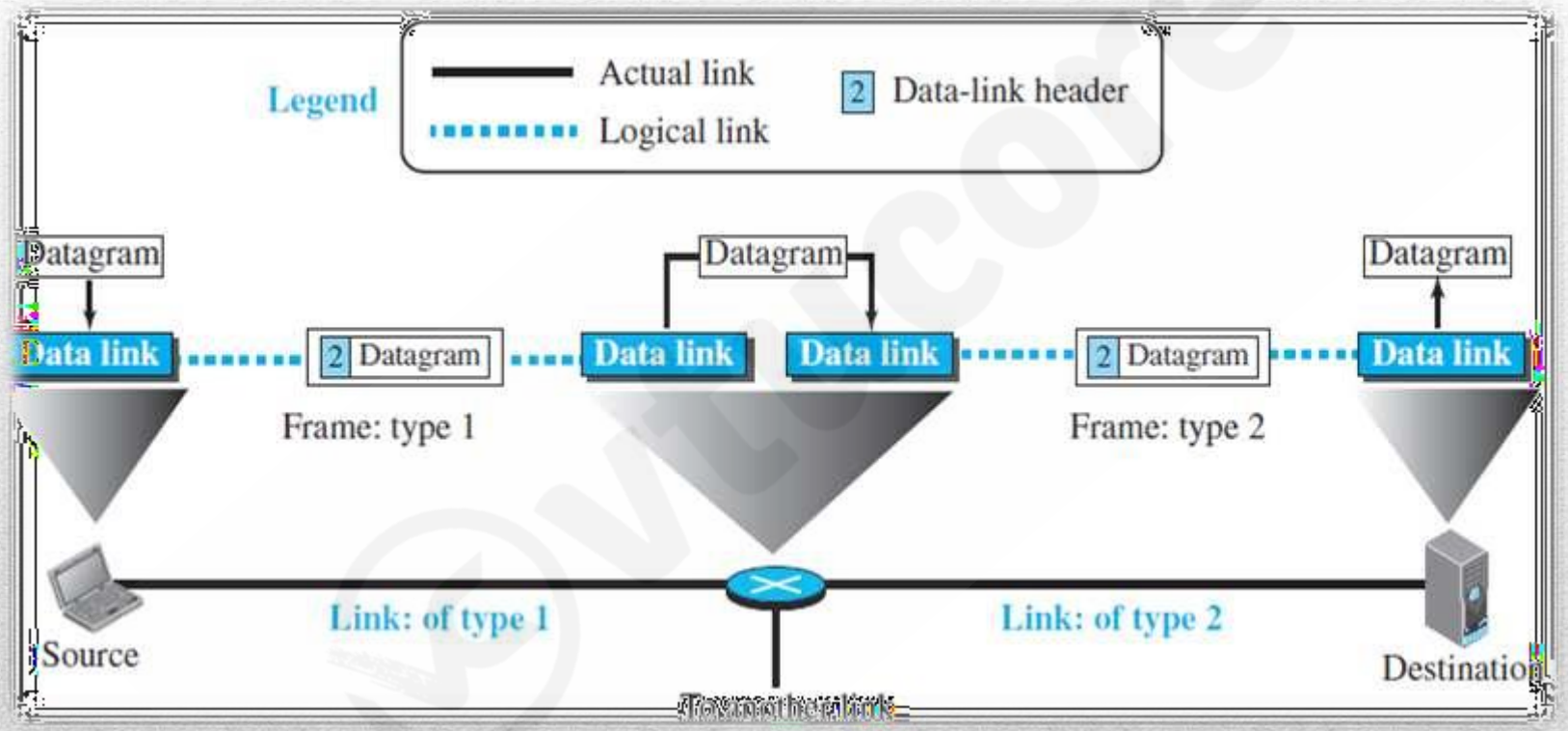
•The datagram received by the data-link layer of the source host is encapsulated in a frame.

•The frame is logically transported from the source host to the router.

Services

- The frame is decapsulated at the data-link layer of the router and encapsulated at another frame.
- The new frame is logically transported from the router to the destination host.

Services



A communication with only three nodes

Services

- *Framing*
- *Flow Control*
- *Error Control*
- *Congestion Control*

Framing

- Definitely, the first service provided by the data-link layer is framing.
- The data-link layer at each node needs to encapsulate the datagram (packet received from the network layer) in a frame before sending it to the next node.
- The node also needs to decapsulate the datagram from the frame received on the logical channel.
- Different data-link layers have different formats for framing.

Flow Control

- Whenever we have a producer and a consumer, we need to think about flow control.
- If the producer produces items that cannot be consumed, accumulation of items occurs.
- The sending data-link layer at the end of a link is a producer of frames; the receiving data-link layer at the other end of a link is a consumer.
- If the rate of produced frames is higher than the rate of consumed frames, frames at the receiving end need to be buffered while waiting to be consumed (processed).
- We cannot have an unlimited buffer size at the receiving side. We have two choices.
- The first choice is to let the receiving data-link layer drop the frames if its buffer is full.
- The second choice is to let the receiving data-link layer send a feedback to the sending data-link layer to ask it to stop or slow down.
- Different data-link-layer protocols use different strategies for flow control.
- Since flow control also occurs at the transport layer, with a higher degree of Importance.

Error Control

- At the sending node, a frame in a data-link layer needs to be changed to bits, transformed to electromagnetic signals, and transmitted through the transmission media.
- At the receiving node, electromagnetic signals are received, transformed to bits, and put together to create a frame.
- Since electromagnetic signals are susceptible to error, a frame is susceptible to error.
- The error needs first to be detected.
- After detection, it needs to be either corrected at the receiver node or discarded and retransmitted by the sending node. Since error detection and correction is an issue in every layer.

Congestion Control

•Although a link may be congested with frames, which may result in frame loss, most data-link-layer protocols do not directly use a congestion control to alleviate congestion, although some wide-area networks do.

•In general, congestion control is considered an issue in the network layer or the transport layer because of its end-to-end nature.

Two Categories of Links

Point-to-point link - the link is dedicated to the two devices

Broadcast link - the link is shared between several pairs of devices

Two Categories of Links

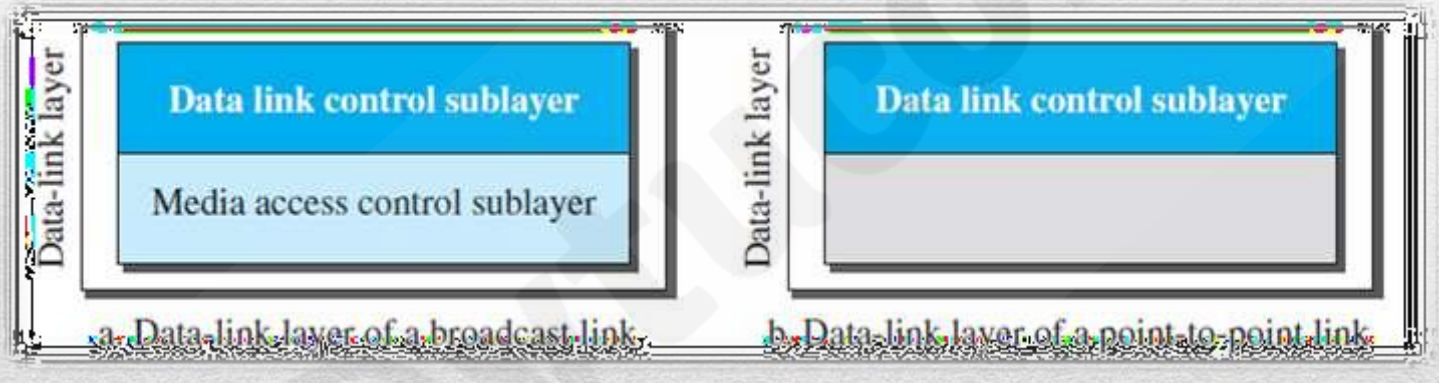
- Although two nodes are physically connected by a transmission medium such as cable or air, we need to remember that the data-link layer controls how the medium is used.
- We can have a data-link layer that uses the whole capacity of the medium; we can also have a data-link layer that uses only part of the capacity of the link.
- We can have a point-to-point link or a broadcast link.
- In a point-to-point link, the link is dedicated to the two devices; in a broadcast link, the link is shared between several pairs of devices.
- For example, when two friends use the traditional home phones to chat, they are using a point-to-point link; when the same two friends use their cellular phones, they are using a broadcast link (the air is shared among many cell phone users).

Data-Link Layer

Two Sublayers

- To better understand the functionality of and the services provided by the link layer, we can divide the data-link layer into two sublayers: data link control (DLC) and media access control (MAC).
- The data link control sublayer deals with all issues common to both point-to-point and broadcast links; the media access control sub-layer deals only with issues specific to broadcast links.

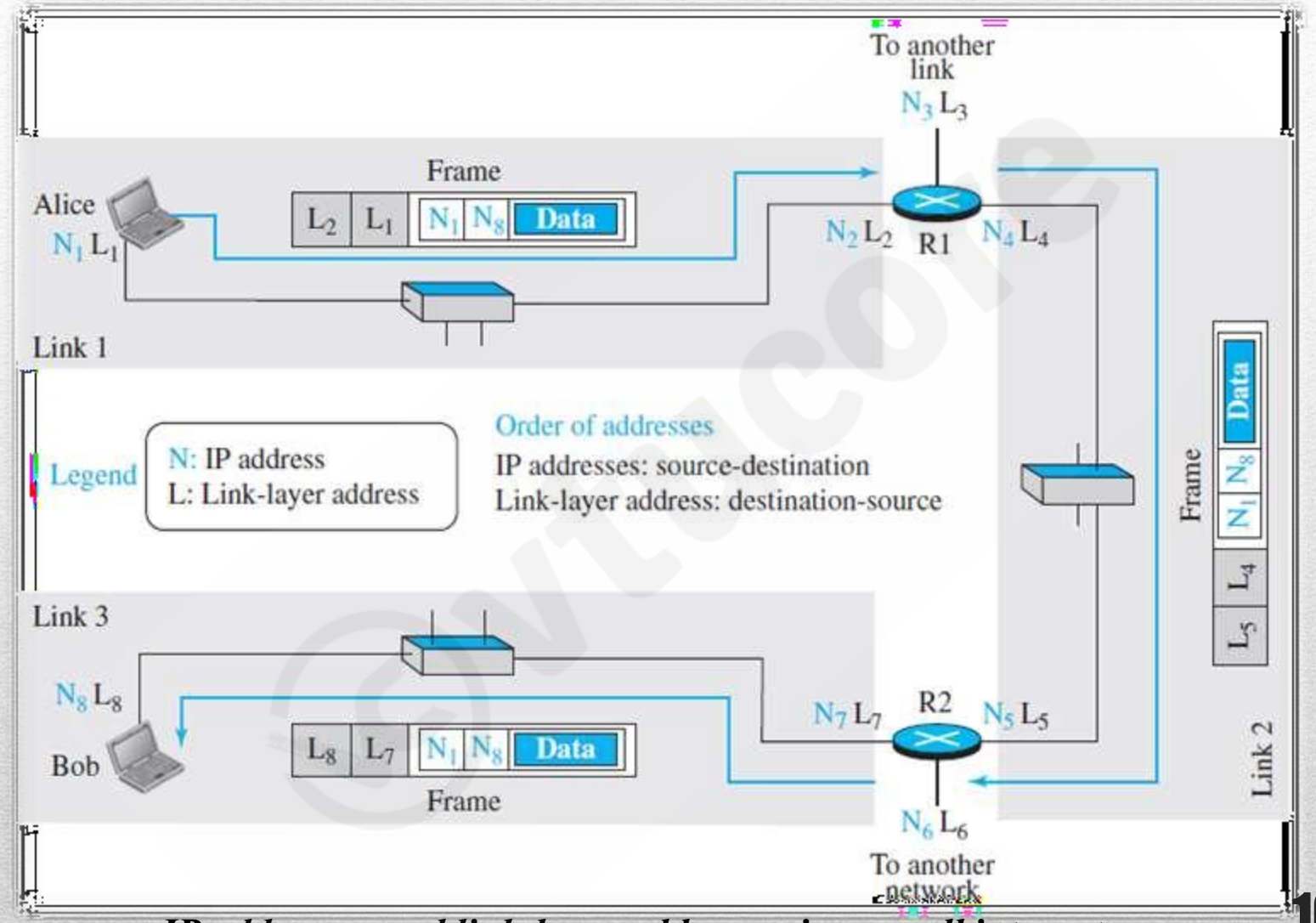
Two sub layers



LINK-LAYER ADDRESSING

- A link-layer address is sometimes called a link address, sometimes a physical address, and sometimes a MAC address.
- Since a link is controlled at the data-link layer, the addresses need to belong to the data-link layer.
- When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and two data-link addresses are added to the frame header.
- These two addresses are changed every time the frame moves from one link to another.

LINK-LAYER ADDRESSING



IP addresses and link-layer addresses in a small internet

•In the internet in Figure 9.5, we have three links and two routers.
•We also have shown only two hosts: Alice (source) and Bob (destination). For each host, we have shown two addresses, the IP addresses (N) and the link-layer addresses (L).
•Note that a router has as many pairs of addresses as the number of links the router is connected to.
•We have shown three frames, one in each link. Each frame carries the same datagram with the same source and destination addresses (N1 and N8), but the link-layer addresses of the frame change from link to link. In link 1, the link-layer addresses are L1 and L2. In link 2, they are L4 and L5.
•In link 3, they are L7 and L8.
•Note that the IP addresses and the link-layer addresses are not in the same order.
•For IP addresses, the source address comes before the destination address; for link-layer
•addresses, the destination address comes before the source.
•The datagrams and frames are designed in this way, and we follow the design.

Three Types of addresses

- ***Unicast Address-*** Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

Eg:A3:34:45:11:92:F1

- ***Multicast Address-*** Multicasting means one-to-many communication. However, the jurisdiction is local (inside the link).

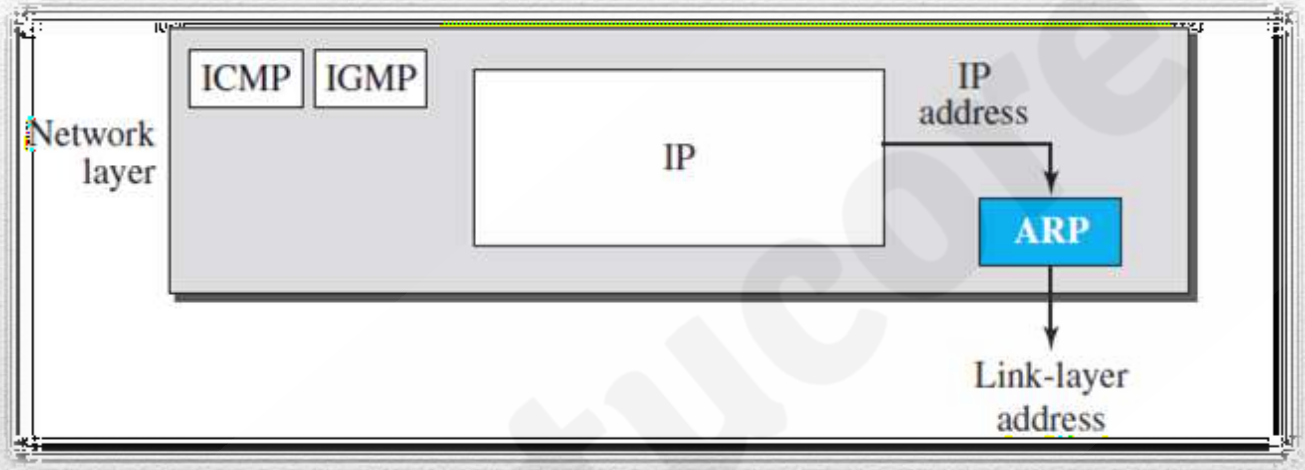
Eg: A2:34:45:11:92:F1

- ***Broadcast Address -*** Broadcasting means one-to-all communication. A frame with a destination broadcast address is sent to all entities in the link.
- Eg: FF:FF:FF:FF:FF:FF

Address Resolution Protocol (ARP)

- When a node has an IP datagram to send to another node in a link, it has the IP address of the receiving node.
- The source host knows the IP address of the default router.
- Each router except the last one in the path gets the IP address of the next router by using its forwarding table.
- The last router knows the IP address of the destination host.
- The IP address of the next node is not helpful in moving a frame through a link; we need the link-layer address of the next node.
- This is the time when the Address Resolution Protocol (ARP) becomes helpful.
- The ARP protocol is one of the auxiliary protocols defined in the network layer, as shown in Figure 9.6.
- ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.

Address Resolution Protocol (ARP)

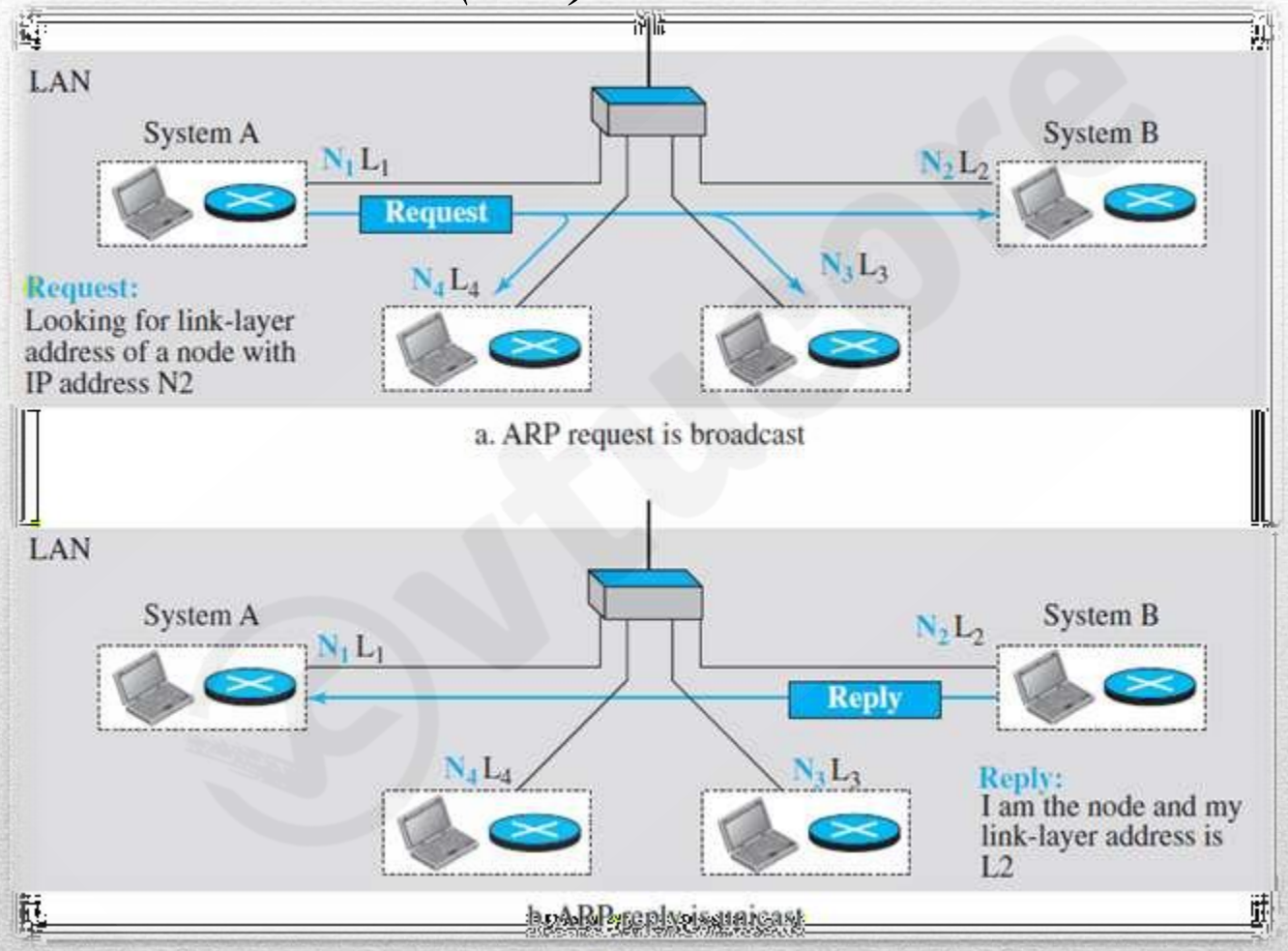


Position of ARP in TCP/IP protocol suite

•Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet.

•The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address.

Address Resolution Protocol (ARP)



ARP operation

Address Resolution Protocol (ARP)

- Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.
- The response packet contains the recipient's IP and link-layer addresses.
- The packet is unicast directly to the node that sent the request packet.
- In Figure 9.7a, the system on the left (A) has a packet that needs to be delivered to another system (B) with IP address N2.
- System A needs to pass the packet to its data-link layer for the actual delivery, but it does not know the physical address of the recipient.
- It uses the services of ARP by asking the ARP protocol to send a broadcast ARP request packet to ask for the physical address of a system with an IP address of N2.
- This packet is received by every system on the physical network, but only system B will answer it, as shown in Figure 9.7b.
- System B sends an ARP reply packet that includes its physical address.
- Now system A can send all the packets it has for this destination using the physical address it received.

Caching

•A question that is often asked is this: If system A can broadcast a frame to find the link layer address of system B, why can't system A send the datagram for system B using a broadcast frame? In other words, instead of sending one broadcast frame (ARP request), one unicast frame (ARP response), and another unicast frame (for sending the datagram), system A can encapsulate the datagram and send it to the network.

•System B receives it and keep it; other systems discard it.

•To answer the question, we need to think about the efficiency.

•It is probable that system A has more than one datagram to send to system B in a short period of time.

•For example, if system B is supposed to receive a long e-mail or a long file, the data do not fit in one datagram.

•Let us assume that there are 20 systems connected to the network (link): system A, system B, and 18 other systems. We also assume that system A has 10 datagrams to send to system B in one second.

a. Without using ARP, system A needs to send 10 broadcast frames. Each of the 18 other systems need to receive the frames, decapsulate the frames, remove the datagram and pass it to their network-layer to find out the datagrams do not belong to them. This means processing and discarding 180 broadcast frames.
b. Using ARP, system A needs to send only one broadcast frame. Each of the 18 other systems need to receive the frames, decapsulate the frames, remove the ARP message and pass the message to their ARP protocol to find that the frame must be discarded. This means processing and discarding only 18 (instead of 180) broadcast frames. After system B responds with its own data-link address, system A can store the link-layer address in its cache memory. The rest of the nine frames are only unicast. Since processing broadcast frames is expensive (time consuming), the first method is preferable.

Packet Format:

•The names of the fields are self-explanatory. The hardware type field defines the type of the link-layer protocol. Ethernet is given the type 1.

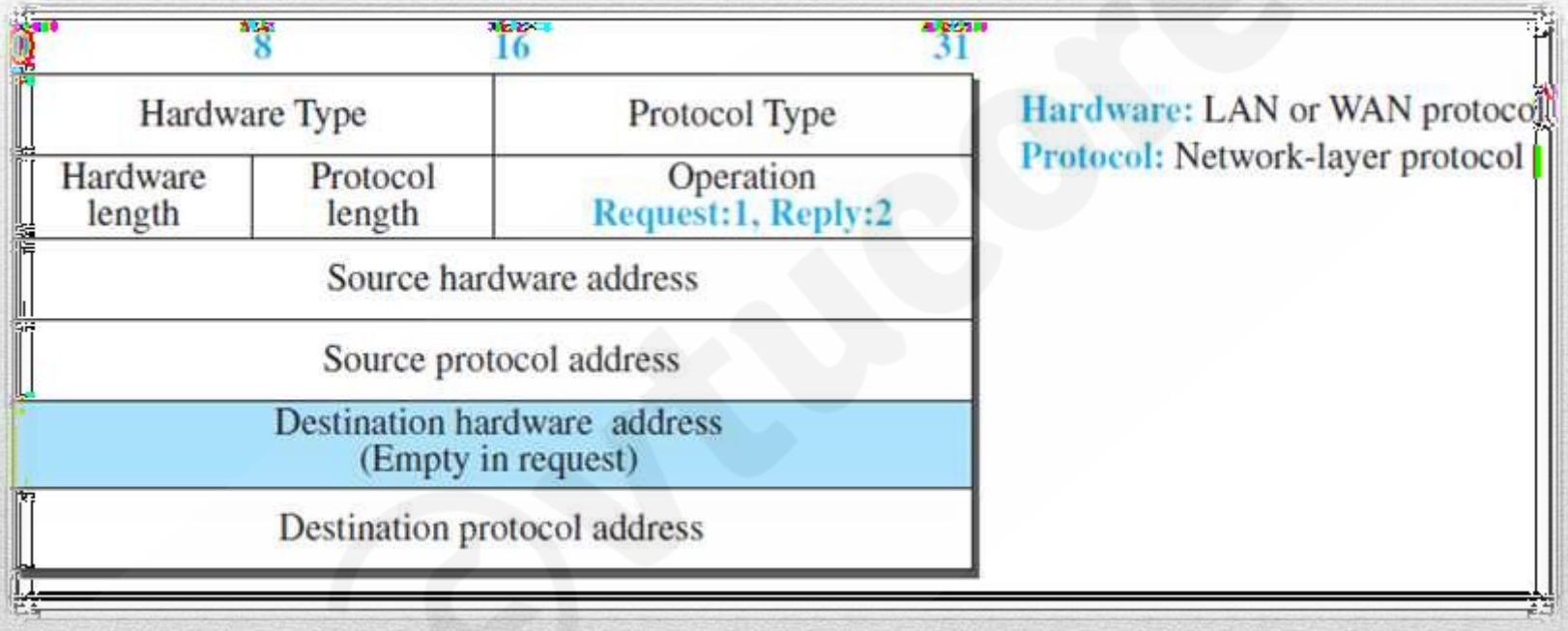
•The protocol type field defines the network-layer protocol: IPv4 protocol is (0800)16.

•The source hardware and source protocol addresses are variable-length fields defining the link-layer and network-layer addresses of the sender.

•The destination hardware address and destination protocol address fields define the receiver link-layer and network-layer addresses.

•An ARP packet is encapsulated directly into a data-link frame.

Address Resolution Protocol (ARP)



ARP packet

THANK YOU